CYBER DEFENSE MAGAZINE

eMAGAZINE

JUNE 2025

In This Edition

From Firefighting to Future-Proof: How AI is Revolutionizing Incident Management

Security Awareness Programs Are Failing - Here’s What Actually Works

Quantum-Resilient AI Security: Defending National Critical Infrastructure in a Post-Quantum Era

…and much more…

MORE INSIDE!

Contents

CYBER DEFENSE MAGAZINE
is a Cyber Defense Media Group (CDMG) publication distributed electronically via opt-in GDPR compliance-Mail, HTML, PDF, mobile and online flipbook forwards All electronic editions are available for free, always. No strings attached. Annual EDITIONs of CDM are distributed exclusively at the RSAC Conference each year.

Key contacts:

PUBLISHER
Gary S. Miliefsky
garym@cyberdefensemagazine.com

V.P. BUSINESS DEVELOPMENT
Olivier Vallez
olivier.vallez@cyberdefensemagazine.com

EDITOR-IN-CHIEF
Yan Ross
yan.ross@cyberdefensemagazine.com

MARKETING, ADVERTISING & INQUIRIES
Interested in writing for us:
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: +1-833-844-9468
International: +1-603-280-4451
New York (USA/HQ): +1-646-586-9**545**
London (UK/EU): +44-203-695-2952

E-mail: marketing@cyberdefensemagazine.com
Awards: www.cyberdefenseawards.com
Conferences: www.cyberdefenseconferences.com
Jobs: www.cyberdefenseprofessionals.com
Radio: www.cyberdefenseradio.com
TV: www.cyberdefensetv.com
Webinars: www.cyberdefensewebinars.com
Web: www.cyberdefensemagazine.com
Wire Service: www.cyberdefensewire.com

To Reach Us Via US Mail:
Cyber Defense Magazine
276 Fifth Avenue, Suite 704
New York, NY 10001
EIN: 454-18-8465
DUNS# 078358935

@MILIEFSKY

From the

Publisher…

As Publisher of *Cyber Defense Magazine*, I'm proud to witness our continued growth and leadership in the cybersecurity community. Our June 2025 issue features nearly 80 powerful articles — a testament to the unstoppable momentum of this industry and the brilliant minds shaping its future.

But today, I want to draw your attention to something even more exciting — our **flagship top awards programs for 2025 are now open** for nominations:

🎖️ **Top Global CISOs**
🏆 **Top InfoSec Innovators**
🦄 **Black Unicorn Awards**

These are not just accolades — they are global platforms that recognize *true cybersecurity leadership and innovation*. Whether you're a Chief Information Security Officer, a disruptive cybersecurity startup, or a fast-scaling company poised to become the next unicorn, *this is your chance to shine on the world stage*.

Nominate yourself, your company, or someone you admire at:
👉 https://www.cyberdefenseawards.com

Winners will be recognized at **Cyber Defense Conference 2025**, taking place October 28-29 in Orlando, Florida — an exclusive, high-trust gathering of 300+ CISO award winners and top cybersecurity leaders. Learn more at https://cyberdefenseconferences.com.

And if you're curious about where AI is headed — and what it means for our future — check out my new book, *The AI Singularity: When Machines Dream of Dominion*, available now on Amazon: https://amzn.to/4dPyakN

Stay sharp, stay secure — and remember:
Cybercriminals never sleep. Neither can your cyber defense.

Warm regards,

Gary S. Miliefsky

Gary S. Miliefsky
Publisher, *Cyber Defense Magazine*

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF
Yan Ross, JD
yan.ross@cyberdefensemagazine.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

https://www.cyberdefensemagazine.com

Copyright © 2025, Cyber Defense Magazine, a division of
CYBER DEFENSE MEDIA GROUP
1717 Pennsylvania Avenue NW, Suite 1025
Washington, D.C. 20006 USA
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.

PUBLISHER

Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
https://www.cyberdefensemagazine.com/about-our-founder/

13 YEARS ★★★★★ ANNIVERSARY

13 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense Magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

PROFESSIONALS WIRE WEBINARS

CYBERDEFENSECONFERENCES

Welcome to CDM’s June 2025 Issue

From the Editor-in-Chief

In the June 2025 issue of Cyber Defense Magazine, we are fortunate to include nearly 80 articles of vital interest to our readers. As our audience continues to grow, we provide important information for all readers, from highly technical professionals to general interest readers and users of cybersecurity products and services.

Our own focus has widened, in order to bring actionable information to the broadest spectrum of our audience. We strive to bridge the gap between cybersecurity professionals and the group of organizations needing to understand and act on these developments. It is just as important for users of cybersecurity services to understand and appreciate the value of cyber risk management as it is for those who provide these services to stay up to date in their knowledge of current developments.

I should note that an integral part of my service as Editor-in-Chief of the magazine has been the growth of my own knowledge and understanding of the trends in both threats and responses in cybersecurity practice. Coming from a non-technical background, it has been a steep learning curve. I have found that this process has sharpened our ability to help bring together the providers and users of cyber products and services.

We continue our mission to provide the best and most actionable set of resources for the CISO community and all users of digital technology in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemagazine.com

SPONSORS

NIGHTDRAGON

> **“NightDragon** *Security is not looking to invest in ‘yet another endpoint’ solution or falling for the hype of ‘yet another a.i. solution’, it’s creating a unique platform for tomorrow’s solutions to come to market faster, to breathe new life into a stale cyber defense economy”*
>
> *-David DeWalt*
>
> *Managing Director and Founder NightDragon Security*

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

hello@venturescope.com ✉
www.venturescope.com 🌐
@venturescope

VentureScope®
STRATEGY · DEEP TECH · INVESTMENT

VentureScope® works with creative entrepreneurs, venture capital investors, and large private and public sector organizations around the world that are trying to solve interesting problems. Our team specializes in problem deconstruction and framing, product development, business model refinement, go-to-market strategies, build-buy-partner decisions, strategic partnerships, investment and growth analysis, and a variety of innovation methodologies. Whether you're a budding entrepreneur, a scrappy startup, an experienced investor, or an established organization developing a new service or capability, we will not only advise you on what to do, but work as part of your team to apply our recommendations.

Our team has over 60 years of combined experience launching new business ventures, investing in promising startups, running startup accelerators, teaching and providing strategic innovation and general management consulting services to large private and public sector organizations. We own and operate the MACH37 Cyber Accelerator®. We're on the pulse of emerging and over-the-horizon technology, and are tracking their growth and development against important industry problems to inform our dealflow and give you exceptional advice.

Expertise

LEAN STARTUP METHODOLOGY
BUSINESS MODEL STRATEGY
PROBLEM DECONSTRUCTION & FRAMING
PRODUCT DEVELOPMENT
GO-TO-MARKET STRATEGY
REVENUE GENERATION
TECHNOLOGY SCOUTING & INVESTMENT DEALFLOW
BUILD-BUY-PARTNER DECISIONS
INVESTMENT & GROWTH ANALYSIS
STRATEGIC PARTNERSHIPS
CHALLENGE-DRIVEN & OPEN INNOVATION
INNOVATION PIPELINE DESIGN & IMPLEMENTATION
CREATIVITY & STRATEGIC FACILITATION
INSTRUCTIONAL DESIGN & EXPERIENTIAL TRAINING
HUMAN PERFORMANCE

2009
Founded

2010
Co-Founded and invested in WeatherAlpha

2011
Helped establish and run cross community crowdsourcing program; Obtained certification in InnoCentive's "Challenge-Driven Innovation" and problem deconstruction methodology

2012
Authored the business plan for Booz Allen's "Building a Culture of Innovation" and "Ventures" teams

2013
Launched and piloted Booz Allen's internal shark tank and accelerator

2014
Brokered Booz Allen's partnership with DC's 1776 incubator; Co-Founded and invested in Lunchin; Organized Startup Weekend "Women's Edition"

2015
Directed Smart-X accelerator in the West Bank; Mentee placed 1st out of 100 in GW's New Venture Competition

2016
Served as Entrepreneur-In-Residence at Techstars; Directed Techstars cybersecurity pre-accelerator program; Co-founded HackEd

2017
Joined MACH37® accelerator; Began working with Steve Blank to advise US government on innovation

2018
Acquired MACH37®; Participated in SXSW panel "War Games: From Battlefield to Ballot Box"

2020
Highlighted in Forbes magazine; Joined Steve Blank's Columbia University Business School Lean Launchpad Teaching Team

Altitude Cyber

"Built on passion and expertise, Altitude Cyber delivers strategic advisory services specifically tailored for founders, investors, startups, and their boards. Our unique approach fuses strategic insight with financial acumen to help your company soar to new heights."

Dino Boukouris

Managing Partner, Altitude Cyber

Guiding cybersecurity businesses globally through every stage of growth with tailored advisory services for founders, CEOs, investors, and boards.

Founders & CEOs

Altitude is your trusted advisor throughout your entrepreneurial journey. We guide you as you grow your business, navigate fundraising processes, construct advisory boards, plan your long-term exit strategy, develop strategic relationships with key partners and investors, and more.

Investors

We offer a range of strategic advisory services to support your existing portfolio companies, as well as your potential investments or acquisition targets. Our solutions are tailored to fit your needs, with flexible engagement models that align incentives to maximize outcomes.

Boards

We provide in-depth strategic advisory services, tailored to align with the evolving needs of growing businesses. Our support includes strategic business and corporate development, mergers & acquisitions, corporate finance, long term exit planning, advisor selection, and more.

Firm Highlights

Decades of experience as world class operators and advisors

Highly curated research and thought leadership on strategic activity in the cyber market

Deep industry relationships and partnerships across strategic and financial partners

Cyber Network

15,000+	Cyber Executives
3,000+	Investors
1,000+	CISOs

Cyber Knowledge

4,500+	Company Tracker
3,000+	M&A Transactions
8,500+	Financing Transactions

Extensive, global relationships with cyber executives, investors, CISOs, policy influencers, and service providers

Altitude Cyber, LLC | www.altitudecyber.com

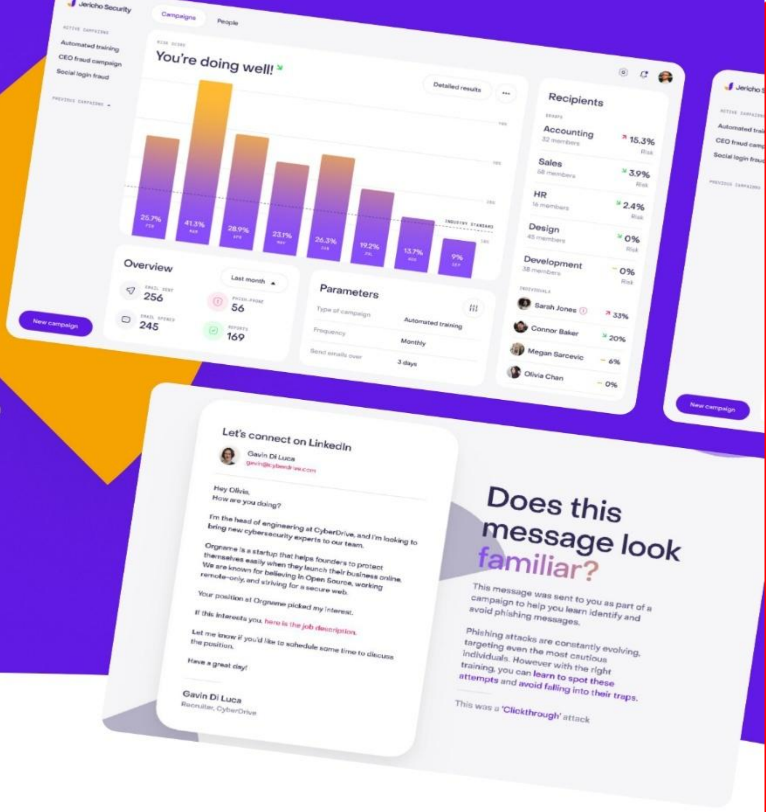
For inquiries or further information please contact Altitude Cyber at: dino@altitudecyber.com

Jericho Security

Jericho Security uses AI to fight AI in a new frontier of cybersecurity

Cyber Threats Evolve—So Should Your Defense

Phishing attacks are no longer generic—they're targeted, adaptive, and constantly evolving. Cybercriminals are leveraging dark web data, deepfake technology, and AI-driven social engineering to bypass traditional defenses.



Parameters

Type of campaign: Automated training

Frequency: Monthly

Send emails over: 3 days

Let's connect on LinkedIn

Gavin Di Luca
gavin@cyberdrive.com

Hey Olivia,
How are you doing?

I'm the head of engineering at CyberDrive, and I'm looking to bring new cybersecurity experts to our team.

Orgname is a startup that helps founders to protect themselves easily when they launch their business online. We are known for believing in Open Source, working remote-only, and striving for a secure web.

Your position at Orgname picked my interest.

If this interests you, here is the job description.

Let me know if you'd like to schedule some time to discuss the position.

Have a great day!

Gavin Di Luca
Recruiter, CyberDrive

Does this message look familiar?

This message was sent to you as part of a campaign to help you learn identify and avoid phishing messages.

Phishing attacks are constantly evolving, targeting even the most cautious individuals. However with the right training, you can learn to spot these attempts and avoid falling into their traps.

This was a 'Clickthrough' attack

How it Works

Defense That Learns. Security That Wins.

1 Hyper-personalized Phishing Simulations

Mimic and keep pace with real-world spearphishing tactics using dark-web intelligence, social engineering, and deepfake deception to test and prepare employees across multiple channels (email, text, audio).

2 Adaptive Security Training Videos

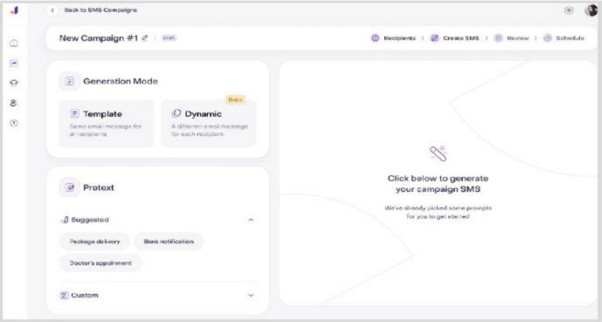
Dynamically customize training based on employee risk profiles and attack patterns, ensuring tailored, effective learning experiences.

3 Automated Threat Remediation

Detect, analyze, and take actions on phishing attempts instantly, feeding data back into the system to strengthen defenses over time.

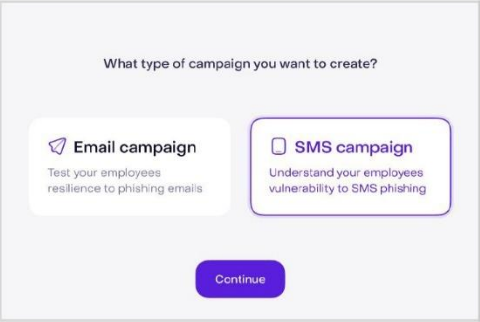
4 Seamless Security Stack Integration

Works with existing SIEM, email security, and compliance platforms, enhancing interoperability and real-time threat intelligence sharing.



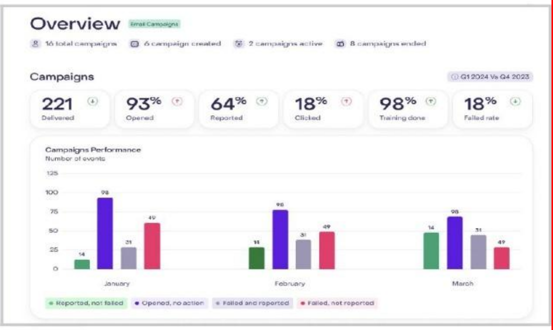
Click below to generate your campaign SMS

We've already picked some prompts for you to get started


What type of campaign you want to create?

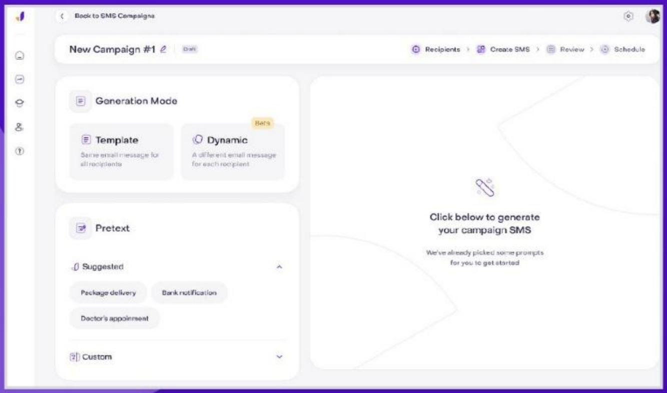
Email campaign
Test your employees resilience to phishing emails

SMS campaign
Understand your employees vulnerability to SMS phishing

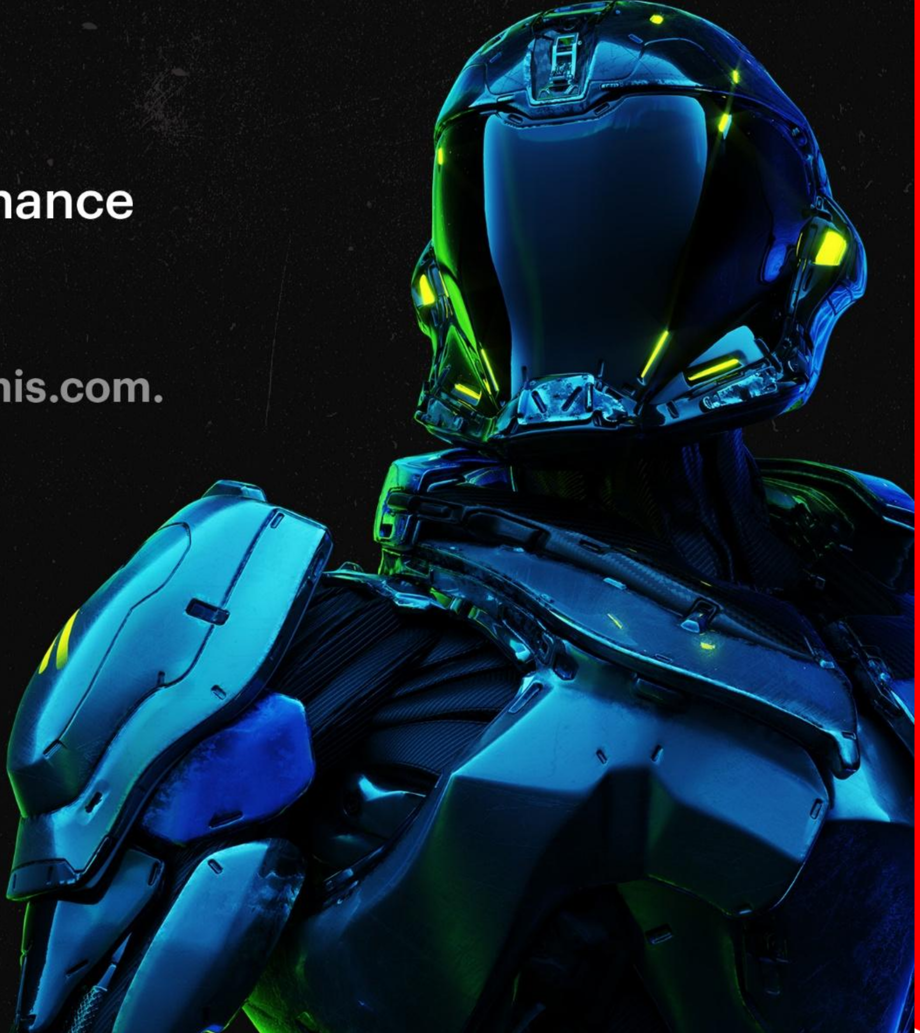


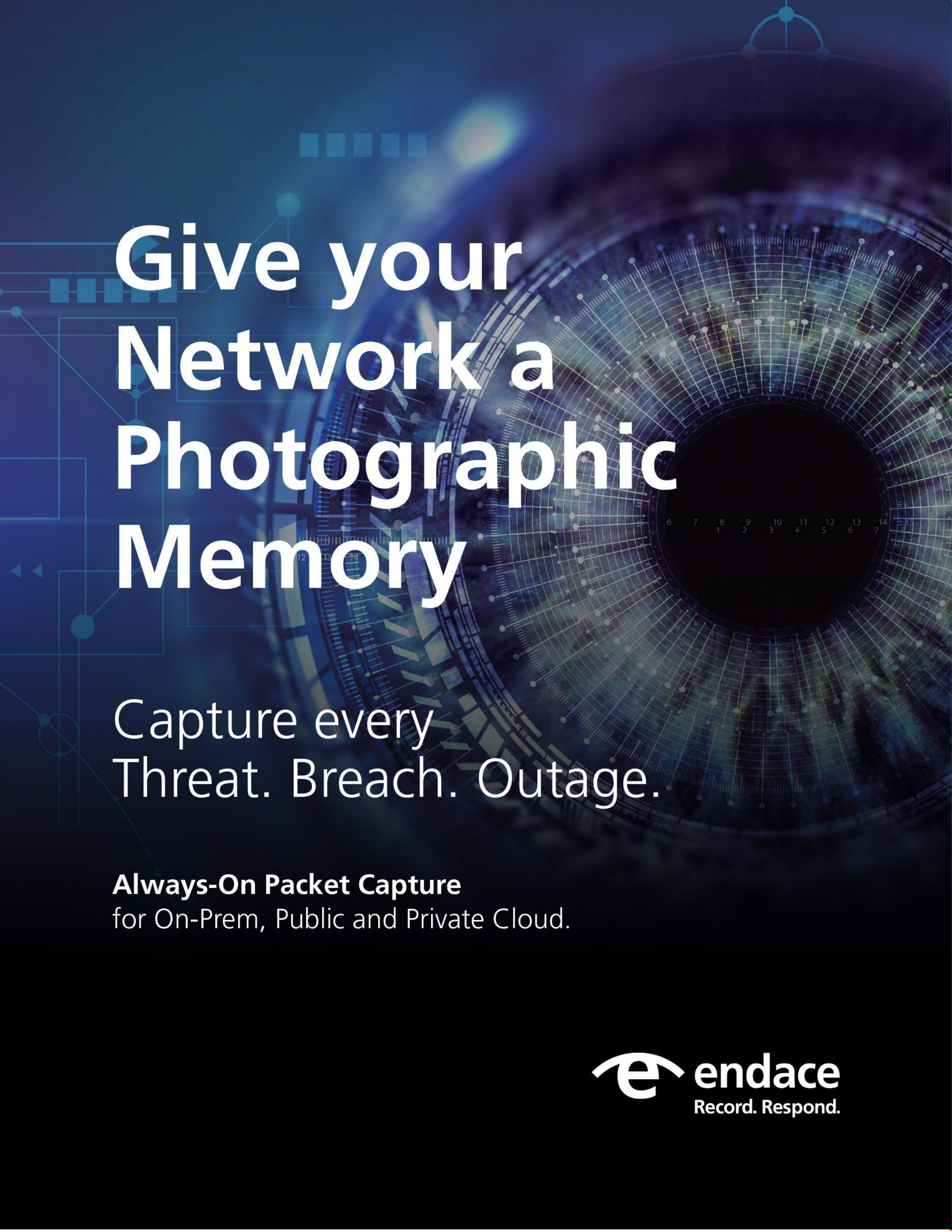
Want to know more? www.jerichosecurity.com

Voice
Email
SMS



125
100
75
50
25
0
14
98
31
49
January
14
98
31
49
February
14
98
31
49
March
● Reported, not failed
● Opened, no action
● Failed and reported
● Failed, not reported




Give your Network a Photographic Memory
Capture every Threat. Breach. Outage.
Always-On Packet Capture
for On-Prem, Public and Private Cloud.
endace
Record. Respond.

JUCY is the Sandbox They Hope You Never Discover

It's time to rethink what's possible!

JUCY Sandbox is the first interactive sandbox to combine dynamic behavioral execution with AI-powered genomic code analysis, running in parallel to catch threats others miss. And unlike traditional sandboxes, JUCY includes hypervisor-based unpacking — invisible to malware and immune to anti-VM evasion.

Developed for the U.S. Intelligence Community and now available for enterprise security teams, JUCY catches new threats designed to evade detection months ahead of other solutions.

Unlike conventional sandboxes that rely primarily on surface-level indicators, JUCY performs deep bytecode analysis to identify malicious code regardless of obfuscation techniques. This groundbreaking approach enables security teams to detect sophisticated malware variants, zero-day exploits, and supply chain malicious insertions that traditional tools fail to recognize.

JUCY works by detonating suspicious files in a secure environment while simultaneously conducting genomic code analysis at multiple levels. The system maps the genetic structure of malicious code, allowing it to identify related malware families even when they've been substantially modified. This function-level detection maintains effectiveness against adversaries who regularly recompile or disguise their code.

Operating at the hypervisor level, JUCY remains invisible to malware, effectively defeating sandbox-aware threats that attempt to evade analysis. The platform's comprehensive memory scanning capabilities also enable it to detect fileless malware and sophisticated memory-resident implants that never write to disk.

JUCY sandbox

www.unknowncyber.com

Application Security, **Reality check.**

Breaking some **myths** about application security

The myth of **simplicity**

Any integration of an open-source library introduces more than 70 additional sub-dependencies.

The myth of **sound analysis**

The application layer is beyond just the code being developed and covered by static scanners, leaving risk valid and unmonitored.

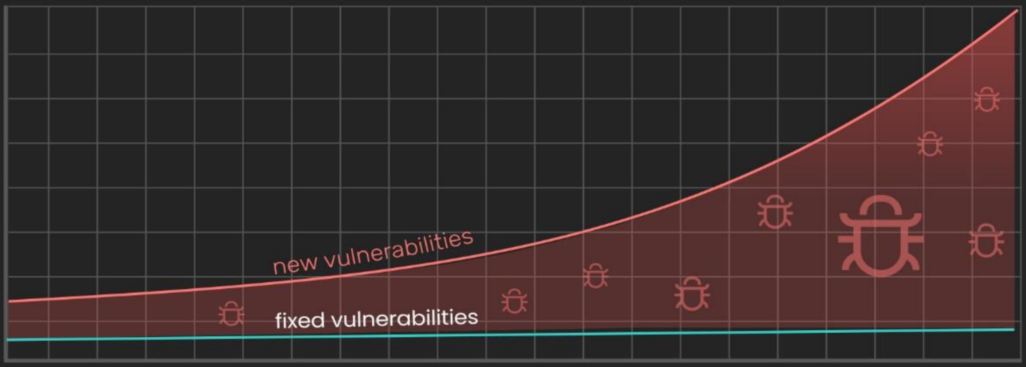
The myth of **accuracy**

Trusting in accuracy without context is a fallacy. More than 90% of alerts are false, generating pure noise.

The myth of **collaboration**

Security tools are never "loved by developers". Engineering appreciates accuracy, thorough research and professionalism.

The **Application Security Gap** is Growing



Vulnerability backlogs explode as code scales, but developers' capacity to fix stagnates— Driven by **a lack of clarity and context** to triage and fix issues

Precious engineering time drained by **manual triaging** and **complex remediation steps**

250 **Developers** x **$150K** **Average annual engineer salary** x **5%** **Time engineers spend on security** = **$1.875M** **Added expense to security**

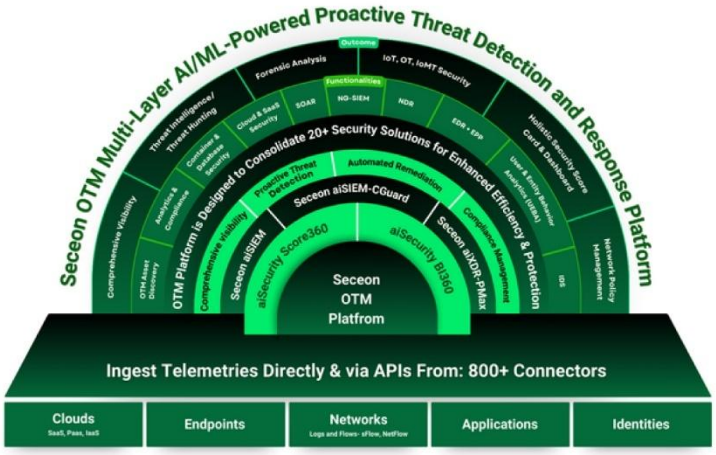
Kodem

Learn more at kodemsecurity.com

Deloitte.
Ready to build resiliency? Scan to get started.

seceon
SECURITY FOR EONS

The Cybersecurity Game Changer


Seceon OTM Multi-Layer AI/ML-Powered Proactive Threat Detection and Response Platform
Outcome
Comprehensive Visibility
Threat Intelligence/ Threat Hunting
Forensic Analysis
IoT, OT, IoMT Security
Holistic Security Score Card & Dashboard
Network Policy Management
Functionalities
OTM Asset Discovery
Analytics & Compliance
Container & Database Security
Cloud & SaaS Security
SOAR
NG-SIEM
NDR
EDR + EPP
User & Entity Behavior Analytics (UEBA)
IDS
OTM Platform is Designed to Consolidate 20+ Security Solutions for Enhanced Efficiency & Protection
Comprehensive visibility
Proactive Threat Detection
Automated Remediation
Compliance Management
Seceon aiSIEM
Seceon aiSIEM-CGuard
Seceon aiXDR-PMax
aiSecurity Score360
aiSecurity BI360
Seceon OTM Platfrom
Ingest Telemetries Directly & via APIs From: 800+ Connectors
Clouds
SaaS, Paas, IaaS
Endpoints
Networks
Logs and Flows- sFlow, NetFlow
Applications
Identities

Five Features That Set Us Apart from the Rest

1. Real-Time Insights Through Flows, Logs, & Identities, (Not Just Logs)

Unlike competitors who rely solely on logs, Seceon harnesses the power of network flows, applications logs, & OS logs & identities. Logs offer a limited, after-the-fact snapshot. Flows provide a complete, real-time picture of network activity, empowering you to detect and respond to threats faster and more effectively.

2. Strategic Placement in the Network

Seceon's solution is strategically positioned to sit beside the network, not in the way. This means:

- Comprehensive visibility of north-south (inbound/outbound) and east-west (lateral) traffic.
- The ability to detect hidden "cross-talk" within your network.
- Faster detection and response—because in cybersecurity, every second counts.

3. Smarter Data Collection and Enrichment

Our collectors are designed for efficiency and precision.

- They extract only the relevant data from packet flows.
- Unnecessary information is discarded, leaving you with enriched, actionable intelligence without the noise.
- This streamlined approach ensures better performance and sharper insights than competitors like Huntress and Arctic Wolf.

4. Competitive, Transparent Pricing

Seceon offers enterprise-grade protection at a price point that scales with your business. No hidden fees, no complicated structures—just straightforward pricing that delivers unbeatable ROI.

5. Flexible, Agnostic Connectors

Our platform is built for compatibility:

- Seceon works seamlessly with any environment, no matter the vendor or system.
- Need a new connector? We're known for going above and beyond to integrate with even the most unique setups.

Why Choose Seceon?

Seceon is designed to outpace the competition, offering comprehensive visibility, proactive threat detection, automated remediation & continuous compliance, and flexible integration—all at the lowest TCO saving end-customers more than 40% of the cost for a comparable solution.

Others talk about the platform approach and still come up with multiple kludged together products that lack the common content& situational awareness. Which are easily bypassed by threat actors.

Take Action Now:

Ready to experience the difference?
Let us show you how Seceon redefines cybersecurity:

Visit *www.seceon.com*
Schedule a Demo Today!

Company HQ:
Westford, MA

Contact Us:
https://seceon.com/contact-us/

WWW.GMSECTEC.COM

OFFERING SERVICES

CLIENTS IN OVER
50 COUNTRIES

GROWING

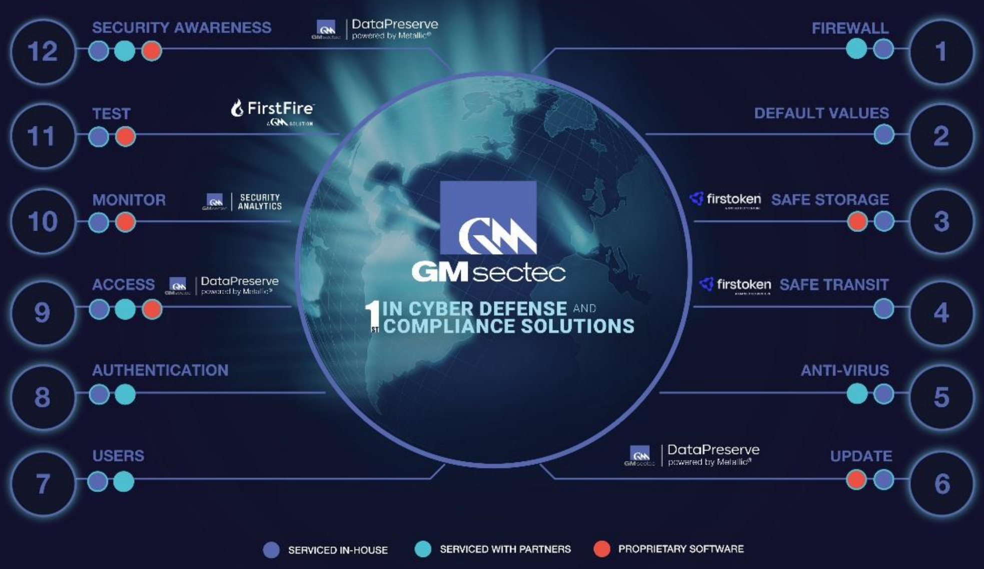
WITH MORE THAN
3 THOUSAND
SECURITY PROFESSIONALS

GLOBAL PRESENCE

OVER
50 THOUSAND
CLIENTS ENROLLED

STRATEGIC ALLIANCE

WITH PR SCIENCE,
TECHNOLOGY AND RESEARCH
TRUST & POLYTECHNIC
UNIVERSITY OF PR



GM sectec

1st IN CYBER DEFENSE AND COMPLIANCE SOLUTIONS

			SERVICED IN-HOUSE	SERVICED WITH PARTNERS	PROPRIETARY SOFTWARE
1	FIREWALL		●	●	
2	DEFAULT VALUES		●		
3	SAFE STORAGE	firstoken	●		●
4	SAFE TRANSIT	firstoken	●		
5	ANTI-VIRUS		●	●	
6	UPDATE	DataPreserve powered by Metallic®	●		●
7	USERS		●	●	
8	AUTHENTICATION		●	●	
9	ACCESS	DataPreserve powered by Metallic®	●	●	●
10	MONITOR	SECURITY ANALYTICS	●		●
11	TEST	FirstFire	●		●
12	SECURITY AWARENESS	DataPreserve powered by Metallic®	●	●	●

● SERVICED IN-HOUSE ● SERVICED WITH PARTNERS ● PROPRIETARY SOFTWARE

PREFERRED PARTNER

VISA | GM sectec

PCI APPROVED SCANNING VENDOR

PCI QUALIFIED SECURITY ASSESSOR

PCI P2PE - QUALIFIED SECURITY ASSESSOR

PCI 3DS ASSESSOR

PCI PA-DSS QUALIFIED SECURITY ASSESSOR

PCI QUALIFIED PIN ASSESSOR

UL LISTED

FIRST

SAN JUAN
PANAMA CITY
FT. LAUDERDALE
MEXICO CITY
SAO PAULO
SANTIAGO
BOGOTA
MADRID
MELBOURNE

ARTICLES

From Firefighting to Future-Proof: How AI is Revolutionizing Incident Management

By Tannu Jiwnani, Senior Security Engineer

Did you know the average cost of IT downtime is over $5,000 per minute?

Despite this staggering figure, many organizations still rely on humans to sift through alerts at 3 a.m. Imagine a world where systems could detect and fix issues *before* you even knew there was a problem. That world is no longer a distant future — it's rapidly becoming reality.

Source: Unity Connect – The Cost of IT Downtime

The Problem: Manual, Reactive, and Stressful

Picture this: It's 3 a.m. A critical system fails. Phones light up, dashboards flash, and people scramble into action. It's not passion, it's panic. You've got alert fatigue, human bottlenecks, and teams trying to untangle chaos with no sleep. Sounds familiar?

Our tech has evolved — from cloud computing to microservices — but incident management often remains stuck in the past: manual, reactive, and high-pressure. The result? Downtime, stress, and missed opportunities to innovate.

The Shift: From Reaction to Proactive Resolution

Here's the good news: we're at the cusp of a powerful transformation. AI and automation are reshaping how we handle incidents. These systems don't just alert you — they learn, adapt, and even act on your behalf.

We're moving from a world of *reaction* to one of *prediction and prevention*. With AI, systems can spot early signs of trouble, cut through alert noise, and sometimes even resolve the issue automatically — often before anyone even notices.

How AI Transforms Incident Management

1. Smarter Triage: From Alert Overload to Actionable Insight

In today's complex IT environments, incident triage can feel like chaos. Picture an emergency room without a triage nurse pouring in patients, alarms sounding, and no clear sense of priority. That's what traditional IT incident management often looks like: hundreds, sometimes thousands, of alerts flooding in every day. Most are noise. Some are critical. All demand attention. And it's up to overworked analysts to figure out what matters, who should respond, and how urgently — often in the heat of the moment.

This process isn't just inefficient — it's risky. When human teams are responsible for manually filtering, prioritizing, and routing every alert, mistakes happen. Critical issues can be missed. Minor ones can consume hours of valuable time. And when every second counts, that delay can mean the difference between a minor blip and a major outage. That's where AI transforms the game.

AI-driven triage acts as an intelligent filter between the deluge of alerts and your human teams. It uses machine learning models trained on historical incident data, system dependencies, threat intelligence, and real-time metrics to automatically:

- **Classify alerts** by severity, urgency, and impact
- **Correlate related events** into a single incident to reduce noise
- **Identify the right owners** based on team roles, past resolutions, and domain expertise
- **Prioritize response** based on business impact, risk level, and operational context

Instead of a human staring at a wall of red alerts, AI enables an automated, prioritized queue — clean, contextual, and actionable. Now, teams don't have to wonder which incident to tackle first. They can see, in real time, what matters most and where to focus their energy.

Credential Leak Incident:

Imagine your credentials leak online. AI systems can instantly classify the threat as high priority, assign it to the right security team, and even factor in whether the credentials affect admin accounts or critical systems. The result? Faster response, less confusion, and more control.

2. Automated Resolution: Digital First Responders

When incidents strike, every second matters. Whether it's a server crash, a data breach, or a misconfigured application, the clock starts ticking the moment something goes wrong. The longer it takes to resolve the issue, the greater the risk — to uptime, to security, to customer trust, and to the business itself.

Traditionally, incident resolution has relied heavily on human responders. Engineers receive the alert, investigate the issue, search for root causes, and manually execute a fix. While this approach can be effective, it's also slow, inconsistent, and prone to error — especially in high-pressure, high-volume environments. Now imagine if you had a team of digital first responders — tireless, precise, and available 24/7 — ready to leap into action the moment something goes wrong.

That's exactly what AI-powered automation delivers. Modern AI systems don't stop at alerting teams about an issue. They *act*. Using pre-approved automation playbooks, AI can trigger workflows that resolve incidents in real time, often before a human even opens a ticket.

These playbooks are defined ahead of time by your teams, so the response logic is both customizable and safe. AI simply executes the plan — fast, repeatable, and error-free. Common automated actions might include:

- Restarting crashed services or containers
- Scaling infrastructure to handle load spikes
- Applying known patches or rolling back faulty deployments
- Revoking leaked credentials and forcing password resets
- Reconfiguring firewalls or isolating affected systems
- Escalating unresolved issues to human teams, with all the context included

Let's return to our credential leak scenario. Traditionally, this would trigger a chain of manual steps: detect the leak, confirm the threat, inform the security team, revoke access, reset passwords, and notify stakeholders. Depending on when the alert is spotted, this process could take hours — during which the attacker could already be inside your systems.

But with AI-powered resolution, the entire flow is automated:

1. **Detection**: AI spots compromised credentials in dark web monitoring feeds.
2. **Trigger**: A predefined playbook activates instantly — no human needed.
3. **Action**: The AI system revokes access for the affected accounts, initiates a forced password reset, and updates access policies.
4. **Notification**: The security team is alerted with a full summary of what occurred, what was done, and what remains to be reviewed.
5. **Audit**: Every step is logged, creating a transparent trail for compliance and analysis.

What used to be a fire drill becomes a smooth, silent operation — swift, secure, and self-healing

3. Always-On Detection: No Blinking, No Breaks

Humans are amazing — but let's face it, we have limits. We need rest, we get distracted, and even the most seasoned analyst can miss subtle signs buried deep in a mountain of logs. Systems, however, don't sleep. And with AI, they don't just *watch* — they *learn*. That's the power of always-on detection.

AI-powered monitoring tools don't just passively collect data. They actively learn what "normal" looks like across your entire environment — from network traffic patterns to login behaviors, system performance baselines, and application usage trends. This means when something *deviates* — even slightly — AI takes notice.

From Static Rules to Dynamic Awareness

Traditional monitoring often relies on static thresholds: If X exceeds Y, trigger an alert. But in today's dynamic, cloud-native, hybrid environments, those fixed rules fall short. What's "normal" for one application on a Monday morning might be a red flag on a Sunday night.

AI changes the paradigm by applying behavioral analytics and anomaly detection in real time. It continuously adapts, evolving its understanding of your systems and users, and flagging anything that doesn't align with established patterns. It doesn't just detect what's *wrong* — it notices what's *different*, and in cybersecurity and operations, that distinction can make all the difference.

Example: Spotting the Pattern Before It Becomes a Problem

Let's revisit our compromised credentials scenario. Suppose one employee's login credentials appear on a dark web forum — a clear warning sign. AI spots it, classifies the alert as high-risk, and the incident is handled.

But what if that wasn't an isolated case?

A few hours later, the second employee's credentials are leaked. Then a third. A human analyst might treat each incident as separate. But an AI system sees the trend. It connects the dots in real time — multiple accounts, similar patterns, shared department, overlapping access privileges. It recognizes the emerging threat: a targeted credential-stuffing attack or an internal system breach.

Instead of reacting to incident by incident, AI detects the pattern and escalates the event. Now, your security team isn't just responding to leaks — they're preventing a coordinated breach.

The Benefits: Speed, Trust, and Healthier Teams

AI doesn't just make incident response faster — it makes it smarter and more sustainable:

- **Reduced MTTR (Mean Time to Resolution):** Issues are solved before they impact your business.
- **Improved reliability:** Customers see a resilient system they can trust.
- **More time for innovation:** Your teams are freed from repetitive tasks and can focus on building what's next.
- **Less burnout:** Automation offloads stress, creating healthier, more empowered IT teams.

What About the Risks?

Like any tool, AI isn't perfect. And responsible implementation matters.

1. Lack of Oversight: Automation Without Guardrails

AI can act in milliseconds — which is great for speed, but risky when something goes wrong. A misconfigured playbook or a wrongly classified incident could trigger automated actions that cause more harm than good: shutting down the wrong system, escalating a false positive, or missing a critical alert.

The fix? Always include human-in-the-loop checkpoints for sensitive actions. Build safety nets into your workflows and ensure there's clear accountability for every automated step. Let AI handle the speed — but let humans guide the direction.

2. Bias in AI Algorithms: Garbage In, Garbage Out

AI learns from data — and data isn't always neutral. If your training data is biased, outdated, or incomplete, your AI will inherit those flaws. That could mean prioritizing the wrong alerts, underestimating certain risks, or ignoring edge cases that don't fit historical patterns.

The fix? Prioritize data diversity and quality. Regularly audit the datasets and decision patterns your AI is using. Engage cross-functional teams to evaluate fairness and equity in how AI makes decisions. Think of it like tuning an engine — the better the fuel, the better the performance.

3. Loss of Transparency: The Black Box Problem

One of the biggest concerns with AI is explainability. If your system flags an incident or takes automated action, your team needs to understand *why*. When decisions are made inside a "black box," trust erodes — especially in high-stakes situations.

The fix? Design for transparency. Choose AI platforms that offer audit trails, decision logs, and explainable outputs. Make it easy for your team to trace an action back to its source. Clear visibility builds trust — and helps humans learn from AI, not just follow it blindly.

4. Over-Reliance on Automation: Losing the Human Edge

AI is incredibly powerful — but it can't replace human intuition, creativity, or critical thinking. The risk is that teams become too dependent on automation, ignoring red flags or failing to step in when something doesn't feel right.

The fix? Strike the right balance. Use AI to handle the repetitive, the routine, and the time-sensitive — but always reserve space for human judgment in complex, nuanced, or strategic decisions. Encourage your team to stay engaged, question the system, and continuously improve it.

AI and the Human Element: Amplifying, Not Replacing

It's one of the most common concerns whenever AI enters the conversation:

"Is this going to take my job?"

The fear is understandable — and in some industries, not unfounded. But when it comes to incident management and IT operations, the truth is far more empowering:

AI isn't here to replace humans. It's here to elevate them.

AI Takes the Noise — You Take the Lead

Modern incident response is noisy. Endless alerts, blinking dashboards, and triage tasks create constant pressure and fatigue. It's no wonder teams feel overwhelmed, burned out, or stuck in a reactive loop.

Here's where AI shines it absorbs the noise. It filters the false positives, classifies the alerts, automates the handoffs, and even resolves the repetitive issues. It acts as your first digital responder fast, focused, and tireless.

The result? You're free to do the work that matters. The work machines can't do. The work that drives innovation builds trust and moves your business forward.

Humans Bring What Machines Can't

AI can crunch data and spot patterns, but it doesn't understand *why* something matters. It can triage an alert, but it can't have a conversation with a stressed-out client, reassure a team during a crisis, or weigh the trade-offs of a complex business decision.

That's where human strengths come in — and they're irreplaceable:

- **Empathy** helps you understand how an outage impacts people, not just systems.
- **Creativity** leads to new approaches, better solutions, and smarter architectures.

- **Critical thinking** allows you to assess risk, adapt to uncertainty, and make judgment calls when the path isn't clear.

AI can help get you to the moment that matters — but what happens next? That's all you.

Final Thought: Building a Future That Works for Us

The future of incident response isn't about robots replacing people. It's about **building intelligent systems that support people** — systems that lighten the load, reduce the noise, and allow humans to focus on what they do best. This shift isn't just technical — it's cultural. It marks a move away from reactive firefighting toward proactive resilience. From burnout-inducing chaos to calm, confident control. From endless triage to purposeful innovation.

AI doesn't take away the human element — it **amplifies it**. It turns stress into strategy. Disruption into insight. And downtime into opportunity.

By designing systems that anticipate issues before they escalate, that automate the repetitive while elevating the essential, we create more than operational efficiency — **we create space**. Space for recovery. Space for innovation. Space to lead, rather than chase.

Because in the end, the goal isn't to remove the human touch —

It's to make it matter more than ever.

About the Author

Tannu Jiwnani is a cybersecurity professional with expertise in incident response, threat detection, and managing global threat actors at a leading software company. She is passionate about creative problem-solving and continuous learning. Tannu advocates for diversity and inclusion in tech, inspiring individuals from all backgrounds to bring fresh perspectives to cybersecurity. Beyond her technical achievements, she actively mentors and supports the community, sharing knowledge to empower others in the cybersecurity field. Her dedication embodies a commitment to building both resilient systems and inclusive professional environments.Tannu reached online at ragsd8@gmail.com

Security Awareness Programs Are Failing - Here’s What Actually Works

Learn why security awareness alone fails to prevent human error and how technical controls, and strong security culture can reduce risk.

By Koby Zvirsh, Cyber Security Consultant, Sygnia

Every year, statistics are published on the top root causes of cyber breaches. The human element is notoriously present in one of the top places. It’s no surprise, then, that a fair share of effort goes to security awareness activities. Yet, despite these initiatives, the trend is not changing dramatically, and human errors continue to occur, often leading to major incidents, such as compromised credentials and infected machines.

In the security world, it is common to hear that users are the weakest link in the security chain (raise your hand if this phrase showed up in your recent awareness training). Such statements shift the focus away from technology and onto people, suggesting that people are the problem. But the issue isn’t just that users make mistakes - it’s that many organizations fail to take a holistic approach that integrates technical controls, security-by-design principles and effective training, which actually change behavior. Without it, companies leave major gaps in their defense strategy.

Why Security Awareness Training Fails

While security awareness training is considered common practice in many organizations, these programs often **serve compliance purposes rather than driving real behavioral change**. Employees sit through annual, outdated training that feels like a corporate obligation rather than something practical. Instead of embedding security into daily operations, organizations overwhelm employees with generic recommendations that are quickly forgotten. Since the goal is often to pass a mandatory quiz rather than adopting security concepts, the lessons rarely lead to meaningful behavioral change.

Another reason awareness programs fail is that they teach users to spot warning signs like misspellings, suspicious links, and urgent requests. While this has some benefits, **modern attacks have become more sophisticated.** As observed in our latest Field Report, there is increasing use of generative AI tools to make scam messages more convincing. Relying on users to detect every threat is not an effective strategy.

Beyond outdated training methods, security can be perceived as a set of guidelines rather than an enforceable process. For example, employees are told not to reuse passwords, but without implementing systems like password managers that can help the users, or enforcing policies, these recommendations can be easily ignored. When security behaviors aren't built into daily operations, employees view them as suggestions rather than requirements.

In some cases, employees don't see security as part of their job. **Many believe cybersecurity is the IT or security team's responsibility, not theirs**. Without clear incentives or a "What's in it for me?" mindset, security best practices often lose to convenience. Employees will prioritize getting their work done as quickly as possible, sometimes at the cost of taking shortcuts like sharing passwords or bypassing security controls. If security feels like a burden rather than a natural part of work, people will tend to choose the path of least resistance.

Given these challenges, it's clear that traditional awareness training alone is not enough. Human mistakes are inevitable, and security efforts must **shift from simply 'educating' users to reducing opportunities for errors** through well-designed technical controls.

Mitigating User Mistakes with Technology

People don't always make the same decisions throughout the day - distractions, fatigue, and urgency all impact judgment. That's why even the most comprehensive security awareness program is not enough. Organizations need built-in security mechanisms that not only help users avoid mistakes but also provide fail-safes when they happen.

In every awareness program there are fundamental themes that always repeat themselves - passwords and emails. Users are told to choose strong passwords, long, with symbols and digits, and we want them to change them every couple of months. Many times, users also have more than one password. This is the point where reusing credentials, storing them insecurely, or choosing weak variations comes into play. This creates a direct path to identity compromise. In order to avoid that, security teams can implement multiple tools that are able to help. For example, enforcing Single Sign-On (SSO) ensures users only need one set of credentials for all company applications. For cases where multiple passwords are still necessary, organizations should provide **password manager** solutions. Avoid the chase of which passwords are considered strong enough by implementing **passwordless solutions**, such as FIDO2 keys, that also provide phishing-resistant protection.

Another common focus in awareness training is email security, particularly phishing risks. Eliminating URLs from emails isn’t realistic, and users will inevitably click links. Instead of expecting users to identify every phishing attempt, organizations should implement automated security controls that reduce the risk before a mistake happens. **URL scanning** solutions can inspect links before a user clicks, blocking access to known malicious sites. If a user does click a suspicious link, browser isolation can contain the threat by opening the link in a secure virtualized environment, or to prevent the user from entering information into text fields - depending on the arsenal of controls.

File and application handling is another common concern, especially when end users require administrative permissions. Same as before, preventing attachments in emails or file downloads completely is not realistic for the vast majority of the organizations. Nevertheless, this risk can be mitigated by fail-safe controls - such as **application allowlisting**, which ensures only approved applications are allowed to run. Elevated permissions can be granted temporarily using a Just-in-time solution, or by utilizing an Endpoint Privilege Management tool that **elevates permissions to specific process or application**. These controls allow security teams to provide solutions that support business requirements, but in a secure manner.

Setting applications with secure default configurations can be an effective method to prevent mistakes before they happen. For example, sharing settings in collaboration platforms often provide capabilities to restrict the sharing of data with external parties. Organizations that require this capability can choose to allow external sharing but set the default option to internal users, to minimize mistakes that might lead to data leakage. This approach is another way that companies can adopt to integrate security into business processes from the start.

At the same time, security must also be practical. If security controls are too rigid, users will bypass them. For example, when employees need new software, a complex or frustrating approval process will push them to find their own solutions, creating Shadow IT instances across the organization. When you inflate a balloon too much, at some point it bursts. Similarly, when security controls are too restrictive, users may ‘break out’ and find ways to circumvent them.

Security teams should evaluate how to enforce security standards that minimize opportunities for mistakes. By combining technical controls with usability, organizations can significantly reduce human error while ensuring security does not become a barrier to productivity.

Creating a Positive Security Culture

Technology plays a critical role in minimizing users' mistakes, but security awareness and technical controls alone are not enough. This is where security culture comes into play. A strong security culture ensures that security isn’t just a set of rules - it becomes part of how employees work and behave.

Security culture is not established through one-time training. It requires ongoing maintenance and a deep understanding of how employees perceive security. If employees see security as a compliance requirement rather than a shared responsibility, they won't prioritize it. Organizations should regularly assess their security culture - gathering feedback on policies, identifying knowledge gaps, and understanding how employees feel about the security team. With this information, organizations can tailor security initiatives to address focus areas raised from the field.

Making security a **natural part of workplace norms is key to changing behavior**. There are several methods this can be achieved. A **no-blame policy** ensures that employees feel comfortable reporting incidents rather than hiding them out of fear of consequences. Employees are more likely to follow security practices if they see their colleagues doing the same, and encouraging employees to report suspicious activity or admit mistakes without fear of punishment helps create an environment where security is proactive rather than reactive. In addition, making security relevant to employees' daily lives, such as safeguarding personal devices, banking accounts, and social media, fosters a stronger connection to workplace security practices. With that, it is more likely that employees will follow the same principles at work.

Security teams should also be seen as enablers, not blockers. Security should support employees in doing their jobs safely, rather than making their work harder. Meeting with different business stakeholders to align security with operational needs helps remove unnecessary roadblocks. A security team that collaborates rather than dictates is more likely to be embraced by the organization. Employees should have easy ways to ask security-related questions without hesitation. One way to achieve this could be through Slack or Teams "Ask Me" security channels. These can provide a place for an open, less formal space where employees can get security guidance and help. Instead of being the "Department of No," security teams should embed security into business processes in a way that minimizes friction while maintaining strong protections.

That said, security culture efforts must be supported by the leadership. If executives and managers don't take security seriously, employees won't either. Leadership should communicate the importance of security and actively support security initiatives. When security is prioritized at all levels of the organization, it becomes a shared responsibility.

A strong security culture doesn't happen overnight. It takes continuous work, alignment with business needs, and a commitment to making security both accessible and beneficial. Prioritizing low-hanging fruit can generate quick, visible wins that signal a positive shift. This will allow you to set the stage for some more complex initiatives, while presenting a momentum force as part of a bigger plan where security is considered a partner and not a blocker.

Conclusion

The key to reducing human error is not just preventing mistakes but creating an environment where mistakes are less impactful and harder to make. A strong security posture is achieved by integrating security into daily operations, rather than relying solely on user awareness.

Technical controls must be at the core of security efforts - modern authentication, access controls and endpoint protections provide a strong defense that doesn't rely on users making the right decisions every time. Without these controls, supported by a strong security culture, even the best security awareness programs will fall short.

To sum up, in order to strengthen security posture, organizations should:

- Survey employees on security practices to understand their perceptions, identify pain points, and improve engagement.
- Assess the current security posture by evaluating controls that complement user behavior, such as SSO, Password managers, Application allowlisting, and advanced email scanning.
- Implement phishing-resistant authentication (e.g., passwordless logins, FIDO2 keys).
- Foster a no-blame policy and provide approachable security knowledge through channels like "Ask Me" security chats, Lunch & Learns, and roundtables.
- Leverage leadership influence to promote secure behaviors.

At the end of the day, security isn't just about stopping mistakes - it's about ensuring that when they happen, they don't lead to disaster.

About the Author

Koby Zvirsh is a Cyber Security Consultant at Sygnia. He is an Information Security expert with over 15 years of experience in startups and global enterprises. Koby holds an extensive background in multiple disciplines such as: Security Management, Product Security, Cloud Security, Project Management, Risk Management, Privacy, Compliance Audits, Modern Workforce, Endpoint Security, Incident Response, Resiliency, Zero TrustFirst. Koby can be reached online at LinkedIn

Quantum-Resilient AI Security: Defending National Critical Infrastructure in a Post-Quantum Era

Why CISOs Must Urgently Prepare for the Collision of AI-driven Threats and Quantum Decryption Risks

By Ankit Gupta, Cybersecurity Leader and Researcher, SecureAzCloud.com

In the next five to seven years, the cybersecurity landscape is expected to undergo a radical transformation, driven by the simultaneous evolution of quantum computing and adversarial artificial intelligence (AI). While each on its own presents serious risks, their convergence poses a critical threat to the security of national critical infrastructure (NCI).

Chief Information Security Officers (CISOs) face a narrowing window to act. Without immediate and strategic preparation, the systems powering our economies, healthcare, transportation, energy, and defense could become vulnerable to catastrophic breaches that surpass anything we've encountered to date.

This article presents a deep dive into these looming challenges and provides practical, urgent recommendations for cybersecurity leadership tasked with safeguarding the lifeblood of modern civilization.

Quantum Computing: The Ultimate Cryptographic Threat

Quantum computers, once the domain of theoretical physics, are moving closer to breaking real-world cryptography. The estimated timeline to achieve a "cryptographically relevant quantum computer" (CRQC) — one capable of shattering widely used public-key algorithms like RSA-2048 and ECC — is shrinking rapidly. Some experts place this milestone within the next decade, with aggressive nation-state programs aiming for even earlier breakthroughs.

When that moment arrives, adversaries could retroactively decrypt vast stores of captured encrypted data (a phenomenon known as "harvest now, decrypt later") — including classified government communications, healthcare records, financial transactions, and grid control systems.

NIST's Post-Quantum Cryptography (PQC) project has proactively selected four algorithms for standardization, including CRYSTALS-Kyber and CRYSTALS-Dilithium, urging organizations to begin migration planning immediately. Yet industry surveys reveal that fewer than 20% of critical infrastructure operators have even initiated quantum-readiness efforts.

This lack of urgency could soon prove devastating.

AI-Powered Attacks: The Silent Saboteur

Simultaneously, AI is revolutionizing the offensive playbook for cyber adversaries. Sophisticated AI models are being weaponized to automate social engineering, malware generation, vulnerability discovery, and lateral movement inside complex networks.

Key AI-driven threats include:

- **Automated Reconnaissance:** AI can analyze vast attack surfaces to identify the weakest entry points across thousands of assets in seconds.
- **Deepfake Social Engineering:** Convincing voice or video deepfakes could manipulate employees controlling critical systems.
- **Self-Adapting Malware:** AI-enabled malware can autonomously change its code to evade detection by traditional antivirus and endpoint detection solutions.
- **Faster Exploitation of Zero-Days:** AI models can detect and weaponize software flaws faster than defenders can patch them.

When combined with quantum decryption capabilities, AI-driven attackers could penetrate, pivot, and disrupt national infrastructure at speeds beyond human response.

Real-World National Security Impact

The national security stakes are immense. Consider the following plausible attack scenarios:

- **Energy Sector:** Quantum-decrypted credentials allow adversaries to infiltrate energy management systems. AI-driven malware disables circuit breakers across the grid, causing blackouts in major cities.
- **Healthcare:** Hospitals' encrypted patient records are retroactively exposed, leading to identity theft, ransomware attacks on life-saving equipment, and mass patient care disruption.
- **Defense:** Defense contractor communications and weapon system blueprints, once considered secure, are decrypted and weaponized against national forces.
- **Finance:** National banking systems face simultaneous AI-driven fraud attacks and retroactive compromise of transaction ledgers, undermining public trust in the financial system.

These aren't abstract risks. U.S. intelligence agencies have repeatedly warned that adversaries are stockpiling stolen encrypted data today for future decryption once quantum capabilities mature.

Preparing for the Collision of Quantum and AI

CISOs and security executives must embrace a proactive, two-pronged defense strategy: quantum resilience and AI-enabled cybersecurity.

1. Accelerate Post-Quantum Cryptography (PQC) Transition

- **Asset Inventory:** Identify systems using vulnerable public-key cryptography.
- **Prioritization:** Focus first on systems protecting critical assets (grid controllers, SCADA systems, hospital networks, defense communication).
- **Crypto-Agility:** Architect systems to support algorithm switching without full system redesign.
- **Vendor Engagement:** Demand roadmaps for PQC support from technology suppliers.

2. Deploy AI for Defensive Advantage

- **AI-based Threat Detection:** Implement behavioral analysis tools leveraging AI to detect anomalies invisible to traditional security systems.
- **AI Red Teaming:** Simulate AI-driven attacks against your own environment to identify blind spots before adversaries do.
- **Real-Time Response Automation:** Develop playbooks where AI assists or triggers automated containment actions when quantum-era attacks are detected.

3. Collaborate for Resilience

- **Sector-wide Intelligence Sharing:** Join sector-specific ISACs (e.g., Energy ISAC, Healthcare ISAC) to exchange threat intelligence and defense techniques.
- **Government Engagement:** Participate in public-private initiatives like CISA’s "Shields Up" program focused on critical infrastructure protection.

- **International Cooperation:** Cyberattacks in a quantum AI era will transcend borders; engage with international cyber defense forums to align threat response.

Case Study: A Quantum-Resilient Pilot in Energy Sector

A major U.S. energy operator, facing quantum readiness concerns, launched a pilot initiative in 2024:

- They mapped cryptographic assets across operational and information technology systems.
- High-priority systems were retrofitted with crypto-agile architectures.
- They conducted a PQC migration simulation under a mock "CRQC breach" scenario.
- AI threat detection was layered across OT networks, focusing on anomaly detection.

Result: The operator achieved a 75% reduction in average threat detection time and completed first-stage PQC upgrades within 12 months — setting a new sector benchmark.

This proactive model must become the new standard.

The Time to Act Is Now

In cybersecurity, timing is everything. CISOs who wait for mature quantum computers or publicized AI-driven mega-breaches will find themselves reacting too late, with catastrophic consequences.

National critical infrastructure must not just be resilient; it must be **quantum-resilient** and **AI-resilient**. Organizations that embrace this paradigm now will not only defend their own operations but will contribute to the broader protection of national sovereignty and global stability.

The quantum-AI era will separate those who are merely compliant from those who are truly secure.

The future belongs to the proactive.

About the Author

Ankit Gupta is a cybersecurity leader specializing in quantum security, AI-driven threat defense, and critical infrastructure protection. With over 15 years of experience, he holds a Master’s in Cybersecurity from NYU and advanced certifications including CISSP, CCSP, and ISSMP. Ankit is the founder of SecureAzCloud.com, a platform dedicated to advancing security practices in the quantum and AI era.

He can be reached via LinkedIn at https://www.linkedin.com/in/ankytgupta and through his website https://secureazcloud.com.

From Firewalls to Families: Why Cyber Resilience Begins at Home

Building cyber awareness in the household lays the foundation for stronger, safer workplaces

By Elcin Biren, Founder & CEO, Swiss Cyber Smart

Playing an innocent-looking mobile game, a 10-year-old girl received a message from a stranger posing as her age. Within minutes, she was requested her parents' work schedule and her school name. Communication features on online platforms are facing growing challenges.

We have educated our teams and strengthened the cloud. What about the majority of families? Operating without a map, vulnerable, stressed, and frankly unprepared for the dangers lurking in daily digital life.

More than 80% of parents say they feel "somewhat to completely overwhelmed" by the responsibility of safeguarding their children online, says the 2024 Family Digital Safety Index. CISOs are becoming more conscious, meanwhile, of the growing attack surface caused by home networks and remote work; yet, thorough plans to spread corporate security awareness to workers' home settings are lacking.

Families Are the New Endpoints in the Blind Spot

Children and parents have become the most unprotected victims in our security system as cyberattacks change.

Deepfakes, artificial intelligence-generated phishing, and algorithmic manipulation now impact more than just governments or businesses: Through games, social media, and messaging apps, they reach into homes. Families don't receive cybersecurity onboarding, unlike staff members: Their education? TikTok. YouTube. Experimentation.

Rising AI Threats to Children: A 2025 Overview

AI's fast development is significantly changing online dangers for kids. Key trends in 2025 show important dangers:

- AI-Generated Child Sexual Abuse Material (CSAM) Proliferation: Synthetic CSAM is surging in volume and realism, with deepfakes blurring the lines between real and fake, re-victimizing survivors, and becoming indistinguishable even for experts.
- Predators using AI chatbots: Mimicking trusted people and realistic fake media to groom and extort children.
- Unmoderated AI interactions: Expose children to harmful ideas, false advice on sensitive issues, and unhealthy relationship attitudes, which may cause social isolation and higher bullying chances.
- Children’s evolving cognition: Makes them particularly susceptible to AI-generated deepfakes and false material used for bullying, harassment, and harmful ideas, amplified by social media algorithms.
- Parental and Teacher AI Illiteracy: A notable lack of artificial intelligence knowledge among parents and teachers makes children more exposed to these changing AI-driven dangers.

Unlike corporate breaches with set procedures, compromised child safety can cause permanent damage ranging from privacy violations to psychological trauma.

What's Missing: Digital Parenting Is Not Parental Control

In much of the world, "cyber safety" still means installing an app or setting screen time limits. While parental controls have a role, this approach is fundamentally flawed and ignores the complexity of today's threat landscape.

The hard truth is that most of parental control software fails to detect sophisticated social engineering attempts because they're designed to block content, not identify manipulation. Cybersecurity isn't just about blocking; it's about teaching. Organizations need to apply the same rigor to family digital safety as they do to corporate security awareness training. This means implementing:

- Digital resilience over restriction: Equipping kids to navigate risks and make smart choices
- Algorithm awareness: Teaching the mechanics of how content finds them and why
- Emotional resilience: Drilling recognition patterns for manipulation that masquerades as friendship
- Prompt literacy: Building competency with AI tools that are increasingly embedded in educational platforms
- Privacy fundamentals: Establishing non-negotiable boundaries for data sharing
- Neuroscience applications: Implementing evidence-based approaches to counter digital addiction and manipulation

The market for family digital safety solutions is increasing, yet these products still focus exclusively on content filtering rather than skill-building. This represents a critical misalignment of resources against actual threats. We need competency development, not just more restrictions.

Make Cyber Resilience a Family Skillset

We teach kids to look both ways before crossing the street. Now we must teach them to pause before clicking, to question before sharing, and to recognize red flags before reacting.

Family cyber resilience must be operationalized through measurable, repeatable protocols:

- Implement family security agreements: Document clear expectations, responsibilities, and consequences
- Conduct regular threat simulations: Run monthly phishing tests adapted for different age groups
- Establish authentication protocols: Deploy verification systems for all external communications
- Perform security co-browsing: Allocate dedicated time to jointly audit children's digital environments
- Document incident response plans: Create step-by-step procedures for common threat scenarios

A comprehensive family security posture requires 8-12 hours of initial setup and 3-4 hours of monthly maintenance. This represents less than 3% of the average family's screen time, a reasonable investment against catastrophic risk.

Practical Digital Safety That Actually Works

Not every solution requires cutting-edge tech or hours of research. In many families, simple, consistent habits are proving more effective than complex software. Here are a few real-world strategies that show how small changes can make a big impact:

- Family Verification Codes: One household set up a low-effort but high-impact system after a close call online. Before anyone shares personal information like a home address they send a family group text asking, “Green Light?” Another family member replies with a pre-agreed phrase that changes monthly. The whole system takes about 15 minutes a month to manage and has already prevented multiple potential breaches. It's quick, it's simple, and it works.

- Monthly Digital Safety Meetups: A group of families started gathering once a month to walk through online safety scenarios together parents and kids included. These casual "cyber circles" help kids recognize red flags in real time. One young gamer recently spotted a suspicious link in a chat and immediately flagged it to an adult, all thanks to what they'd practiced. Peer learning and shared vigilance beat going solo.
- When Kids Teach the Adults: In one school program, IT specialists team up with teachers to lead interactive safety lessons then students go home and teach what they've learned to their families. This "child-as-teacher" model turns out to be highly effective.

These aren't flashy solutions. They're intentional, repeatable, and they deliver real results. Protecting your family online doesn't start with tools it starts with habits.

What Industry Can Do

CISOs, educators, and tech leaders have both a professional obligation and strategic opportunity to extend security beyond corporate perimeters.

The boundary between work and home security has virtually disappeared. Security professionals have dealt with at least one incident where a home device compromised corporate assets, signifying a complete blurring of the lines. Industry leaders must implement:

- Family-inclusive security awareness: Extend training modules to employee households
- BYOD+ policies: Expand device management to include family device security
- School-business partnerships: Allocate 5% of security awareness budgets to educational initiatives
- Age-appropriate resources: Develop targeted materials for each developmental stage
- Board-level reporting: Include family security metrics in overall cyber risk reporting

Addressing these escalating AI threats requires a multi-faceted approach, including:

- Stronger Legal Frameworks: There is a growing urgency to update legal definitions and penalties to effectively address AI-generated CSAM and other AI-facilitated harms.
- Enhanced Detection and Removal Technologies: Developing and deploying advanced AI tools to detect and remove harmful AI-generated content is crucial.
- Increased AI Literacy Education: Educating children, parents, and educators about the benefits and risks of AI, including how to identify and respond to potential threats, is paramount.
- Collaboration and Information Sharing: Increased collaboration between tech companies, law enforcement, child safety organizations, and governments is essential to develop effective prevention and intervention strategies.
- Prioritizing Child Safety in AI Development: Companies developing AI technologies must prioritize the safety and well-being of children in their design and deployment processes.

The cost of implementing family-centric security measures between $250-$300 per employee annually is less than 0.5% of the average cost of a single data breach ($4.45M in 2024 - IBM report). Because every employee is also a parent, a child, or a caregiver, this isn't just a school issue or a tech issue it's a core business risk management imperative.

The Global Education Gap

The stark reality is that worldwide, few governments have truly implemented comprehensive cyber curriculum into their education systems. Success Stories Worth Scaling:

- Estonia’s Digital Competence Framework integrates digital literacy—including cybersecurity and online safety—from the first grade through high school. Aligned with the EU’s DigComp framework, it emphasizes skills like safe communication, critical evaluation of information, and secure use of digital tools.
- Singapore’s Cyber Wellness curriculum is embedded within the national Character and Citizenship Education (CCE) framework. It combines technical digital skills with ethical, emotional, and social considerations. Students learn to evaluate online risks, practice empathy in digital spaces, and develop personal responsibility.
- Qatar is steadily advancing its digital education agenda through the Qatar Digital Learning and Skills Strategy, part of its broader National Vision 2030.

The Race Against Time

We face a critical challenge: the pace of threat evolution versus the pace of protection implementation. While governments debate curriculum standards and funding priorities, children are navigating sophisticated digital threats daily.

The solution isn't waiting for perfect systems, but acting with the tools and knowledge we have now:

- Simultaneous implementation: Education, technology, policy, and community initiatives must progress in parallel, not in sequence
- Public-private partnerships: Companies must share responsibility for creating safer digital ecosystems
- Cross-border cooperation: Cyber threats don't respect national boundaries; our solutions shouldn't either

Summary of Strategic Recommendations

- For organizations: Allocate 5% of security awareness budgets specifically to family digital safety resources.
- For educational institutions: Implement a minimum of 24 hours of digital safety education annually for every grade level.

- For technology companies: Dedicate product development resources to native safety features.
- For governments: Establish baseline digital safety standards that follow the Estonia or Singapore model.
- For families: Apply the same rigor to digital safety planning as you would to physical safety planning.

Cyber Resilience Isn't Optional It's Infrastructure

The consequences of digital threats are personal, emotional, and in some cases, irreversible. Empowering parents is a necessity. When parents are equipped, children are protected. When families are informed, futures are secured.

The most sophisticated security stack in the world means nothing if our children don't know how to protect themselves when technology is in their hands.

Because today Cyber Resilience Saves Lives

Family digital security isn't just another checkbox; it's the foundation of our collective digital future. Let’s shift the conversation from fear and control to education and empowerment.

About the Author

Elçin Biren is a global, award-winning cybersecurity expert and mother of two, with 20 years of experience advising IT leaders, board members, and non-technical decision-makers. She is the founder of SwissCyberSmart and creator of the Cyber Resilience Masterclass for Families, a 10-minute, self-paced training series that empowers parents to protect their children from digital risks and foster safer tech habits at home.

With a background in industrial engineering, ethical hacking, and executive leadership, Elçin brings a uniquely multidimensional lens to today's evolving threat landscape. She has served as a CISO advisor, cyber strategist, and AI ethics advocate, leading global initiatives to align security, compliance, and human impact. As Global Ambassador for the Responsible AI Council and President of the Switzerland Chapter, Elçin helps shape international cybersecurity standards and sits on multiple advisory boards advancing digital safety and resilience.

Named among the "40 Under 40 in Cyber" in 2023 and 2024, she is also a sought-after speaker and lecturer at institutions like IMD and St. Gallen University, and a passionate mentor for women in tech. She has been shortlisted for the Cybersecurity Woman of the Year Awards 2025.

Her mission is clear: to shift the cybersecurity conversation from fear to resilience, from complexity to clarity, and from technical silos to shared responsibility because in today's world, access to cybersecurity is a basic human right.

Elcin can be reached online at elcin@swisscybersmart.com via https://www.linkedin.com/in/elcinbiren/ and at company website www.swisscybersmart.org

You May Be Well-Architected, But Are You Secure?

Lessons from 6 Major Shared Infrastructure Incidents

By Anirban Sengupta, Chief Technology Officer and Senior Vice President of Engineering at Aviatrix

Cloud and network architects often focus on building high-performance, scalable environments in accordance with the “well-architected” frameworks prescribed by their cloud service providers (CSPs). They’re asking, are we following the published best practices to ensure our architecture is secure? But here’s the real question: Is your architecture truly secure, or is there a weakness not yet exposed?

Recent incidents — including Salt Typhoon’s GhostSPIDER malware campaign, Microsoft Azure compromise, and a potential breach at Oracle — underscore a critical lesson: **a well-architected cloud environment does not guarantee security.**

If security isn't designed into the network from the beginning, the very infrastructure that enables business agility can become an attack vector for advanced cyber threats.

By learning from real-world security failures, we can **shift left** in cloud and network security, ensuring organizations are prepared before the next breach—rather than reacting after the damage is done. The following incidents highlight how shared infrastructure compromises can ripple through cloud providers and disrupt entire industries.

Case Studies: When Cloud Providers and Shared Infrastructure Become the Weak Link

1. Oracle Cloud Infrastructure Breach (March 2025)

Oracle recently confirmed that it was investigating unauthorized access to its cloud infrastructure, possibly linked to the same threat actors behind the recent Snowflake-related breaches. A threat actor claims to have exfiltrated approximately 6 million records, potentially affecting over 140,000 tenants. Early reports suggested compromised credentials and the potential for lateral movement within shared services.

Business Impact:

- **Operational Risk:** Organizations utilizing Oracle Cloud services may experience disruptions due to the need for immediate security assessments and remediation efforts.
- **Compliance Risk:** Entities, especially those in regulated sectors, must evaluate their obligations for breach notifications and ensure adherence to data protection regulations.
- **Reputational Risk:** Businesses reliant on Oracle's infrastructure may need to address concerns from stakeholders regarding the security and integrity of their data.
- **Financial Risk:** Companies could incur unplanned expenses related to incident response, forensic investigations, credential rotations, and potential legal actions.

Lesson for Cloud Architects & Ops Teams: Cloud architects and ops teams must maintain visibility and control in shared infrastructure environments to reduce risk. Encrypt all data in transit using customer-managed, high-performance encryption to avoid reliance on cloud provider defaults. Enforce workload-level isolation to contain potential breaches, and apply Zero Trust principles through continuous identity verification and distributed, context-aware security policies.

2. Salt Typhoon's GhostSPIDER Attack (2023-active)

In Salt Typhoon's GhostSPIDER attack, nation-state malware targeted telecom and cloud-edge infrastructure. The attack exploited weak segmentation, misconfigured network interfaces, and unpatched VPN concentrators.

The business impact included service disruptions across industries that depend on ISP backbones and cloud networking. It also caused potential espionage or intellectual property theft from compromised cloud environments. Organizations suffered financial losses from downtime, breach response costs, and regulatory fines.

Business Impact:

- **Operational risk**: Service disruptions across industries that rely on cloud edge and ISP infrastructure.
- **Data security risk**: Lateral movement enabled potential theft of sensitive or regulated data.
- **Financial risk**: Downtime and remediation led to revenue loss and incident response costs.
- **Compliance risk**: Breach events triggered regulatory reporting obligations.

Lesson for Cloud Architects & Ops Teams: Assume the network is compromised—implement high-performance encryption, network segmentation, and real-time visibility to prevent attackers from moving freely.

3. Microsoft Azure Compromise (July 2023)

In this attack, state-sponsored attackers stole an authentication token. The token gave them unauthorized access to Microsoft corporate email accounts, including high-ranking executives.

The attack exposed sensitive corporate data, leading to reputational and financial damage. It raised potential regulatory fines for failing to protect sensitive user data and caused a loss of customer trust and increased scrutiny on cloud provider security.

Business Impact:

- **Strategic risk**: Exposure of sensitive business plans, contracts, or correspondence shared with Microsoft personnel.
- **Reputational risk**: Enterprises were forced to explain their exposure and dependence on Microsoft infrastructure.
- **Compliance risk**: Enterprises had to assess potential breach notification responsibilities under regulations such as GDPR, HIPAA, or SEC rules.

Operational risk: Internal audits, key rotations, and response planning diverted resources from core business operations.

Lesson for Cloud Architects & Ops Teams: Relying on a cloud provider for security is not enough—organizations must enforce strict IAM (Identity and Access Management) policies, monitor for unauthorized access, and implement an independent encryption strategy.

4. CenturyLink Outage (August 2020**)**

The CenturyLink outage was caused by a telecom network misconfiguration. Its blast radius included AWS, Azure, and other cloud providers.

This outage caused massive downtime for businesses dependent on cloud services. The impact included financial losses from disrupted operations and SLA penalties. Because CSPs use telecom or internet service provider (ISP) backbones, the incident highlighted the risks of shared infrastructure.

Business Impact:

- **Operational risk**: Cloud-based applications and services became inaccessible, disrupting workflows and transactions.
- **Financial risk**: Lost revenue due to service downtime, especially in e-commerce, finance, and streaming services.
- **Resiliency risk**: Organizations without multicloud or redundant network designs experienced prolonged outages.

Reputational risk: Service interruptions eroded customer trust and brand reliability.

Lesson for Cloud Architects & Ops Teams: Avoid single points of failure by designing multicloud failovers and redundant network pathways.

5. SolarWinds Supply Chain Attack (December 2020)

This attack was a supply chain compromise through a backdoored software update. It infiltrated Microsoft Azure and other cloud environments, affecting thousands of organizations.

The attack caused widespread security breaches impacting both cloud providers and customers. It increased regulatory scrutiny and security costs for affected organizations and damaged trust in cloud-based supply chains.

Business Impact:

- **Security risk**: Backdoors granted threat actors prolonged access to sensitive systems and data.
- **Compliance and legal risk**: Organizations had to manage breach disclosure, notify affected customers, and respond to regulatory scrutiny.
- **Operational risk**: Patch freezes, monitoring gaps, and resource redirection delayed IT projects.
- **Reputational risk**: Even indirect exposure damaged customer confidence and supplier trust.

Lesson for Cloud Architects & Ops Teams: Security doesn’t stop at your perimeter—third-party dependencies must be continuously monitored, and Zero Trust policies should apply to all vendor access.

6. AWS Route 53 BGP Hijacking (April 2018)

This hijacking was done through border gateway protocol (BGP) manipulation. Attackers redirected AWS DNS traffic to malicious servers, intercepting data.

Through this attack, bad actors stole sensitive business and customer data. They caused service disruptions for companies relying on AWS Route 53 for critical operations and exposed weaknesses in global internet routing security.

Business Impact:

- **Data security risk**: Intercepted DNS traffic potentially exposed credentials, tokens, and private communications.
- **Availability risk**: Routing errors caused downtime and performance degradation for mission-critical apps.
  Reputational risk: Customers were blamed for issues rooted in internet infrastructure.
- **Digital sovereignty risk**: Trust in the global routing system was undermined, requiring additional traffic encryption and path validation controls.

Lesson for Cloud Architects & Ops Teams: Never assume internet routing is secure—encrypt all traffic, even when using private cloud interconnects.

You Built It, But is It Secure?

3 Security Areas to Integrate from the Start

Many organizations assume that cloud security is someone else's problem—whether it's the cloud provider, the security team, or a third-party vendor. But ops teams and cloud or network architects must integrate security into their designs from the beginning, not as an afterthought.

1. Secure Network Segmentation & Microsegmentation

Segmentation and microsegmention are essential because **flat networks are a hacker's playground**. Once inside, attackers like Salt Typhoon can move laterally across workloads undetected. To integrate security early:

- Use network segmentation at the VPC and subnet level to isolate workloads.
- Implement microsegmentation between applications to enforce least-privilege access.
- Design with Zero Trust principles, requiring authentication before network access.

2. High-Performance Encryption Under Your Control

High-performance encryption matters because, as we saw with the GhostSPIDER campaign, **unencrypted network traffic can be exploited** to intercept sensitive data and inject malicious payloads. To integrate security early:

- Implement high-performance encryption to control both the infrastructure and encryption at each hop.
- Use encryption solutions that don't sacrifice speed or visibility.
- Ensure traffic remains encrypted across multicloud environments without relying on third-party ISPs.

3. Real-Time Network Visibility & Anomaly Detection

Most security incidents go undetected until it's too late. The SolarWinds attack remained **undiscovered for months**, allowing attackers free access. To keep your network secure:

- Implement real-time traffic monitoring to detect anomalies before they escalate.
- Use AI-driven security analytics to spot suspicious behavior across cloud workloads.
- Ensure full visibility across hybrid and multicloud environments—a single blind spot can be an entry point.

The Bottom Line: Security is an Architecture Decision

Salt Typhoon, SolarWinds, the Azure compromise, and now potentially the Oracle Cloud breach, all exposed the same reality—even the most well-architected environments can be easily compromised without built-in security.

If your ops team only reacts after an incident, or if your network architects assume security is someone else's responsibility, you're already behind. **You built the infrastructure. Now make sure it's protected.**

Start today by integrating network segmentation, high-performance encryption, and real-time visibility into your cloud and network designs. The next security event shouldn't be your wake-up call—it should be one you were already prepared for.

About the Author

Anirban Sengupta serves as Chief Technology Officer and Senior Vice President of Engineering at Aviatrix, leveraging over three decades of engineering and management expertise. Prior to Aviatrix, he was Senior Director of Engineering at Google, where he led the development and security of Google Kubernetes Engine (GKE) and Anthos. Anirban played a pivotal role in scaling the Anthos business to over $200M in annual recurring revenue and launched the GKE Enterprise offering.

Before his tenure at Google, Anirban was Vice President of Engineering - NSBU at VMware where he expanded the NSX networking and security portfolio, including NSX Edge, Distributed Firewall and NSX Intelligence products. His previous roles include leadership positions at Cisco Systems, Lucent Technologies, and Ascend Communications.

Anirban holds a B.S. degree in Computer Science and Engineering from the Indian Institute of Technology, Kharagpur, India and an M.S. degree in Computer Engineering from Santa Clara University, California.First

Anirban can be reached online on LinkedIn and at our company website https://aviatrix.com/

From AI to Generative AI: The Evolution of Cloud Security Operations

By Ranjan Kathuria, Cloud Security Architect at Rubrik Inc.

Cloud Security plays a crucial role in the field of information security operations, handling much of the heavy lifting needed to protect systems and data. Starting in 2016, the security industry recognized that scaling security operations effectively required the integration of artificial intelligence. This awareness led to the emergence of new AI tools specifically designed for enhancing security operations. While AI has been around in this space for some time, the advancements in Generative AI are revolutionizing the landscape. With these improvements, the future of security operations looks promising and robust thanks to Gen AI.

Why is Artificial Intelligence not new in Cloud Security Operation?

AI's role in security operations is certainly not a recent development but it has been evolving for quite some time. A notable example is the rise of Cloud Security Posture Management (CSPM) tools, which have been actively identifying and addressing security configuration issues in cloud environments for years.

These tools typically function either through an agentless scanning approach for cloud workload scans or a role-based read access for cloud metadata or configuration management scans. To monitor the cloud assets effectively, these tools require the setup of a role or a programmatic user with read-only access to the cloud environment. This access allows the CSPM tools to gather essential cloud metadata and configuration data. By running periodic scans, they feed this information into their rule engines, which analyze the data to produce actionable security findings.

An example of Metadata or Cloud config scan could be an S3 bucket in your AWS account that allows read access to all the objects via a bucket policy, the tool's rule engine will detect this vulnerability. It will produce a finding indicating that there is an S3 bucket with insecure policies allowing unrestricted access to all objects within the bucket. This proactive detection helps organizations immediately address potential security risks and enhance their overall cloud security posture.

Conversely, an example of a workload scan could involve a virtual machine running Ubuntu 22.04, where the CSPM tool executes an agentless scan on that VM.

During scans, these tools can evaluate the configuration of cloud assets. For example, they can determine if an asset is completely exposed to the internet without any IP firewall restrictions, if it is an internet-exposed asset with firewall restrictions, or if it is completely non-internet facing. Based on these assessments, the CSPM tool can then decide the severity of the findings, providing organizations with valuable insights to address potential security vulnerabilities

These tools also allow customers to add custom rules or mark certain findings as false positives based on their specific environment. For instance, imagine you have an AWS account and receive a finding indicating that some snapshots or backups are missing encryption. If you have compensating controls in place, you can configure the tool to recognize this finding as a false positive in your environment. Consequently, future findings of this nature will be flagged as false positives, streamlining the review process and reducing unnecessary alerts. While most CSPM platforms today rely on rule-based suppression or manual exceptions for this purpose, some leading tools are starting to incorporate machine learning to generalize from user feedback and automatically suppress similar findings in the future.

Many leading CSPM tools have incorporated AI/ML for risk prioritization and anomaly detection, but traditional rule-based engines are still common. The depth of AI integration in these tools has increased over time, with GenAI being the most recent and transformative advancement. Their ongoing evolution continues to enhance security practices, making them an integral part of an organization's security strategy.

What’s New and Game Changing: Generative AI & Cloud Security

Generative AI or GenAI is truly changing the game in cloud security operations, making it easier and more intuitive for security teams to work with their tools and data. Imagine you’re a CISO logging into your CSPM tool and, instead of sifting through complicated dashboards, you’re greeted by a friendly chatbot. You simply type, “Show me the users without MFA who have access to my most critical assets.”

Within moments, you get a clear list. This is just one way that security tools are beginning to use large language models to let users ask questions in everyday language, simplifying the process tremendously.

Take AskAI from wiz.io, for example. With this feature, security teams can ask natural questions like, “What are the critical risks for my publicly exposed resources?” The GenAI engine takes these prompts and turns them into complex security queries, returning clear, actionable insights in response. This is especially helpful for security analysts who may not have deep expertise in cloud security; now they can get guidance on what actions to take. For instance, by asking, 'What steps do I need to fix my over-permissive S3 buckets?' they could get instant, practical advice from AskAI.

Another great example of how GenAI is making an impact is with Microsoft Copilot for Security. This tool acts as a virtual assistant for security analysts, helping them sift through mountains of security data, summarize incidents, suggest ways to respond, and even automatically generate scripts for investigations. Imagine how empowering that is!

With GenAI in the mix, security tools are becoming not just more user-friendly but also incredibly powerful. They’re transforming how teams approach cloud security, making it accessible and manageable for everyone involved.

The Road Ahead: GenAI Shaping the Future of Cloud Security

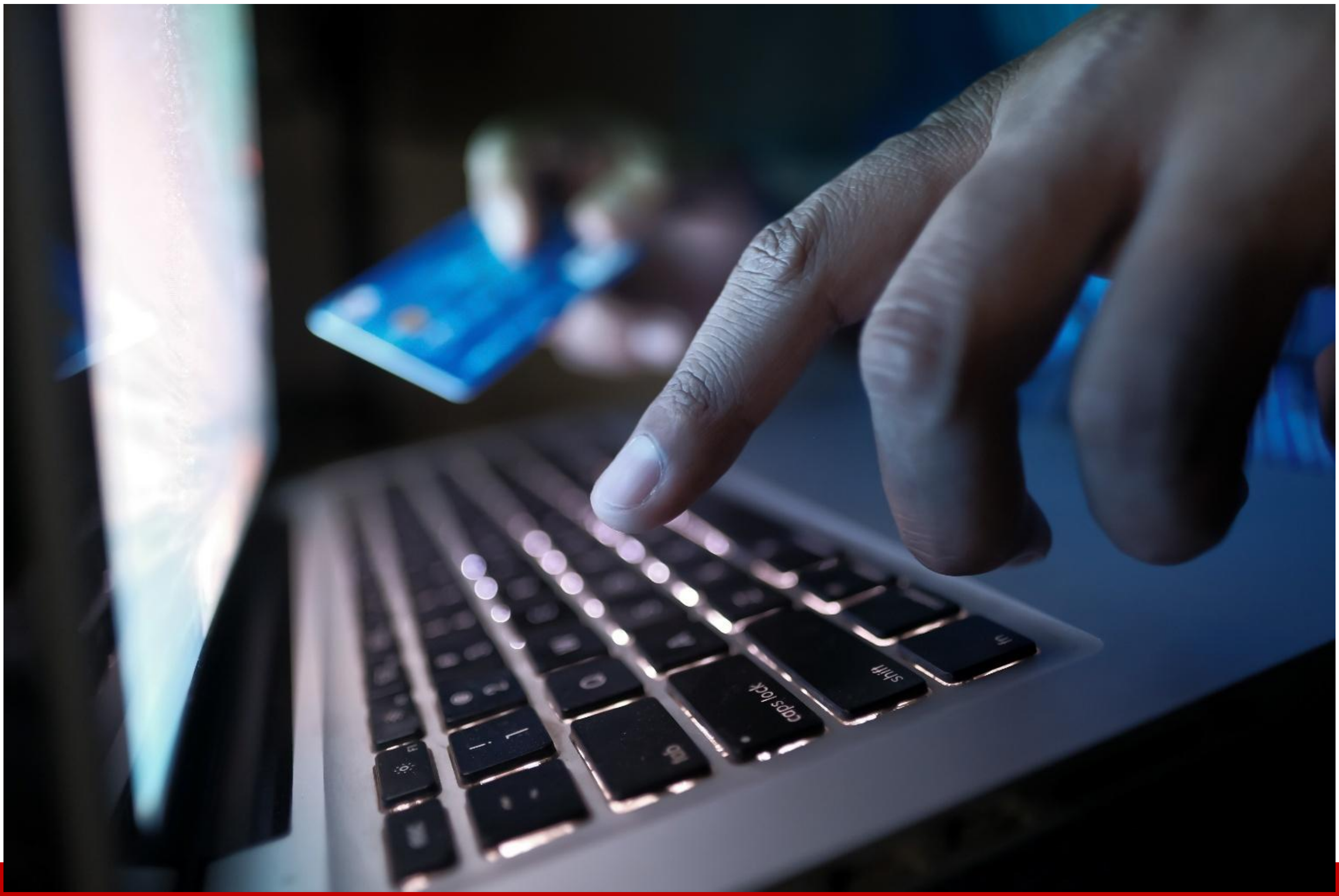
As we look to the future, cloud security operations are about to get a whole lot smarter and more helpful. Today’s security tools already do a great job of spotting issues and even fixing some of them automatically. But what’s coming next is even more exciting.

Soon, with GenAI, cloud security tools will go beyond simply answering your questions or generating scripts. They will be able to create comprehensive, end-to-end security plans tailored to your unique cloud environment by learning from every interaction and continuously analyzing alerts and behaviors. Instead of just reacting to threats or responding to isolated incidents, these systems will proactively assess your entire cloud landscape, identify evolving risks, and recommend or even orchestrate coordinated defenses across all platforms-no matter how complex your setup is. By anticipating vulnerabilities and adapting to new challenges in real time, GenAI-powered tools will help you stay ahead of threats and ensure your cloud infrastructure remains secure from end to end.

In the coming years, we’ll see security operations become more collaborative, with humans and AI working side by side. GenAI will handle the repetitive and complex tasks, freeing up people to focus on strategy and big picture thinking. The future of cloud security isn’t just about automation but it’s about making security smarter, more intuitive, and accessible for everyone.

About the Author

Ranjan Kathuria has over nine years of experience in the security industry, where he has played a key role in developing and mentoring security engineers for recent employers. Currently, he serves as a Cloud Security Architect at a data security company, where his focus is on safeguarding the cloud environment. Additionally, he is recognized as a top-tier security researcher for HubSpot and Quora's Bug Bounty Programs on Bugcrowd, contributing to the enhancement of security measures on these platforms.



A Function-By-Function Guide to Common Fraud Schemes and How to Prevent Them

Strategically Addressing Fraud Risk by Function Can Help Organizations Reduce Risk

By Brian Lafountain, Partner at The Bonadio Group

According to the 2024 Occupational Fraud Report by the Association of Certified Fraud Examiners (ACFE), organizations lose 5% of revenue to fraud each year. Fortunately, the presence of anti-fraud controls is associated with both quicker fraud detection and lower fraud losses.

Fraud schemes can take many different forms depending on the access and opportunities a perpetrator has within the victim organization. Strategically addressing fraud risk by individual function can help organizations implement the necessary controls to prevent a wide variety of common fraud schemes.

Fraud Risks by Function

Cash

Theft of petty cash is one of the most obvious ways that fraud can occur. Installing surveillance cameras in areas where cash is stored can be an effective way to prevent this. Skimming is another common type of cash fraud. Skimming involves pocketing cash before it's recorded in the books. Common controls to prevent skimming include separating the billing and collection function, comparing revenue to inventory values and including outstanding balance reconciliation on invoices to repeat customers.

Payroll

Commonly, payroll schemes include falsifying earnings by overstating hours worked, claiming unearned overtime or increasing wage and salary rates within the payroll system. Detailed reviews of payroll registers and payroll system audit logs can help spot these errors quickly. Creating ghost employees within the payroll system is another type of payroll fraud. To help prevent this, periodically distribute physical payroll checks and regularly review employee data for duplicates. Employees may also commit payroll fraud by falsifying commissions and overstating sales made. Ratio analysis for receivables and bad debt may help uncover this.

Disbursements

The accounts payable (AP) function is very broad and cash disbursement fraud schemes pose a persistent threat to organizations of all sizes. These may involve billing, check tampering, wire transfer and electronic payments, and kickback schemes. The best protection against fraudulent disbursements is segregation of duties across purchasing, receiving and payment functions for any type of disbursement so that no single individual can complete all steps.

Expense Reimbursements

Expense reimbursement schemes fall under the category of fraudulent disbursements but deserve special focus because of the frequency at which they occur. Employees may submit invoices or receipts for reimbursement of personal, extravagant or otherwise inappropriate expenses, overstate expenses, create fictitious expenses or submit duplicate requests for reimbursement. All of these can be prevented by establishing thorough policies and procedures for approving, incurring and substantiating the purpose and timing of business expenses.

Inventory

Company funds aren't the only asset at risk of fraud. Theft of inventory may be concealed by falsified inventory counts, phantom inventory or claiming spoilage or loss. To help prevent fraud in inventory, ensure that responsibilities for inventory management, receiving, recording and reconciliation are divided among different employees.

Financial Reporting

Financial statement fraud is the least common type of fraud scheme, but also the costliest. Financial reporting fraud involves misrepresentation of the financial condition of an organization through the intentional misstatement or omission of amounts and/or disclosures in the financial statements to deceive financial statement users. Establishing strong internal controls, following appropriate accounting standards, conducting external audit or financial statement reviews and establishing an audit committee within your organization can all help prevent financial statement fraud.

Cybersecurity

While cyber breaches are usually perpetrated by external actors, they often occur with cooperation from the inside—your people or your weak controls. Common controls include user access management; segregation of duties, change management and audit logs; whistleblower mechanisms and incident response plans; training and awareness; and SOC certifications.

Other Fraud Protection Tips

Identifying risks, assigning responsibility for mitigation, designing controls and evaluating effectiveness can't be done overnight or in every functional area simultaneously. In the meantime, the following tips can help you mitigate fraud within your organization.

Create and communicate a path for reporting anonymous tips

43% of the frauds reported by the ACFE last year came to light because of tips. Proactively creating a phone hotline service, dedicated email address or web form can all help organizations identify fraudulent activities. Whatever method you choose, just make sure it protects the identity and safety of the reporter.

Establish an Internal Audit Function

The second most common method of detecting fraud is through internal audits. Whether an individual, department of external provider conducts the audit, ensure they are up to date on the new Global Internal Audit Standards—effective January 9, 2025—and that they stay independent of management.

Examine Procedures Around Documentation and Reconciliation

Older organizations often let their procedures around documentation and reconciliation become outdated. When bringing them up to date, make sure that you have adequate segregation of duties and clear responsibilities outlined within them. Once issued, create a system for keeping them updated and accessible.

Document and Enforce Regular Management Review

Whenever your policies and procedures documents call for management review, make sure that specific steps for that review are outlined. Also, be sure your policies and procedures hold managers accountable for completing each step of their review responsibilities

Develop and Communicate an Anti-Fraud Policy Through Anti-Fraud Training

An anti-fraud policy is exactly what it sounds like—a document that identifies the stakeholders in your organization, their responsibilities to prevent, detect and report fraud, and describes the controls in place that uphold the security of information and safe custody of resources. Once published, an anti-fraud policy should be communicated to and acknowledged by employees at least annually. This can be done via live or recorded anti-fraud training.

Leverage Your Human Resources Function to Identify and Reduce Risk Factors

More than 80% of the time, fraudsters exhibit behavioral red flags that are risk factors for fraud. The most common of these are living beyond means, personal financial difficulties and close relationships with vendors, especially for personnel in operations, sales and accounting. Offering an Employee Assistance Program (EAP) can double as a fraud control, giving would-be perpetrators an avenue to pursue confidential help before they turn to plundering company resources.

Review These Components Annually at the Board/Executive Level

Appropriate governance includes the consideration of risk to the organization. If your Board of Directors or finance committee has never had a comprehensive discussion about fraud risk, now is the time. Consider including it as an agenda item at your next meeting.

While this list is far from comprehensive, preventive actions like these can help your organization guard against fraud and send a message that fraud, waste and abuse will not be tolerated.

About the Author

Brian Lafountain is a Partner at The Bonadio Group. He leads Transportation Advisory Services (TAS), one of The Bonadio Group's consulting businesses. TAS is the nation's largest dedicated student transportation consulting operation, with over 550 clients in 22 states. Brian is also a partner in the firm's Fraud and Forensic Accounting services to public and private clients. He has spent over 20 years in public accounting and internal audit services, helping safeguard his clients from fraud and abuse. A court-recognized expert, Brian also provides expert witness testimony and litigation support services in an advisory capacity. Brian can be reached at blafountain@bonadio.com and at our company website www.bonadio.com.

Accelerating Cyber Resilience by Activating the Value Chain

How To Use Operational Insights to Rapidly Build a Stronger Cyber Defense Posture

By Tamara Nolan, Managing Director, Cyber & Operational Resilience (CORe), MorganFranklin Cyber

Organizations need to be prepared to manage a cybersecurity incident now more than ever. The increased threat of bad actors having access to tools to get ahold of sensitive employee or customer data is prompting board-level attention on a company's cyber resilience.

Events such as the Snowflake Data Breach in mid-2024, where hackers exploited vulnerabilities in Snowflake's cloud data platform, accessing data from over 100 of its customers, the Change Healthcare Breach, where a ransomware attack disrupted healthcare transactions for 100 million people, and the Telecom Hack where hackers accessed the computer systems of nine U.S. telecommunications companies, exploiting vulnerabilities in network devices and routers, gaining access to metadata of users' calls and text messages, underscore the need for cyber resilience plans and capabilities regardless of the industry.

Being prepared to continue those functions within the company that are critical from a financial, reputational, regulatory, and safety perspective, should the organization experience a cyberattack, is critical. It should be demonstrable to the company's board of directors, shareholders, and other key stakeholders. Unlike common IT failures, a cyberattack can take down an organization's technology environment for an extended period. There have been instances where email, for example, was inaccessible for two weeks and critical clinical systems were unavailable for four weeks as the organization worked to isolate the breach and restore IT operations.

To kickstart the initiative of building plans and capabilities to continue critical business functions during a cyber breach or other adverse event it's key to first understand which functions are, in fact, critical. Historically, organizations would undertake a Business Impact Analysis (BIA) to identify and prioritize critical functions and the technology and third parties needed to execute them. Given the speed by which organizations need to demonstrate their ability to manage a breach, however, laborious BIAs are often not an option.

An alternative to the traditional, detailed BIA is an approach that allows organizations to quickly identify critical functions by examining the company's value chain. Central to every organization, regardless of industry, is a set of activities that drive the organization's value, mission, and purpose. When these activities are disrupted for a duration beyond the company's tolerance, the organization can face significant financial, reputational, regulatory, and safety impacts. Identifying and prioritizing critical business functions and the resources needed to perform them by examining the organization's value chain allows companies to get to the BIA answers more quickly. While the detail will not be there, the organization will have the foundation for creating robust cyber resilience plans.

Once the functions and resources are defined, companies can develop their cyber resilience plans. Depending on the industry, companies may elect to have department-level resilience plans only (i.e., Finance, Human Resources, Supply Chain, etc.). If the company manufactures products, it might choose to create factory-level plans that address the continuity of Operating Technology (OT) and other site operations. If you are a hospital system, you might also create resilience plans for clinical functions that extend beyond downtime procedures given the longer-term nature of a cyberattack. Regardless of the industry, the plans and capabilities the organization develops will consist of strategies for continuing those functions that were deemed critical in the organization's value chain.

It's not enough to have plans and capabilities to manage a cyberattack. They must be validated through regular tabletop or functional exercises to ensure the continuity strategies are viable and that key stakeholders are familiar with their individual and team responsibilities. Through scenario-based discussions that prompt participants to think through and discuss their roles, key stakeholders build muscle memory and relationships. Fortunately, tabletop exercises have evolved. While traditional tabletop exercises continue to be very effective, tools to enhance the exercise experience now exist, which can make exercises more interesting and dynamic.

The bottom line—every organization within every industry needs to be prepared for the inevitable cyberattack. For each company, this might mean something different but the need for some level of cyber resilience plan and capability exists. Identify and prioritize critical functions and supporting technology and third parties, build plans and capabilities, and validate the plans and capabilities through regular exercise.

About the Author

Tamara Nolan is Managing Director of Cyber & Operational Resilience (CORe) for MorganFranklin Cyber, where she drives strategic direction and client resilience solutions. With over 20 years in cybersecurity and operational resilience, she leads integrated CORe services and empowers organizations to manage complex threats. Her expertise spans crisis response, executive training and cross-sector strategic advisory. Connect with Tamara Nolan on LinkedIn and at https://www.mfcyber.com/.

AI and the Automation Dilemma

Organizations' critical need to take an integrated approach to their AI deployments

By Sohrob Kazerounian, Distinguished AI Researcher, Vectra AI

With the ever-present hype and buzz around artificial intelligence (AI), it has become relatively tedious to gauge just how far AI has advanced in the last few years and to what extent it is actually deployed in the products we use on a day-to-day basis. At one end of the continuum are companies that previously had nothing to do with AI, who now claim that they are powered by AI or Generative AI (GenAI). At the other end are technologists and economists who continually emphasize how consequential and revolutionary AI could be on society, referring to AI as the new electricity, the fourth industrial revolution, and so on.

The truth, rather unexcitingly, lies somewhere between vaporware and the new human epoch. AI capabilities have indeed been progressing at breakneck pace, advancing more quickly than many of us in the field would have predicted more than a few years ago. GenAI models are now able to coherently answer questions across a wide variety of topics; they can write, code, generate images and music, and much more. Nevertheless, these models are just fallible enough that they cannot be trusted to autonomously carry out end-to-end operations in mission-critical domains like cybersecurity. However, that does not mean that they can't be hugely valuable in mission-critical workflows or trusted in production. Indeed, with thoughtful implementation, GenAI can be deployed to good effect.

Although there are many factors that can guide how to deploy AI into production applications in a safe and robust manner, here, we'll dive into two broad principles that can guide the process.

First, is the idea of *Defensive UX* (user experience). Roughly speaking, defensive UX constitutes a set of design principles that ultimately aim to anticipate the types of errors that could arise when using AI in a product or workflow, and mitigate them by ensuring that those errors either cannot occur, or are non-catastrophic if they do. For example, if you know that your Large Language Model (LLM) occasionally hallucinates details when summarizing logs, a defensive design might automatically surface links to source data alongside every response, or constrain the output space through structured query generation, rather than freeform language completion.

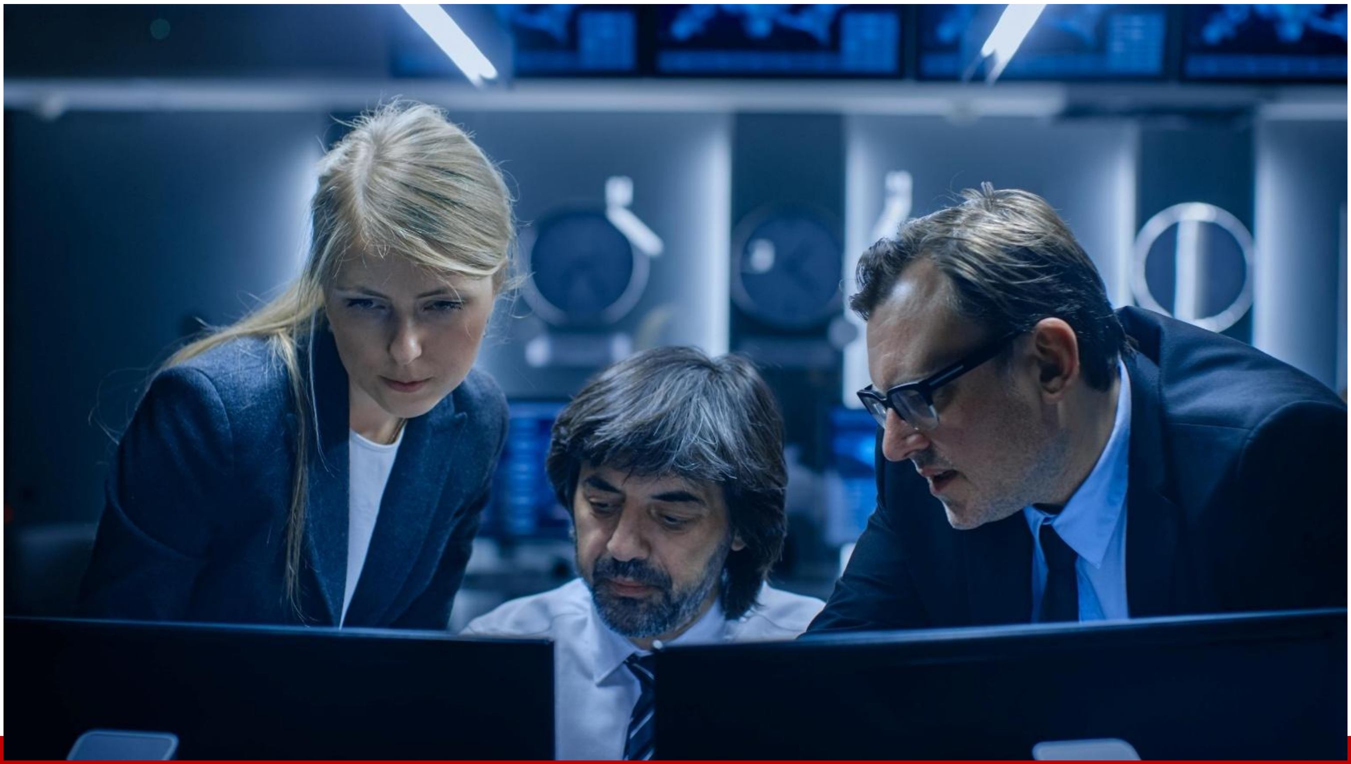
Another high-level design principle, and one that is increasingly popular because of how successful it has been, is the notion of *Agentic AI*. Although it is not fundamentally different from using an LLM on its own, organizing how the LLM interacts with a user or interface by way of agents increases the correctness, verifiability, and robustness of LLM solutions. Agents pair a base LLM with the ability to use tools, access data, maintain a memory, and step through complex state diagrams of actions, all while adapting based on intermediate outcomes and user feedback. Rather than asking a model to output a perfect answer in one go, an agent treats a task as a series of steps — planning, retrieving, verifying, and ultimately resolving — not unlike how a skilled analyst or operator might proceed. This shift toward agent-based architectures is particularly important in security and automation, where precision is non-negotiable, and the cost of error can be high. Agents make it possible to integrate LLMs into environments that require not just linguistic fluency, but rigorous adherence to policy, traceability of decisions, and integration across disparate data systems.

Furthermore, this is to say nothing of the remaining challenges in deploying agentic AI systems in production. For instance, organizations must think not just in terms of how their AI is functioning, but also about things like AI and data governance; how feedback is collected, how performance is audited, and how workflows are adapted over time. This is where engineering culture meets organizational maturity - deployments succeed when they are not treated as one-off model integrations, but as ongoing product programs that blend UX, data, security, directly alongside AI.

Although AI is not on its own a silver bullet, it is nevertheless increasingly important for organizations to make effective use of AI to increase efficiency and productivity for themselves and their customers. As experimentation and adoption of AI progresses across a variety of sectors, we are likely to see that the organizations that succeed are the ones that have taken a more holistic and integrative approach to AI.

About the Author

Sohrob Kazerounian is a Distinguished AI Researcher at Vectra AI where he develops and applies novel machine learning architectures in the domain of cybersecurity. After realizing that his goal of becoming a skilled hacker was not meant to be, he focused his studies on Artificial Intelligence, with a particular interest in neural networks. After receiving his Ph.D. in Cognitive and Neural Systems at Boston University, he held a postdoctoral fellowship at the Swiss AI Lab (IDSIA) working on Deep Learning, Recurrent Neural Networks, and Reinforcement Learning. Sohrob can be reached on LinkedIn and at our company website www.vectra.ai.



Amid Cyberthreats, Telecom Companies Must Balance Security with Innovation

Proactive Strategies Telecom Companies Can Take to Safeguard Their Data and Operations

By Nick Chitopoulos, Technology, Media and Telecommunications Senior Analyst at RSM US LLP

Telecommunication companies continue to face significant cybersecurity issues as network consumption by businesses and individuals evolves. Growing uncertainty related to geopolitical tensions, a shifting tariff landscape, and evolving artificial intelligence technologies are key factors forcing telecommunication companies to strike a delicate balance between security and innovation.

While the threat environment continues to become more complex, reported breaches have declined, per recent RSM research. According to findings in the 2025 RSM US Middle Market Business Index Cybersecurity Special Report, nearly one in five (18%) middle market companies experienced a data breach in the previous year, falling from a record-high 28% in the 2024 data. That dip could easily lead to complacency, but companies need to remain diligent as threats persist.

Underscoring the importance of taking the threat environment seriously are cybersecurity regulations—such as the cybersecurity risk management standards articulated in Executive Order 14028—that require companies to ensure the integrity of their systems.

Unconventional cyber warfare

With global tensions stemming from conflicts in the Middle East, Ukraine, and India as well as trade wars affecting geopolitical relationships, there are increased risks of cyber-attacks between foreign adversaries.

Companies also continue to navigate physical attacks on their global telecommunications networks. The physical network of cables, data centers, and energy connections is so vast that it would be almost impossible to defend the entire network from targeted attacks or extreme weather conditions. Underwater transoceanic internet cables are some of the most vulnerable telecommunications infrastructure.

The situation between China and Taiwan highlights the potential vulnerabilities of transoceanic internet cables. Taiwan has 15 undersea cables that connect its internet network to the rest of the world. An attack from China could sever these links and leave the country, and its inhabitants, disconnected from outside information and communication. In response, Taiwan has started to build its own satellite network to remain operational in case of an attack. This increase in satellite broadband capabilities will allow people there to communicate even when networks are down. During the Los Angeles wildfires, satellite connections were used to allow first responders and victims to communicate via text throughout the ordeal.

Artificial intelligence changing the cybersecurity landscape

AI has changed the landscape for most industries as the technology evolves into different applications and its functions improve. From a cybersecurity standpoint, AI has had implications on both sides of the equation. For attacks, AI can increase the scale and automation of cyberattacks, make data and intelligence gathering more efficient, and allow attackers to better customize and adapt their processes. There is also the threat of AI improving social engineering attacks with AI-generated deepfake videos, audio, or images to better fool targets.

On the other side, using AI to comb through and analyze data can help companies improve their ability to detect cybersecurity threats by honing pattern recognition capabilities, automating repetitive tasks, and enabling real time responses to incidents. AI tools can also help free up human members of organizations' cybersecurity teams for more meaningful tasks and allow them to use such tools to analyze and interpret findings.

According to the RSM Cybersecurity Special Report, 34% of smaller middle market companies indicated that they do not yet have AI governance steps in place. To successfully deploy AI, technology companies need to have the employee resources and skills to implement an effective governance framework. Various frameworks are currently available from the National Institute of Standards and Technology, industry organizations, and several countries.

Proactive strategies

Customers of telecommunication companies need to trust that their data and personal information is secure. Any potential data breach or other cyber-attack could damage a telecommunication company's brand.

As noted in this April article from RSM, "The increase in the number and sophistication of attempted cyberattacks over the last five years has led to several high-profile system compromises in the telecom sector and across most industries in the U.S." The FBI received an average of 758,000 complaints per year from 2019 to 2023 and calculated around $12.5 billion of losses in 2023 alone.

Here are some proactive strategies telecom companies can take to safeguard their data and operations:

- Reexamine capital expenditures and make strategic decisions to strengthen the organization's cybersecurity function
- Explore how teams may be able to combat adversarial AI with their own AI cybersecurity applications (while adhering to an effective AI governance framework)
- Conduct regular security audits and continue to monitor and react to suspicious activity
- Develop and test plans and procedures related to potential data breaches or physical issues on an ongoing basis
- Make sure employees have the necessary skills and training to identify the latest threats and respond effectively and in a timely manner

The takeaway

As they navigate a complex host of challenges, telecommunication companies need to make sure that their networks are resilient and equipped for what threats may come their way. Physical security, disaster relief plans, and backups will play a vital role in securing networks and allowing trade and information to flow uninterrupted.

About the Author

Nick Chitopoulos is a senior tax manager at RSM US LLP. In 2024, he was selected as a member of RSM's Industry Eminence Program, which positions its senior analysts to understand, forecast and communicate economic, business and technology trends shaping the industries the firm serves. As an analyst in the program, Nick focuses on the technology, media and telecommunications industry. He is based in the firm's Boston office. Nick can be reached at nick.chitopoulos@rsmus.com and at our company website at rsmus.com.

Beyond Production: Why Securing Dev and QA Environments Matters

By Ranjan Kathuria, Cloud Security Architect at Rubrik Inc.

In secure software development, development teams usually write and test their code in dedicated environments before it goes live for customers. These are called the development (dev) and quality assurance (QA) environments. The dev environment is where engineers build and test their own parts of the software or application. It's set up with all the tools, packages and mock data they need, and engineers often start with a branch or snapshot of the latest code from the production. Once the code is ready, it moves to the QA environment, where automated tests run to check if everything works as expected.

Most people know it's important to protect the production system, but they often forget about dev and QA environments. If these environments are left open to the internet, attackers can use them to find vulnerabilities that are not even introduced in production yet. That's why it's just as important to secure dev and QA environments as it is to protect production. Treating them with the same level of security helps keep your whole organization safe.

Why Securing Dev and QA Environments Is Business Critical

Before we discuss why securing development environments is critical, let's examine the current landscape:

- The State of API Exposure 2024 report found nearly 3,945 development APIs publicly accessible across major organizations, with 198 highly critical vulnerabilities directly related to these exposures. Many of these APIs lacked proper security controls, exposing sensitive information and providing easy entry points for attackers.
- According to Black Duck's 2024 snapshot, information leakage and predictable resource locations are among the most common vulnerability classes, affecting 66% and 35% of organizations respectively. These issues frequently stem from exposed development environments, where sensitive data and endpoints are inadvertently left accessible.
- In December 2024, Cisco confirmed that attackers accessed and exfiltrated data from its public-facing DevHub environment. The breach involved leaked source code, credentials, and confidential documents, all due to a misconfigured environment that was accessible from the internet without proper authentication or authorization controls.

These incidents highlight a systemic problem which is publicly exposed Dev and QA environments are a prime target for attackers. When these environments are accessible over the internet, they act as an open invitation for threat actors to probe, enumerate, and exploit vulnerabilities that would otherwise remain internal.

You might wonder why attackers are so interested in dev and QA environments. Here's a closer look at the reasons:

- Constant Change and Lower Security: Dev and QA environments are where new code is written, integrated, and tested daily. Unlike production, these environments often lack rigorous security controls, as the focus is on rapid development and testing rather than security hardening.
- Incomplete Security Coverage: Security teams may not continuously monitor or test these environments, leading to unpatched vulnerabilities, misconfigurations, and exposed secrets (like API keys and credentials).
- Shadow APIs and Unmanaged Assets: The rapid pace of development can lead to "shadow APIs" endpoints that are undocumented, unmanaged, or forgotten. These APIs often bypass security reviews and are left exposed, increasing the attack surface.
- Weak Authentication: Development APIs and services may use weak or default authentication, or none at all, making it trivial for attackers to gain access.
- Risky Dependencies: Developers may install third-party libraries or packages that contain known vulnerabilities, further weakening the environment's security posture.

Once attackers discover an exposed Dev or QA environment, they can:

- Enumerate APIs and endpoints to find vulnerabilities.
- Extract sensitive data, credentials, and source code.

- Use the environment as a foothold for lateral movement into more sensitive systems.
- Exploit misconfigurations and unpatched software to escalate their access.

Best Practices for Protecting Dev and QA Environments

While there are many ways to improve security, every Dev and QA environment should meet these basic requirements set by a security architect:

1. Keep Dev and QA Environments Internal

- Dev and QA environments should not be exposed to the public internet. Some people worry that moving these environments behind internal networks or VPNs will hurt productivity, but this step is crucial for security. Exposing these environments makes it much easier for attackers to find and exploit vulnerabilities before they are fixed. The biggest lesson from past breaches is simple: always keep Dev and QA environments internal.
- If certain APIs need internet access (for example, A Vendor API), only expose those specific endpoints. Use a Web Application Firewall (WAF) to restrict access by IP address and allow only the necessary paths. This targeted approach protects your environment while still enabling essential connectivity.

2. Scan for Vulnerabilities from the Start

A common problem is when developers install vulnerable packages in their virtual environments and then push this code to GitHub or another source code repository. To prevent this:

- Set up vulnerability scanning in your CI/CD pipeline or source control system to block commits or deployments that contain known vulnerable packages.
- Use automated tools or built-in security features in GitHub to scan dependencies.
- While EDR solutions can help detect malware, dedicated dependency scanning tools are better suited for catching vulnerable packages early.

3. Enforce Automated Code Review Before Deployment

Only allow code to be deployed after all issues flagged by automated code review tools (such as SonarQube, CodeRabbit, or Codacy) have been addressed and fixed. This ensures that code quality and security standards are met before anything reaches the Dev or QA environment.

4. Additional Best Practices

- Network Segmentation: Isolate Dev and QA environments from production and from each other to reduce the risk of lateral movement if one is compromised.
- Datas
- Regular Updates and Patching: Keep all software, dependencies, and operating systems up to date in Dev and QA environments.

- Audit and Monitor: Continuously monitor these environments for suspicious activity and regularly review access logs.
- Always use mock or anonymized data in Dev and QA environments to protect sensitive information. This minimizes the risk of data leaks if these environments are exposed or compromised.
- Secure Secrets Management: Never hard-code secrets or credentials in code. Use secure vaults or environment variables managed by trusted tools.

About the Author

Ranjan Kathuria has over nine years of experience in the security industry, where he has played a key role in building security programs and mentoring security engineers. Currently, he serves as a Cloud Security Architect at Rubrik Inc, where he focuses on safeguarding the cloud environment. Additionally, he is recognized as a top-tier security researcher for HubSpot and Quora's Bug Bounty Programs on Bugcrowd, contributing to the enhancement of security measures on these platforms.

Beyond The Firewall: Why Cross Domain Solutions Are Mission-Critical for Federal and Defense Agencies

Rethinking Secure Data Access and Transfer Across Classified and Controlled Environments

By Jill Bradshaw, Senior Product Marketing Manager at Everfox

In the complex landscape of national cybersecurity, evolving threats are increasingly matched by the growing demands of data-driven missions, making the role of Cross Domain Solutions (CDS) more vital than ever. For CISOs, CTOs, and federal cybersecurity leaders, CDS is not only a security feature; it is a critical mission enabler.

The heightened demand for timely, secure access to data across classification levels and network boundaries is a reality for federal agencies, particularly those in defense, intelligence, and homeland security. The traditional model — isolated, air-gapped networks — is now insufficient in an era where multi-domain operations, cloud transformation, and real-time collaboration are operational imperatives.

Identifying and defining Cross Domain Solutions, common misconceptions and implementation challenges, are key considerations for every agency when evaluating and deploying the right solution to help ensure a secure mission.

Understanding Cross Domain Solutions

A Cross Domain Solution (CDS) facilitates secure data sharing and access across networks that operate at different classification or security levels. These networks may be physical or virtual, isolated by design to prevent unauthorized data leakage or cyber intrusion. A secure CDS makes it possible to access, transfer, or transform data between these environments without compromising confidentiality, integrity, or availability.

A helpful analogy to understand the importance of a secure CDS is airport security sophistication. Firewalls function like check-in desks as they verify identification and allow authorized individuals through. Diodes act like one-way exits in an airport; they are set up to allow one-way flow of traffic throughout the airport and not let traffic come back in the other direction. Cross Domain Solutions act like a TSA checkpoint: Inspecting every item, scanning for threats, and enforcing rules about what may or may not pass through. Just as airport security prevents contraband from boarding a plane, Cross Domain Solutions are designed to ensure no malicious data or unauthorized information crosses boundaries between classified and unclassified environments. All of these components work in concert to protect against persistent threats, insider misuse, and accidental data spillage.

Why CDS Matters Now More Than Ever

As cyber threats advance, several trends are converging to heighten the need for Cross Domain Solutions:

- **Remote Access to Sensitive Information at multiple classification levels**: Field agents, personnel on temporary duty assignment or employees with approved teleworking agreements often require secure remote connections. Additionally, it is ideal to have a plan for secure connections if unforeseen circumstances (such as emergencies or health-related issues) arise.
- **Cloud Adoption and Modern IT Architectures**: Agencies are increasingly using cloud services, which introduce complexities in managing data flows between cloud-based environments and on-premises classified networks.
- **Multi-Domain Operations**: Collaboration between intelligence, operations, and logistics requires real-time data sharing across domains and classification levels with other partners and agencies.
- **Increasing Threat Landscape**: The sophistication of cyber threats- ransomware, zero-days, and nation-state actors- necessitates deeper inspection and greater assurance than what traditional perimeter defenses can offer.
- **AI Model and Integratio**n: As AI becomes more important to modern applications -- and ultimately to decision dominance -- solutions should support secure, high-speed access to AI models operating at lower classification levels and enable the rapid transfer of data to highly classified AI environments.
- **Policy and Compliance Mandates**: Initiatives like NCDSMO's Raise-the-Bar (RTB) standards are increasing requirements on what qualifies as acceptable CDS, requiring modern and accredited solutions.

These drivers combined make CDS even more essential—not only to safeguard data but to enable agile, responsive mission execution.

Evaluating a CDS: What to Look For

As agencies evaluate a Cross Domain Solution, they should be aware that not all solutions were created equal. Here are some key areas that should be considered for evaluation:

1. **Transfer or Access Support:** Many times, CDS solutions that allow access without transferring data may meet mission requirements. However, consider whether a transfer CDS is necessary and if there are requirements for bi-directional or one-way data transfer.
2. **Latency and Data Type Handling:** Assess how the solution handles different data types required and if the solution meets latency requirements.
3. **Scalability:** Ensure solutions can grow with your organization and support future requirements.
4. **Compliance and Accreditation Readiness:** Most solutions for government require NCDSMO RTB compliance and not all CDS solutions can meet this.
5. **Security Features**: Real-time filtering, inspection, validation, and diode capabilities are important and can vary with CDS providers.
6. **Tactical Edge Requirements:** Solutions deployed to the tactical edge must deliver robust capabilities while meeting specialized requirements for size, weight, power and cooling to meet mission requirements. There are also specialized requirements for environments like space or air that require different solutions than something that will be deployed in a backpack or in the desert.
7. **Other considerations:** Centralized management capabilities, training and support models, and cost and ROI are also important considerations as you consider a CDS solution for your environment.

The Future of Cross Domain Solutions

Modern missions require real-time, multi-domain collaboration. To meet these evolving demands, future Cross Domain Solutions (CDS) should integrate artificial intelligence and automation to enhance filtering processes and boost threat detection capabilities. Embracing Zero Trust Architectures is essential, helping to ensure that every transaction undergoes rigorous verification to maintain system integrity. Furthermore, enabling mobile and edge access to classified systems is crucial, particularly for operations in remote and contested environments where timely information is vital. Adopting cloud-native designs will support containerized, scalable deployments, allowing flexibility and responsiveness in dynamic operational contexts.

Enabling the Mission with Confidence

Cross Domain Solutions are not just a checkbox in a compliance framework. They are mission-critical infrastructure. The right CDS allows your agency to operate with agility and confidence, share intelligence, coordinate operations and respond to threats in real-time.

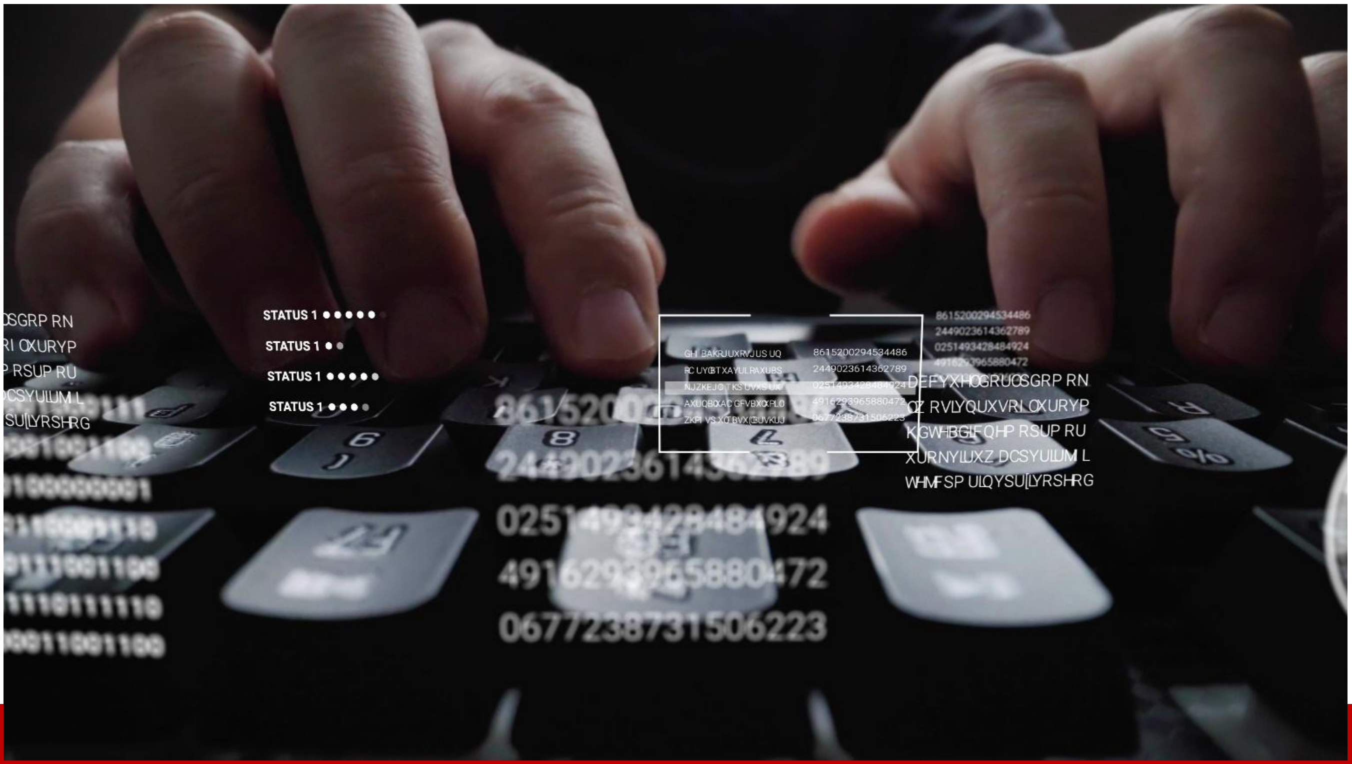
For CISOs and security leaders, this is an opportunity to lead from the front. By championing smart, scalable, and accredited CDS deployments, you can empower your teams, reduce cyber risk, and help your agency deliver on its most critical objectives securely.

About the Author

Jill Bradshaw is Senior Product Marketing Manager at Everfox, bringing over 20 years of experience in the technology sector, with a focus on networking, zero trust architecture, cross domain solutions, tactical systems, and AI technologies. She collaborates closely with government, industry, and executive stakeholders to ensure that technology solutions align with evolving federal and critical industry requirements. Jill earned her MBA from Baylor University and Bachelor's degree from Texas Tech University. Beyond her professional role, she serves on the board of the Rocky Mountain Deaf School and as a Commissioner on the Colorado Commission for Deaf, Hard of Hearing and DeafBlind. In her personal time, Jill enjoys hiking, camping, and spending time with her family.

Email: Jill.Bradshaw@everfox.com

Website https://www.everfox.com/



Breaking Down the Application Programming Interface (API) Security Lifecycle

A Comprehensive Guide to API Security

By Adam Arellano, Field CTO, Harness

APIs are the heartbeat behind nearly all of our digital interactions. From checking the weather, using Uber, or asking Alexa to turn the lights on in our personal lives to e-commerce integrations, Google Drive, Microsoft SharePoint, or Okta in our professional lives, it’s hard to find a digital function that APIs don’t touch.

While APIs have been a driver of digital transformation, they haven’t come without risks. Over half (57%) of organizations have suffered from API-related breaches in the past two years, with 73% experiencing three or more incidents. Without the proper security controls, APIs can open the door for threat actors to access sensitive data and critical business resources — leaving significant reputational and financial damage in their wake.

We must change the narrative and take the right actions to secure APIs. Safeguarding APIs is not one singular function but a series of steps that follow alongside the API lifecycle from design to development and production and require collaboration between different teams. To bolster API security posture and reduce the number of API-related attacks, it’s important to take the following steps:

1. Understand Who Owns API Security

It can be difficult to pinpoint a single API security owner because responsibility is shared across so many functions. Typically, one of three roles acts as the API security champion at the top: the chief information security officer (CISO), the head of enterprise and/or security architecture, or the head of product security. These leaders are typically responsible for designing and enforcing the API security program and providing strategic leadership, resource allocation, design standards, tool selection, security testing, and vulnerability management.

Next, are the “responsible stakeholders,” — those directly responsible for implementing and operating the critical API security activities designated by the CISO, the head of enterprise and/or security architecture, and/or the head of product security. Teams in this category include product and application security teams and security operations and incident response teams.

Then comes adjacent stakeholders whose job functions may not directly be responsible for securing APIs, but have responsibility for other initiatives that coincide with API security. Typically, these teams inform API security policies or use APIs to fulfill their roles. Teams in this category include governance, risk, compliance, and anti-fraud teams, data protection officers, and the API developers themselves.

2. Dividing the NIST Cybersecurity Framework Actions By Team

The NIST Cybersecurity Framework 2.0 serves as a tool to outline the key functions and outcomes of cybersecurity programs overall and translates well to create and maintain a robust API security program. To build an “API security lifecycle,” organizations can mirror the six stages of the NIST framework. From an API security lens, this would look like:

Identify

When building an API security program, it’s important to catalog all APIs within the organization, including internal, external, and third-party APIs. Next, organizations need to conduct risk assessments to understand potential vulnerabilities.

To help with this stage, security and development teams should consider implementing automated tools to continuously discover and inventory all deployed APIs. Then, organizations can maintain an updated catalog of APIs, including multiple versions and endpoints. These tools can also identify unmanaged or “shadow” APIs that pose significant security risks.

Key stakeholders in this stage include the product, application security, and GRC teams.

Protect

After understanding the extent of APIs on the network, product and application security teams and API developers must require certain safety measures such as authentication, authorization, and encryption — on top of regular security testing.

Performing automated and manual application security testing (DAST) can help these teams identify runtime vulnerabilities and test API resilience against common threats. Organizations should also create a centralized management system to identify vulnerabilities and then prioritize them based on severity and impact. Then, security teams can implement remediation efforts to address any issues before deployment.

Detect

Next, the SOC, incident response, and anti-fraud teams, with the data protection officer, have to work together for the "Detect" phase. To detect and analyze potential attacks, these teams must track API activity in real-time, using logging and alerting mechanisms, and creating and storing detailed logs for any investigation.

The goal of the "Detect" phase is to monitor and log API activity to identify threats in real-time — preventing long dwell times and minimizing the risk of a threat actor accessing sensitive data. This includes capturing and analyzing API logs, proactively looking for indicators of compromise (IOCs) and using signature-based detection to identify known attack patterns.

Respond

Now that the organization has the ability to detect potential attacks, it's important to have a plan to respond. After all, it is not a matter of if an attack is going to happen, but when. The SOC and incident response team must have a plan in place that ensures business continuity, can block malicious activity, and execute incident response protocols when an attack occurs.

The key to success in the "Respond" phase is configuring actionable alerts based on predefined terms and integrating them with incident management systems like security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools.

Recover

The SOC and incident response teams will also be the primary stakeholders once the dust has settled on API security attacks. Recovery is arguably one of the most important steps to restoring business operations and maintaining a business' reputation.

It is critical for organizations to have a robust recovery process that ensures API functionality and security in the event of an incident. The "Recovery" phase includes a thorough investigation to determine the root cause of the attack, analyzing API sequences and traces to understand attack vectors, and collaborating with the right teams to implement corrective measures.

It's important for organizations to learn from mistakes. Taking the time to document lessons learned, conduct tabletop exercises, and update security protocols can prevent a similar attack from happening in the future.

Govern

The final piece of the API Security Lifecycle is the "Govern" phase, which involves developing API security policies that are aligned with broader security and compliance requirements such as CCPA, GDPR, and HIPAA, all while implementing role-based access controls and continuous monitoring.

Enterprise architecture, product and application, and GRC teams have to work together to establish clear responsibilities for API security, ensure that all stakeholders are informed and processes are well-documented. This, in combination with a strong API security platform, will offer visibility, control, and report capabilities to keep enterprises safe, enforce policies, and demonstrate compliance.

To slow down attacks on APIs, organizations need to consider incorporating the "API Security Lifecycle" into their day-to-day operations. By clearly defining ownership across the teams and having a strong API security plan in place, organizations can have truly resilient APIs and reduce API-related risks, safeguard sensitive data, and provide seamless and secure digital experiences.

About the Author

Adam Arellano is the Field Chief Technology Officer (CTO) at Traceable by Harness, where he provides partnership and guidance to customers and the broader industry on API security. He is well known as a progressive and inventive technology executive offering over 15 years of success in championing mission-driven initiatives focused on cloud, AI, and information security innovation.

He has assembled a rich blend of technical prowess and business acumen, culminating with a talent for building effective cybersecurity programs and teams as a foundation for scalable and highly secure information architectures. He's a pragmatic advisor and team leader who thrives when harnessing insights into interactions between people and systems to build genuinely unique technology solutions.

Adam is a devoted parent to six children living in Charlotte, NC, where he is a profoundly amateur cook with a strong aversion to cleaning the kitchen. As an analogue to his time in the Marine Corps, he is passionate about helping transitioning service members and promotes causes that offer foster care and adoption services to local community members.

Building a True Zero Trust Strategy for Cloud Environments

Closing Every Door Hackers Use to Breach Cloud Environments

By Jay Jangid, SEO Specialist at Tecuy Media

Zero trust is simple to define but complex to implement. It means never trust, always verify—especially in cloud environments where perimeters no longer exist. As digital transformation accelerates, the need for a resilient, context-aware cybersecurity model becomes urgent. A well-architected zero trust strategy is no longer optional—it's essential.

Understanding Zero Trust Architecture

At its core, zero trust challenges the decades-old assumption that things inside a network can be trusted. Instead, it verifies every user, device, application, and workload at every interaction.

Its foundational pillars—identity, microsegmentation, least privilege access, and continuous validation—form a stronghold against lateral movement and unauthorized access. Unlike traditional models that rely on firewalls and network boundaries, zero trust shifts focus to individual entities and their interactions.

The Rise of Cloud Complexity

Cloud computing isn't just a tech shift—it's a security reset. Organizations now operate in multi-cloud and hybrid environments, each with its own tools, policies, and gaps. Add to that shadow IT, where employees spin up services without oversight, and the explosion of APIs, and the result is an attack surface that's growing faster than many can secure.

According to Gartner, by 2025, 99% of cloud security failures will be the customer's fault—most often due to misconfigurations and inadequate identity controls.

Why Cloud Requires a Different Approach

Cloud environments are dynamic, scalable, and decentralized. Traditional perimeter defenses like VPNs or network-based firewalls don't fit this new mold. Here's why:

- Cloud-native apps don't sit behind static IPs—they live in containers and serverless runtimes.
- Traditional identity controls often fail to scale across federated, cross-cloud ecosystems.
- Attackers exploit lateral movement, hopping across systems using compromised credentials or misconfigured APIs.

Zero trust doesn't just improve posture—it brings visibility, control, and contextual access, all critical in today's distributed systems.

Key Pillars of Zero Trust in the Cloud

A successful cloud-based zero trust model rests on these four pillars:

1. **Identity-centric security:** Enforce multi-factor authentication (MFA), use single sign-on (SSO), and manage identity lifecycles tightly.
2. **Device verification:** Check device posture before granting access. Is it patched? Is antivirus running?
3. **Network microsegmentation:** Split your network into fine-grained zones. Limit communication to the bare minimum required.
4. **Continuous monitoring:** Don't trust one-time verification. Use tools like Microsoft Defender, AWS GuardDuty, or Splunk to monitor behavior in real time.

Identity as the New Perimeter

Identity is the backbone of zero trust in the cloud. Access management tools like AWS IAM, Azure Active Directory, and GCP IAM play a central role. But they come with challenges:

- Identity sprawl across clouds makes management complex.
- Overprivileged accounts are a real threat—think developers with full access in production.

- Without centralized governance, inconsistencies creep in fast.

A compromised identity today is often the root cause of cloud breaches.

Enforcing Least Privilege Across Cloud Services

Source: PureStorage

Give users and apps only the access they need—nothing more.

- Use role-based access control (RBAC) or go a step further with attribute-based access control (ABAC).
- Automate access provisioning and revocation using policy engines.
- Regularly audit entitlements using tools like CloudKnox or Sonrai Security.

Least privilege isn't about slowing people down—it's about preventing accidental damage or insider threats.

Zero Trust Network Segmentation in the Cloud

Don't let apps freely talk to each other.

- Define network security groups (NSGs) and firewalls at every layer.
- Use cloud VPCs (Virtual Private Clouds) to isolate environments.
- Introduce service mesh technologies like Istio for deeper microsegmentation and observability.

This approach drastically reduces the blast radius of a breach.

Securing Workloads and Containers

Containers and serverless environments break traditional security molds.

- Implement container runtime security with tools like Aqua Security or Falco.
- Scan images before deployment.
- Use Kubernetes admission controllers to prevent risky workloads from spinning up.

These cloud-native architectures demand cloud-native security.

Role of Continuous Verification

Authentication isn't a one-time event anymore.

- Apply behavioral analytics to detect anomalies.
- Use machine learning to flag suspicious activity.
- Trigger reauthentication or access revocation when risk signals emerge.

Zero trust security adapts based on context. That's its power.

Zero Trust and DevOps Integration

Security must shift left.

- Integrate security into CI/CD pipelines.
- Use Infrastructure as Code (IaC) to ensure secure configurations by default.
- Enforce policy-as-code using tools like Open Policy Agent (OPA).

If your developers can deploy, they must also help defend.

Visibility and Logging

You can't protect what you can't see.

- Use AWS CloudTrail, Azure Monitor, and GCP Cloud Audit Logs.
- Integrate data into centralized SIEM platforms like Splunk or Elastic.
- Ensure you're logging not just access, but intent and behavior.

Logs are the backbone of incident response and compliance.

Zero Trust Misconceptions to Avoid

Let's clear the air:

- Zero trust isn't a product—it's a strategy.
- It doesn't mean zero usability—done right, it enhances UX.

- Vendor buzzwords don’t equal true zero trust. Beware of rebranded firewalls.

Focus on principles, not marketing.

Challenges and Pitfalls in Cloud Zero Trust

Every journey has bumps:

- Too many tools lead to integration fatigue.
- Alert overload causes teams to miss real threats.
- Without executive buy-in, initiatives fail fast.

The key is a phased rollout—start small, iterate, improve.

Compliance and Zero Trust Alignment

Zero trust isn’t just smart—it’s compliant.

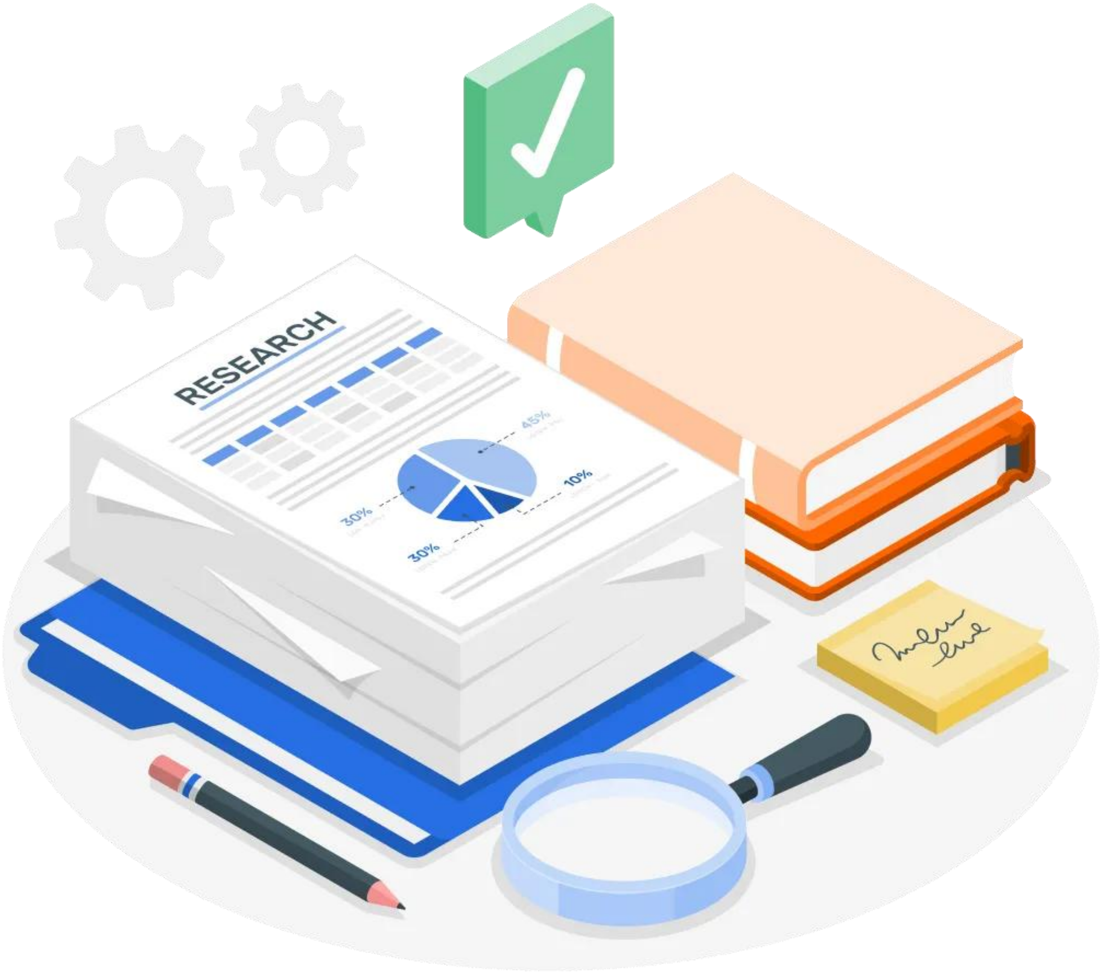
- It maps well to NIST 800-207, CISA zero trust Maturity Model, and ISO 27001.
- Helps meet GDPR, HIPAA, and FedRAMP requirements.
- Makes audit trails easier and more reliable.

Security and compliance, when aligned, create long-term resilience.

Case Study Example

A healthcare provider in the US adopted zero trust post-COVID to protect remote work. Within months:

- Lateral movement dropped 84%
- Phishing click-throughs fell by 72%
- Compliance audits passed with zero major findings



Source: InstaSafe

Their journey began with identity and grew to full network segmentation.

Future of Zero Trust in Cloud Security

The future looks adaptive:

- AI will make predictive access decisions in real-time.
- Identities will verify themselves through biometrics and behavior.
- Cyber threats will be countered by self-healing infrastructure.

Zero trust is evolving—and you need to evolve with it.

Conclusion

Zero trust is not about paranoia. It's about precision. In the cloud, where walls don't exist, and users log in from everywhere, zero trust gives you a way to keep control.

Start with identity. Add verification. Monitor everything. Trust nothing without proof.

And above all, remember—it's not a destination. It's a journey of continuous visibility, validation, and vigilance.

About the Author

Jay Jangid is an SEO Specialist with five years of experience specializing in digital marketing HTML keyword optimization meta descriptions and Google Analytics. A proven track record of executing high-impact campaigns to enhance the online presence of emerging brands. Adept at collaborating with cross-functional teams and clients to refine content strategy. He currently works with Tecuy Media. For inquiries, you can reach him at JayJaangid@gmail.com.

LinkedIn | Instagram | Twitter

Strengthening Remote Work Security: A Guide to Effective Strategies

Addressing Cybersecurity Challenges in the Age of Remote Work

By Rex Johnson, Executive Director, Cybersecurity, CAI

The shift to remote and hybrid work has transformed the way organizations operate, introducing unique cybersecurity challenges that the C-suite at any organization must address. As employees access corporate networks from various locations—often using personal devices such as cellphones—the risk of cyber threats has increased dramatically.

Remote Work and Security Implications on the Rise

The move to a work-from-anywhere model was accelerated by the COVID pandemic, and this trend continues to reshape organizational structures. While remote work offers flexibility and scalability, it significantly expands the attack surface for cybercriminals. The global average cost of a data breach in 2024 reached $4.88 million—a 10% increase over the previous year and the highest total to date.

When it comes to remote or hybrid work models, security teams are challenged:

- **Increased Vulnerability:** Home networks are generally less secure than corporate networks, making them attractive targets for cyberattacks.
- **Device Management:** Employees can use personal devices which may not have the same security controls as company-issued equipment.
- **Data Security Risks:** Transmission of sensitive data over potentially unsecured networks poses significant risks.

These vulnerabilities require a reevaluation of traditional cybersecurity practices. Organizations must adopt tailored strategies that address these specific challenges to maintain security. By implementing these measures, teams can effectively safeguard their digital assets and ensure that remote work environments remain secure.

Simple Ways to Secure Remote Work Environments

Organizations can implement several actions that safeguard assets including, but not limited to:

- **Virtual Private Networks (VPNs):** VPNs are essential for ensuring secure access to corporate resources. They encrypt internet traffic, protecting data from interception and ensuring that employees connect to the company network securely.
- **Secure Collaboration Tools:** As remote teams rely heavily on collaboration tools, it's crucial to choose platforms that offer end-to-end encryption and security features. Tools like encrypted messaging apps and secure file-sharing services can help protect sensitive communications, content, and data.
- **Employee Training:** Regular training sessions can educate employees about phishing and smishing attacks, password creation best practices, and the importance of device maintenance. Fostering a culture of cybersecurity awareness can reduce the risk of human error.

These tactical solutions lay the groundwork for securing remote work environments by addressing immediate vulnerabilities. However, with cyber threats continuously evolving, organizations must also integrate larger, strategic initiatives to ensure long-term resilience.

Best Practices

To effectively secure remote work environments, it’s important to conduct regular security audits. These periodic assessments identify potential vulnerabilities and ensure compliance with established security standards. By systematically evaluating remote work setups, organizations can proactively address weaknesses and reinforce their defenses.

When the risks are understood, then a robust incident response plan can help a team properly navigate it, if a cyberattack does occur. This plan should detail clear procedures for detecting, reporting, and responding to cyber incidents. It will help all team members be aware of their responsibilities during a crisis, minimizing the impact of security breaches and maintaining business continuity.

The best strategies are a joint effort with other departments. Security teams can partner with HR to establish a comprehensive security policy that is highly adopted and visible throughout the company. This policy should clearly define the security protocols and guidelines that govern remote work, covering critical aspects such as device usage, data protection, and incident reporting. A well-defined policy provides a framework for consistent security practices across the organization, ensuring that all employees understand their roles in maintaining security.

Internal and External Partners Enhance Strategies

In addition to working with HR, other internal teams and external partners can enhance an organizations' security measures. This dual focus fosters a comprehensive defense strategy that anticipates and mitigates evolving cyber threats.

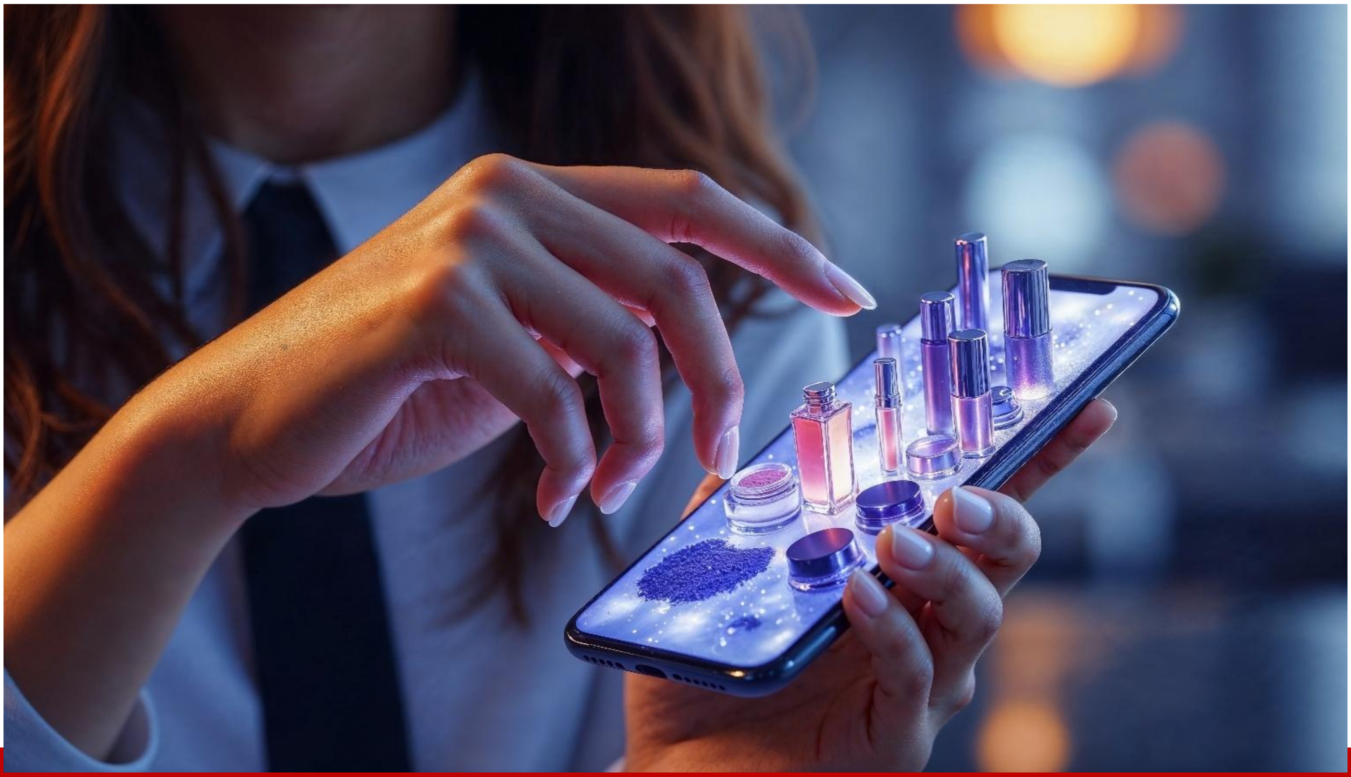
Effective cybersecurity in remote work settings requires participation between IT teams, CISOs, and employees—after all, everyone is on the frontline when it comes to cyber defense. Open lines of communication ensure that everyone is aware of security policies and best practices.

Establishing partnerships with external cybersecurity experts and industry peers can further bolster security effectiveness. Sharing insights with other organizations facing similar challenges provides valuable opportunities to learn and make agile decisions based on past experiences. Plus, networking helps the industry stay informed about the latest threat landscape and emerging technologies.

Cybersecurity relies on the alliance of all stakeholders. By creating in-depth strategies, deploying effective tactics, and complementing it all with both internal and external resources, security and IT teams can build a resilient network that is well-equipped to tackle the complexities of remote work environments.

About the Author

Rex Johnson, Executive Director, Cybersecurity at CAI, has over 30 years of management experience encompassing IT, Cybersecurity, Privacy, Incident Response, Digital Forensics and Analysis, and Enterprise Risk Management. He has assisted numerous organizations in assessing and reducing their risks leading to improved operations and security maturity. Rex has provided both technical and advisory services for both commercial and public sector industries. He sits on Industry Insight Committee supporting the learning content strategy for ISC2. Rex can be reached via LinkedIn, or visit the company website https://www.cai.io/



Future-Proofing Your Organization’s Mobile Strategy with End-to-End Management

By DJ Oreb, President of Managed Services, DMI

When managed properly, government-issued mobile devices enhance daily operations and empower the workforce to collaborate more efficiently. However, these devices pose a massive security risk if compromised by bad actors. Every device increases an agency's attack surface and has the potential to expose critical data like classified communications and secure authentication credentials.

Most federal agencies are responsible for managing and securing tens of thousands of endpoints. Concerningly, a December 2024 audit by the Inspector General revealed challenges the DOD faces in securing classified information on mobile devices. The surge in devices and telework following the pandemic revealed scaling challenges, while the absence of an approved incident response plan left teams unprepared in the event of a security breach.

Managing and securing these endpoints is often disjointed, with employees navigating multiple disconnected systems without a cohesive mobile management strategy. This lack of integration leads to security and compliance gaps, an especially critical risk for high-stakes environments like defense agencies where protecting sensitive information can mean the difference between life and death.

A practical mobile management approach can improve security and streamline operations through enhanced visibility, centralized device management and built-in security measures.

Driving Efficiency and Savings with Centralized Mobile Management

Traditional mobile management strategies span multiple vendors and disconnected systems. While this approach may have been effective when agencies had fewer devices to manage, the proliferation of smartphones, tablets and other devices following the pandemic has made these strategies inefficient and costly, creating unnecessary complexity and increasing administrative overhead.

A single, cloud-based mobility solution can improve security across all aspects of mobility management, from device deployment to lifecycle management. By integrating management services into a single solution, agencies can configure, secure and oversee their entire infrastructure from one single point.

This centralized approach reduces errors and inconsistencies resulting from siloed processes and provides access to real-time data analytics. This enhanced visibility enables agencies to make informed security decisions based on the location and status of their mobile devices—revoking access if a device displays suspicious behavior or tracking down lost or stolen devices. This is particularly vital for agencies operating in environments where access to real-time data is essential for mission success and safety.

Additionally, a centralized management approach is future-resilient. With agencies managing mobile devices across the globe, efficiently scaling infrastructure management is a constant challenge. By eliminating the difficulties associated with managing multiple mobile ecosystems, such as complex integrations, disjointed data flow and fragmented security, agencies are better equipped to scale with the ever-increasing number of mobile devices.

Greater visibility into mobile infrastructure allows leaders to prioritize critical tasks, from enhancing citizen engagement to tackling more sophisticated security challenges.

Protecting Sensitive Data on Every Device

Mobile devices pose an elevated risk for agencies with personnel outside of the U.S. For example, hostile nation-states can exploit customs enforcement or airport procedures to gain unauthorized access to these devices. Furthermore, many groups have some level of access to public networks, providing them with an avenue for launching remote attacks on connected devices.

To combat this threat, the federal government has prioritized mobile security frameworks over the past few years, with guidance like CISA's Mobile Communications Best Practice Guidance, GSA's Securing Mobile Applications and Devices and NIST's Cybersecurity Framework leading the way.

Despite these efforts, mobile devices remain an overlooked attack vector. An end-to-end managed mobility services model can provide built-in security controls to proactively defend against these threats. Strong security measures—including device encryption, access controls, and real-time threat monitoring—help proactively safeguard valuable data from falling into the wrong hands, even if a device is lost.

Additionally, cloud-based platforms enable agencies to keep pace with emerging threats by automating security updates, eliminating the need for manual system adjustments and helping agencies meet regulatory requirements. Frequent updates aligned with new security guidelines will ensure agencies can efficiently manage security across their entire network.

Embracing end-to-end mobile management infrastructure enhances security and can also help agencies become more efficient. Mobile devices are central to DOD and government operations. Keeping up with evolving threats requires a solution that simplifies the complex task of managing the mobile ecosystem across multiple vendors. With the right approach, the benefits of mobile devices can continue to outweigh security concerns.

About the Author

As President of Managed Services at DMI, DJ leads the Managed Services group, overseeing its operations, growth, and strategic market positioning. His leadership is grounded in a customer-first approach, ensuring that every solution is designed to drive value. With extensive expertise in procurement, telecom expense management, and IT operations, DJ has successfully built high-performing, results driven programs that enhance operational efficiency and business growth.

DJ’s vision is centered on innovation, efficiency, and simplifying managed services in an ever-evolving digital landscape. His expertise in mobile lifecycle management, telecom expense management, IT operations, and vendor strategy, enables him to build programs that empower enterprises to optimize and scale their IT Managed Services. His ability to foster collaboration across teams, streamline processes, and implement forward-thinking strategies has positioned DMI as a trusted partner in the managed services space.

Under DJ’s leadership, DMI has reached industry-leading milestones, earning recognition as a Gartner Magic Quadrant Leader for Managed Mobility Services for eight consecutive years. DMI has also received awards, including the AOTMP Mobility Vendor of the Year and two Mobile Breakthrough Awards for Overall Mobility Management Solution Provider of the Year. These achievements highlight DMI’s commitment to innovation, service excellence, and customer satisfaction.

DJ can be reached online at https://www.linkedin.com/in/dj-oreb-4340914a/ and at our company website https://dminc.com/

Medusa Ransomware: A Growing Threat to Cybersecurity

By Ross Brewer, VP and Managing Director of Graylog

In the ever-changing world of cybersecurity, Medusa ransomware has quickly become a significant threat. As a ransomware-as-a-service (RaaS) operation, Medusa has gained attention for its sophisticated attack methods and the substantial impact it has had on various industries. This essay explores the evolution, tactics, and defence strategies against Medusa ransomware, emphasising the need for proactive cybersecurity measures.

Understanding Medusa Ransomware

Medusa ransomware first appeared in June 2021 and has since grown into a major RaaS operation. Unlike traditional ransomware, Medusa uses an affiliate-based model, allowing cybercriminals to use its tools and infrastructure in exchange for a share of the ransom payments. Medusa is known for its double-extortion tactics, where victims are not only encrypted but also threatened with data leaks if the ransom is not paid.

Medusa has targeted a wide range of industries, including healthcare, manufacturing, education, technology, government, legal, and insurance. The damage caused by Medusa's attacks is dangerously extensive, leading to operational disruptions, data breaches, financial losses, and reputational damage. Medusa's affiliates operate globally, affecting organisations across various regions. This widespread reach highlights the need for strong cybersecurity measures to protect against such threats.

The consequences of Medusa ransomware attacks are severe. Victims face significant technical failures, loss of sensitive data, financial burdens due to ransom payments, and long-term reputational damage. The ripple effects of these attacks can be felt across entire industries, underscoring the critical need for effective defence strategies. Already this year, Medusa ransomware has impacted over 300 victims from critical infrastructure sectors. The healthcare sector, in particular, has been heavily targeted, with numerous attacks leading to compromised patient data and disrupted services.

One notable attack involved the Minneapolis Public Schools, where Medusa ransomware encrypted sensitive data and demanded a substantial ransom. The impact on the school district was profound, affecting operations and compromising student information. Another significant attack targeted Compass Group, a global foodservice company. The ransomware encrypted critical systems, leading to significant business disruption and financial losses. The company's response measures included extensive cybersecurity audits and enhanced defence protocols. The healthcare sector has been a prime target for Medusa ransomware. Attacks on healthcare providers have resulted in compromised patient records, disrupted services, and increased scrutiny on cybersecurity practices. These incidents highlight the vulnerability of critical infrastructure to ransomware threats.

Evolution and Rise of Medusa RaaS

Medusa ransomware initially operated as a closed group, with all development and operations controlled by a single entity. This phase allowed the group to refine its techniques and establish a foothold in the cybercrime ecosystem. The shift to an affiliate-based model marked a significant evolution for Medusa. By allowing affiliates to conduct attacks using Medusa's tools, the group expanded its reach and increased the frequency of attacks. Centralised ransom negotiations and control remained a key feature, ensuring consistency in extortion tactics.

Medusa's hybrid approach combines affiliate-driven attacks with centralised control. This model allows for greater flexibility and scalability, enabling the group to adapt to changing cybersecurity landscapes and law enforcement crackdowns. Law enforcement efforts have disrupted several ransomware gangs, creating a void that Medusa has effectively filled. The group's ability to adapt and innovate has allowed it to maintain a strong presence despite increased scrutiny.

Medusa has developed a unique set of tools and branding that distinguishes it from other ransomware groups. This includes innovative extortion schemes, such as offering options on leak site posts, which add a layer of complexity to their operations. The frequency and impact of Medusa ransomware attacks have surged, with a 42% increase in incidents between 2023 and 2024. This rise highlights the growing threat posed by Medusa and the need for enhanced cybersecurity measures. Medusa's extortion tactics have evolved to include creative schemes, such as offering victims the option to delay data leaks by paying additional ransoms. These methods increase pressure on victims and complicate the negotiation process.

Tactics and Techniques: Medusa’s Attack Lifecycle (MITRE ATT&CK Summary)

Medusa ransomware typically gains initial access through phishing campaigns and exploiting vulnerabilities in unpatched systems. The use of Initial Access Brokers (IABs) on Dark Web forums is also common, providing a streamlined entry point for affiliates. Once inside a network, Medusa employs living-off-the-land techniques, using legitimate tools to maintain persistence and evade detection. This includes leveraging built-in utilities like PowerShell to execute commands and automate tasks.

Medusa's actors escalate privileges and move laterally within networks by exploiting vulnerabilities and using remote access tools. This allows them to gain control over additional systems and expand their reach within the target environment. To evade detection, Medusa employs techniques such as Bring Your Own Vulnerable Driver (BYOVD) attacks and obfuscated scripts. These methods disable security defences and allow the ransomware to operate undetected.

Data theft is a critical component of Medusa's operations. The group uses tools like Rclone to exfiltrate sensitive data before encrypting systems. This stolen data is then used as leverage in extortion schemes. Medusa delivers cryptographic payloads to encrypt victim systems and demand ransom payments. The impact of these attacks is significant, leading to operational disruptions and financial losses.

Strategies for Defence

Implementing a Zero Trust architecture is crucial in defending against Medusa ransomware. This approach ensures that all users and devices are continuously verified, reducing the risk of unauthorised access. Security Information and Event Management (SIEM) systems play a vital role in detecting and responding to Medusa ransomware attacks. By aggregating and analysing security data, SIEM solutions provide real-time insights into potential threats.

Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions are essential for identifying and mitigating Medusa ransomware activities. These tools offer advanced threat detection capabilities and automated response mechanisms. Educating users about the risks of phishing and other attack vectors is a key defence strategy. Regular training and awareness programmes can significantly reduce the likelihood of successful ransomware attacks.

Building resilience within the cybersecurity community and fostering collaboration among organisations is critical in combating Medusa ransomware. Sharing threat intelligence and best practices can enhance collective defence efforts. At Graylog, we are committed to providing robust cybersecurity solutions to defend against Medusa ransomware. Our advanced logging and analysis tools help organisations detect, respond to, and mitigate ransomware threats effectively.

Looking Forward

Medusa ransomware has evolved from a closed operation to a sophisticated RaaS model, impacting hundreds of organisations globally. Its innovative tactics and significant threat level underscore the importance of proactive cybersecurity measures. To stay ahead of evolving ransomware threats, organisations must prioritise proactive cybersecurity measures. This includes implementing advanced defence strategies, continuous monitoring, and regularly testing security controls.

Medusa ransomware represents a growing threat to cybersecurity, with its rapid evolution and widespread impact. By adopting comprehensive defence strategies and fostering collaboration within the cybersecurity community, we can mitigate the risks posed by this formidable adversary.

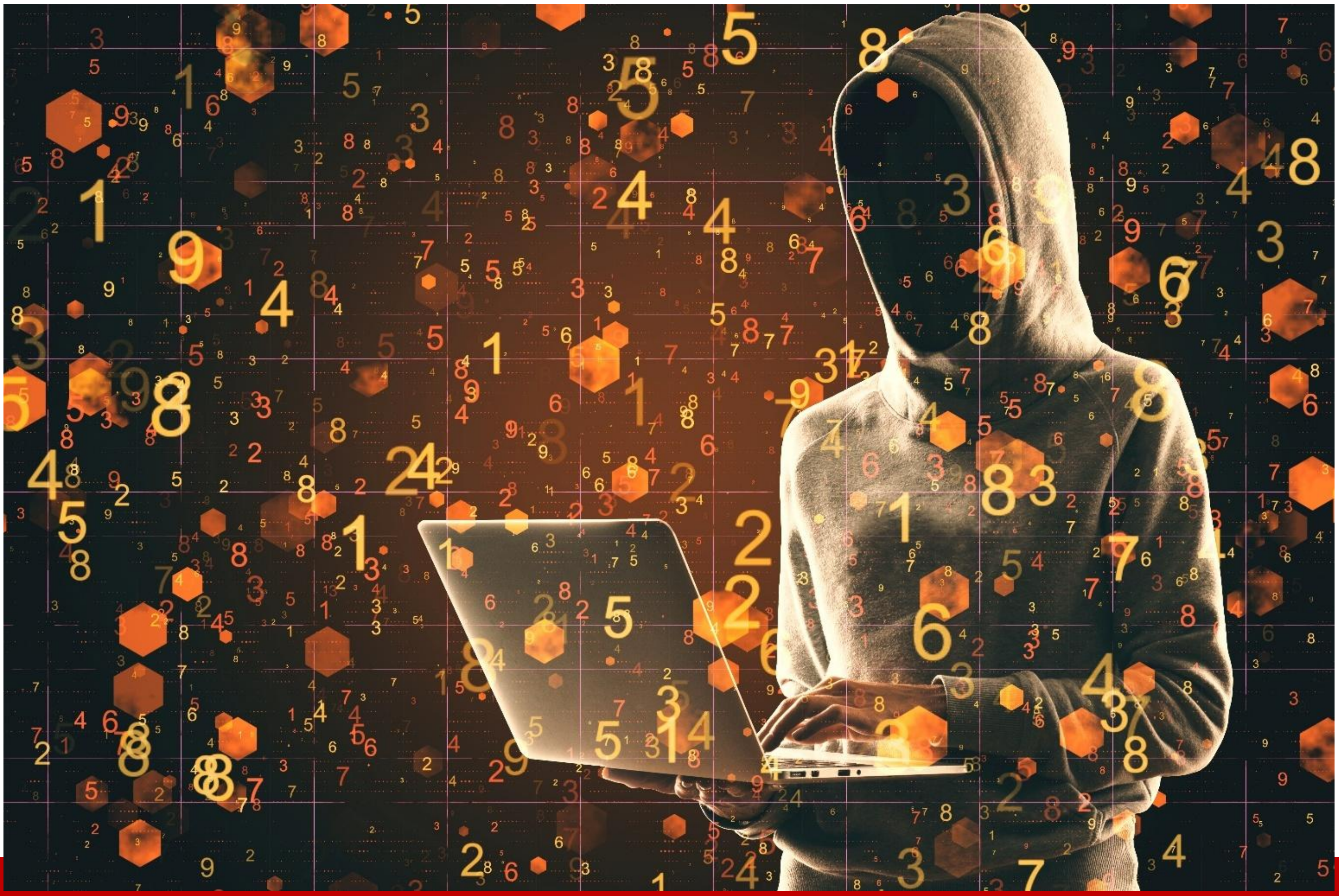
About the Author

Ross Brewer is the Vice President and Managing Director of EMEA at Graylog, a company specializing in Threat Detection & Incident Response solutions. He joined Graylog in March 2024, bringing nearly 40 years of experience in commercial and technical cybersecurity.

Before joining Graylog, Ross served as Chief Revenue Officer at SimSpace. He has also held senior leadership roles at AttackIQ, LogRhythm, and LogLogic, where he built a reputation for developing high-performance teams. His extensive experience and expertise in the cybersecurity domain make him a valuable asset to Graylog as the company continues to expand its presence in the EMEA region.

Ross is based in Graylog's London office, where he focuses on enhancing customer outcomes and accelerating development with partners. His commitment to providing tailored cybersecurity solutions aligns perfectly with Graylog's mission to offer user-friendly and affordable SIEM, Log Management, and API Security options.

Ross can be reached online at ross.brewer@graylog.com and at our company website graylog.org



The Art (and Urgency) of Securing Passwords

By Rob Vann, Chief Solutions Officer at Cyberfort

In cybersecurity, there's no shortage of discussions around the latest technological advancements such as cutting-edge biometrics, AI-powered security models, and zero-trust frameworks designed to keep attackers at bay. Yet despite these innovations, one thing remains stubbornly at the heart of digital security…passwords.

Passwords though often frustrating, easily forgotten, and sometimes dangerously simple remain the first line of defence for countless accounts and systems. Weak credentials continue to be a major factor in security breaches, with many incidents stemming from compromised passwords due to phishing, brute-force attacks, or poor password hygiene such as reuse across multiple platforms. In cybersecurity investigations, credential misuse frequently emerges as a key vulnerability, highlighting the urgent need for stronger authentication practices.

It's easy to assume that passwords should be obsolete by now, given the industry's push towards passwordless authentication and adaptive security models. However, despite these advancements, passwords continue to play a crucial role. The problem is that many organisations—and individuals—fail to manage them properly. Weak passwords remain a major vulnerability, contributing to a significant percentage of security incidents worldwide.

The Evolution of Password Security

Cybersecurity professionals understand that passwords alone aren’t enough to secure systems effectively. That’s why the industry has increasingly embraced passwordless authentication, prioritising methods such as FIDO2/WebAuthn, biometric logins, and Single Sign-On (SSO). These approaches reduce reliance on traditional passwords, creating a more seamless and secure login experience.

At the same time, authentication is becoming smarter, adapting to the behaviour of users through adaptive authentication. This method analyses factors like login patterns, geographic location, and the type of device being used. If an unusual attempt is detected—such as a login request from an unrecognised device or location—the system triggers additional verification steps.

These advancements highlight the need for a security model that relies on more than just passwords. While they remain an essential component, they must be reinforced with additional layers of protection to withstand increasingly sophisticated attacks.

The Anatomy of a Strong Password

Security professionals assess password strength based on several key characteristics. Entropy, or the degree of randomness and unpredictability, plays a vital role in ensuring passwords are resistant to attacks. A strong password should also be sufficiently long and complex, incorporating uppercase and lowercase letters, numbers, and symbols to make it more difficult to crack.

Uniqueness is just as important, as reusing the same password across multiple accounts dramatically increases risk. If an attacker manages to breach one account, they could easily exploit the same credentials to gain access to others. Additionally, passwords need to be resilient to common attack methods, such as brute-force attempts, dictionary-based guessing, and large-scale credential stuffing campaigns.

Despite repeated warnings from security experts, poor password management remains widespread. Weak passwords like "admin123" and "password" continue to be used by individuals and organisations alike, and many users still fall into the habit of recycling passwords across multiple platforms. Studies show that an alarming 65% of people reuse passwords, allowing attackers to escalate a single breach into a full-scale compromise.

Strengthening Password Security

To mitigate the risks associated with weak passwords, cybersecurity experts advocate for additional security measures. Multi-Factor Authentication (MFA) is one of the most effective solutions, adding an extra layer of verification beyond the password itself. Even if a cybercriminal obtains login credentials, MFA requires them to pass an additional check, whether through biometrics, security tokens, or one-time passcodes. Although attackers have developed methods to bypass MFA, it remains one of the strongest tools available.

Another emerging approach is passwordless authentication, which eliminates the need for passwords entirely. Technologies such as WebAuthn and biometric identification ensure that login credentials cannot be stolen or exploited in the traditional sense. Additionally, zero trust security models are gaining traction, shifting the perspective that credentials should automatically be trusted. Instead, they require continuous verification to ensure that the user and device meet strict security conditions before granting access.

At Cyberfort, password security is treated as part of a broader identity and access management (IAM) strategy. This means implementing strong password policies, conducting regular security audits, integrating password managers, and actively monitoring leaked credentials on the dark web to ensure compromised passwords are flagged before they can be exploited.

Best Practices for Password Security

Improving password security requires a proactive approach. Experts recommend using passwords that are at least 16 characters long, combining uppercase and lowercase letters, numbers, and symbols to increase complexity. Common words, predictable phrases, and personal information should always be avoided, as attackers frequently leverage social engineering techniques to guess passwords.

Passphrases, which consist of a string of words or phrases, can serve as a practical alternative. For example, a passphrase like “GrumpyTigers!Chase42Birds” balances memorability with security. Using a password manager such as Bitwarden, 1Password, or Keeper can also alleviate the burden of remembering multiple complex passwords while ensuring credentials are stored securely.

For organisations, security must extend beyond individual user behaviour. Implementing enterprise-grade vaulting technologies, enforcing least privilege access policies, and continuously monitoring privileged account usage can prevent insider threats and credential abuse. Password storage methods should incorporate strong hashing algorithms such as bcrypt, scrypt, or Argon2, with additional safeguards like salting and peppering to prevent attackers from cracking large sets of credentials.

The Future of Password Security

As cybersecurity threats evolve, the approach to password security must adapt accordingly. The rise of passwordless authentication, adaptive security, and zero trust models demonstrates the growing need for more sophisticated protection mechanisms. However, as long as passwords remain in use, they must be managed with care and secured effectively.

By combining strong password practices with MFA, intelligent access management, and continuous monitoring, organisations can significantly reduce their vulnerability to attacks. Cyber threats will continue to advance, but so must our defences.

Whether you're securing personal accounts or overseeing cybersecurity at a global enterprise, adopting modern password security principles is no longer just advisable, it is essential.

About the Author

Rob Vann is the Chief Solutions Officer at Cyberfort, bringing over 35 years of experience in cloud security and managed services. He has successfully led cybersecurity initiatives across various industries, including large corporations, telecommunications, and government sectors. Vann has played a key role in developing managed security services, scaling businesses to revenues exceeding £50 million per year.

Rob can be reached online through his LinkedIn and at our company website cyberfort.com

Beyond Firewalls: The CISO’s Path to Enterprise-Wide Cyber Resilience

How security leaders can move from traditional defenses to holistic, adaptive strategies that withstand real-world threats

By Diego Neuber, CISO and Founder, Disatech

Cybersecurity is no longer just about preventing breaches — it’s about surviving them.

In a world of constant digital acceleration and evolving adversaries, CISOs can no longer afford to rely solely on traditional perimeter defenses. Firewalls, endpoint protection, and patching are still necessary — but they are no longer sufficient.

The modern enterprise must prepare to operate under threat, recover quickly from compromise, and continue delivering value even under attack. This is the essence of cyber resilience — and it’s time we treat it as a first-class objective.

Many security programs are still built on reactive models: detect, respond, recover. But the velocity and sophistication of attacks have outpaced this paradigm.

Instead, resilient organizations assume breach, implement defense-in-depth, and integrate security into the very fabric of business operations. This means planning for degradation, practicing containment, and ensuring continuity across IT and OT environments.

A resilient posture is not just about technology — it's about culture, governance, and architecture.

In my 14+ years of working with organizations across sectors — from logistics and retail to financial services — I've seen firsthand what works and what doesn't.

One client suffered a ransomware attack that bypassed their endpoint controls. But because we had implemented VLAN-based segmentation, offline backups, and privilege restriction policies, the impact was contained to a single subnet. Recovery took hours, not days. That's resilience in action.

In another case, we introduced a simulated failure drill — a "cyberfire drill" — where teams had to recover from a fake intrusion. The outcome was eye-opening: gaps in incident communication, delays in privilege revocation, and over-reliance on specific personnel. Fixing these not only improved preparedness, but created a stronger security culture.

Core Pillars of Cyber Resilience

1. **Segmentation and Containment**
   Don't let attackers pivot freely once inside. Use VLANs, zero trust principles, and identity boundaries to limit lateral movement.

2. **Data-Centric Security**
   Protect data at rest, in transit, and in use. Classify assets, encrypt strategically, and implement robust access controls.

3. **Incident Preparedness**
   Have a tested, documented, and rehearsed incident response plan. Involve legal, PR, HR, and executives — not just IT.

4. **Business Continuity Integration**
   Ensure that IT disaster recovery aligns with business continuity. Have offline backups. Test failover scenarios regularly.

5. **Culture and Awareness**
   Train employees not just to avoid phishing, but to escalate concerns. Build a no-blame reporting environment.

Cyber resilience is not just a security goal — it's a business enabler.

Board members no longer ask "are we protected?" — they ask "how quickly can we recover?" CISOs who speak the language of risk, resilience, and continuity gain credibility and influence in the boardroom.

Moreover, regulations such as DORA (EU), NIS2, and evolving US cybersecurity mandates are increasingly emphasizing resilience over strict compliance.

Firewalls will always matter. But they're no longer the center of the story.

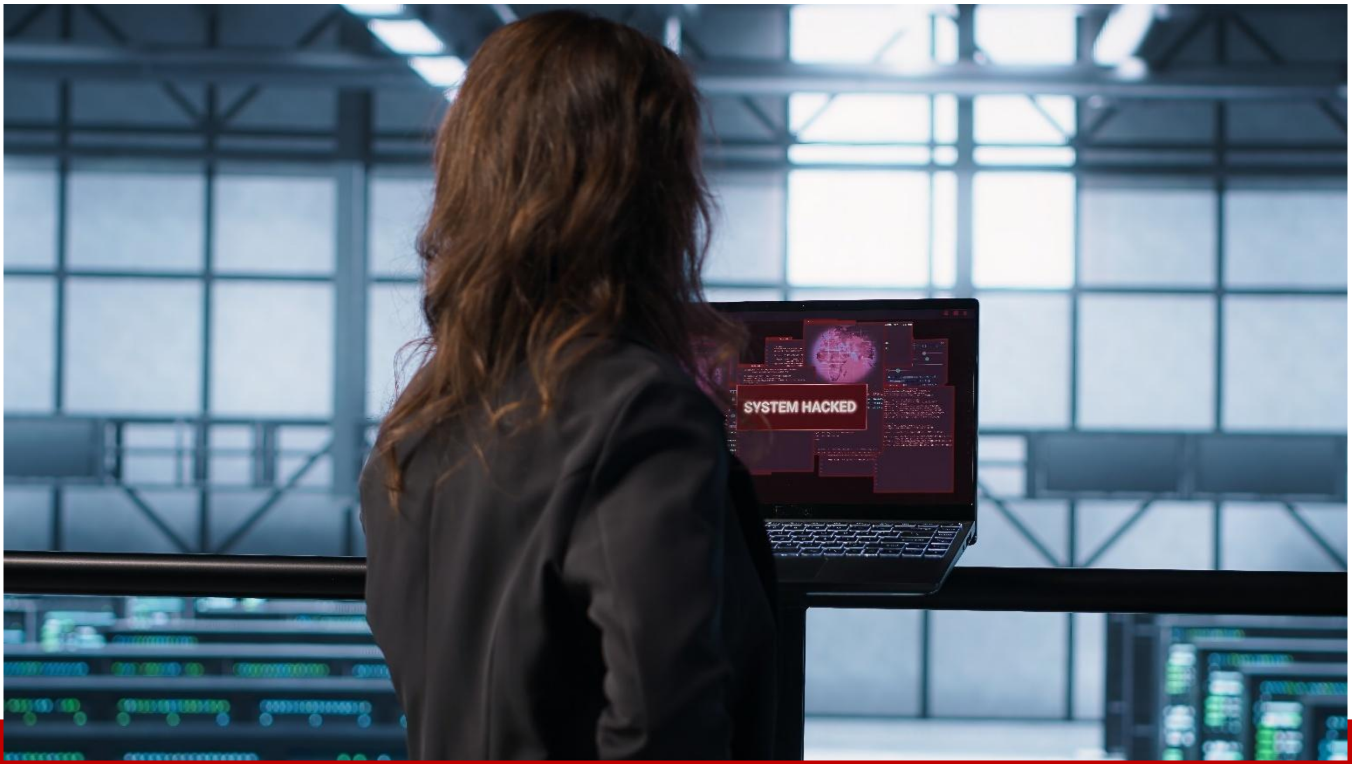
CISOs must lead the way toward adaptive, risk-informed architectures that empower the business to operate — even during disruption. This is the future of cybersecurity: not just defense, but endurance.

The time to act is now. Resilience isn't just a response to today's threats — it's a commitment to tomorrow's continuity.

About the Author

Diego Neuber is a seasoned cybersecurity analyst and the founder of Disatech, a Brazilian company specializing in IT security, training, audits, and secure infrastructure solutions. With over 14 years of experience, he currently serves as CISO for multiple organizations and is a senior member of IEEE. Diego is also a 2025 judge for the Globee® Cybersecurity Awards and is launching Sec4Tech, a cybersecurity venture in the United States.

Diego can be reached at diego@disatech.com.br, your Linkedin https://www.linkedin.com/in/diego-neuber-3484972b/ and through his company website: https://www.disatech.com.br



Combating Cloud Security Threats Leveraging AI Agents

By Nivathan Athiganoor Somasundharam, Technical Account Manager, Teleport

Today, every company has invested in one or more Cloud Security Posture Management (CSPM) tools, such as Wiz, Orca, or Palo Alto Cortex. [1] The CSPM platforms are designed to identify vulnerabilities and misconfigurations across the cloud environments. However, CSPM tools are flooded with numerous alerts and misconfigurations, often numbering in hundreds or thousands. [2]

Additionally, there is a significant shortage of skills and engineers who can understand these alerts and effectively triage them. This exacerbates alert fatigue, as security and infrastructure teams are overwhelmed with alerts and misconfigurations. In some cases, the alerts and misconfigurations remain unresolved for an extended period.

The Complexity of Cloud Infrastructure

Modern cloud infrastructure is highly complex today. Understanding the intricacies of an enterprise's cloud infrastructure landscape is increasingly challenging for engineers. Enterprises no longer run workloads on a single cloud; instead, they run workloads across multiple clouds, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. According to Flexera's 2024 State of Cloud Report, 87% of companies employ a multicloud strategy. [3]

This distribution of workloads makes it more complicated for a security engineer to triage on this issue. In some organizations, the team responsible for the infrastructure should take ownership of triaging these issues. However, the developer typically lacks the knowledge of the infrastructure and the tools like Terraform. This disconnect between alert ownership and remediation capability creates the delay in responding to those alerts and the risk of security breaches. These issues must be resolved as soon as possible to prevent any breaches or cyberattacks.

The Need for Scalable Remediation

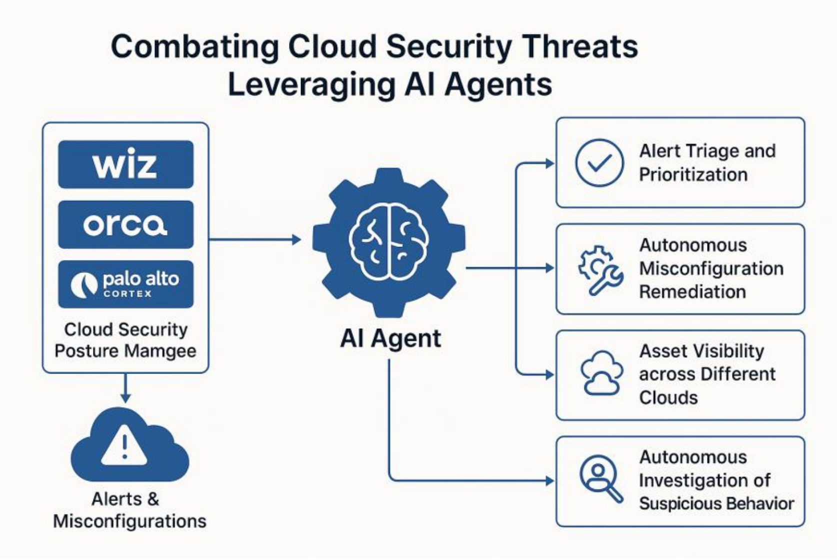
The constantly growing volume of alerts and the complexity of the infrastructure raise a fundamental question: How can organizations or enterprises remediate these issues in a timely and scalable manner?

The latest advancements in Artificial Intelligence and Large Language models offer a more effective solution. Leveraging AI agents and integrating them into security workflows to help triage, prioritize, and even autonomously remediate cloud misconfigurations will be the most effective way to address the challenge of remediation at scale. [4]

What is an AI Agent?

An AI agent is an intelligent system capable of perceiving the context for different data sources like alerts and cloud configurations, making decisions based on the context, and taking action to remediate the issue. These agents should be able to analyze the logs and configurations and make the necessary changes to fix these issues, such as modifying the Terraform code and opening a pull request. [5]

Use Cases for AI Agents in Cloud Security


Combating Cloud Security Threats
Leveraging AI Agents
wiz
orca
palo alto CORTEX
Cloud Security Posture Mamgee
Alerts & Misconfigurations
AI Agent
Alert Triage and Prioritization
Autonomous Misconfiguration Remediation
Asset Visibility across Different Clouds
Autonomous Investigation of Suspicious Behavior

1. Alert Triage and Prioritization

AI agents can analyze the context of the alerts generated by CSPM tools and prioritize high-risk alerts while deprioritizing trivial ones.

Example: If an S3 bucket is flagged for being public. The AI agent can deprioritize the alert since this bucket belongs to the Red team test account, or prioritize it because it belongs to the production environments. [6]

2. Autonomous Misconfiguration Remediation

Rather than a security engineer chasing the developer who owns the infrastructure, the AI agents should locate the code for the infrastructure to make changes in the cloud.

Example: If a new EC2 instance is spun up with port 22 open to the Internet (0.0.0.0/0), the AI agent can locate the code for the EC2 instance configurations and make the necessary changes to remove the rule, creating a pull request (PR) for the changes. [7]

3. Asset Visibility across different clouds

Security teams and DevSecOps teams often struggle with fragmented visibility across cloud environments. AI agents can aggregate data from all cloud providers, serving as a single point of contact.

Example: An engineer can ask the AI agent to list all unencrypted EBS volumes with specific filter tags and receive a comprehensive report. [5]

4. Autonomous investigation of suspicious behavior

AI agents can correlate information from two different systems, such as Endpoint Detection and Remediation (EDR) and Cloud Security Posture Management (CSPM) platforms, and take action based on the perceived information.

Example: If an unusual SSH login pattern is detected on a critical server, the AI agents can correlate the endpoint telemetry, isolate the user's device, and lock it for investigation. [3]

Conclusion

The cloud threat landscape is becoming increasingly sophisticated, and security teams are struggling to keep up with the volume of alerts. AI agents offer a new paradigm in remediating cloud security by automating and accelerating tedious remediation by bringing contextual understanding to complex environments.

The agents are not designed to replace engineers, but to augment their capabilities. By integrating AI into security operations, this organization can reduce risk and the time required to remediate these issues. As cloud environments continue to evolve, AI agents will be essential in helping security teams to combat cloud security threats.

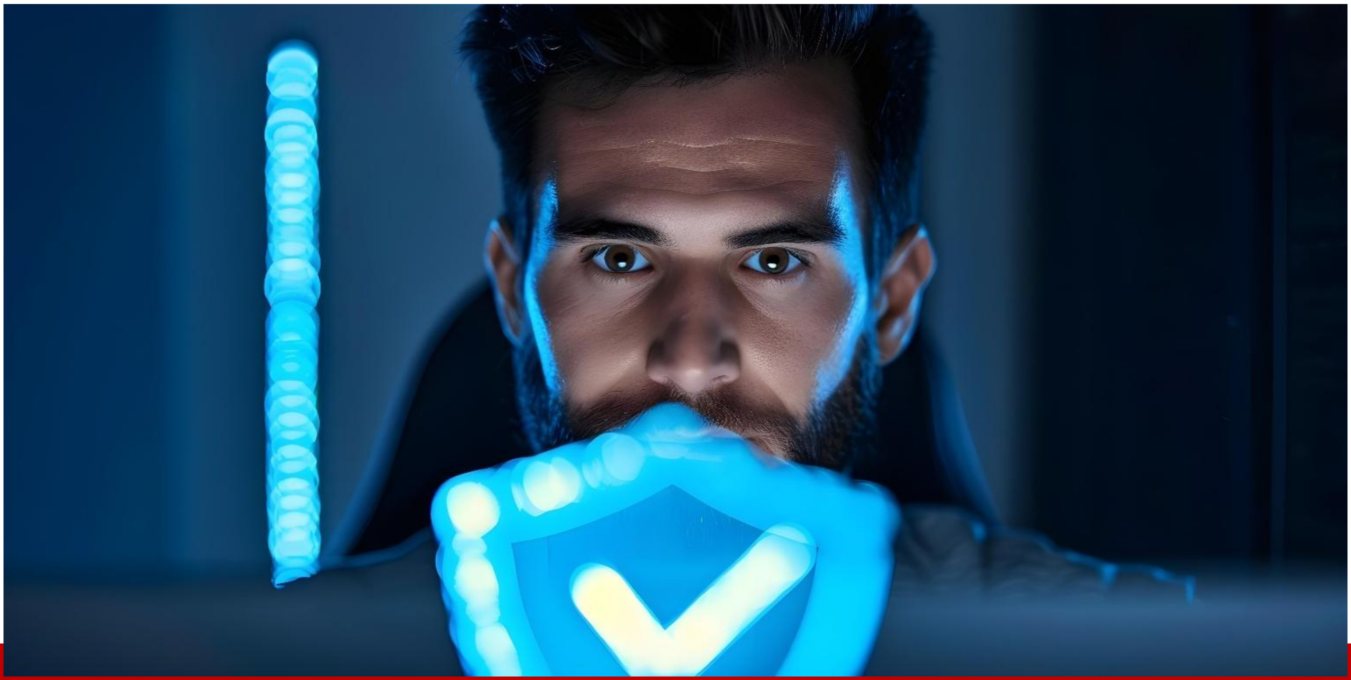
References

[1] Palo Alto Networks – Cortex XDR and CSPM – https://www.paloaltonetworks.com/cortex
[2] Gartner – Cloud Security Alert Fatigue Projections – https://www.gartner.com/en/newsroom/press-releases
[3] Flexera 2024 State of the Cloud Report – https://info.flexera.com/CM-REPORT-State-of-the-Cloud
[4] NIST AI Risk Management Framework – https://www.nist.gov/itl/ai-risk-management-framework
[5] GitHub – Cloud Security Topics – https://github.com/topics/cloud-security
[6] Wiz Security Blog – https://www.wiz.io/blog
[7] Orca Security Resources – https://orca.security/resources

About the Author

Nivathan Athiganoor Somasundharam is a Technical Account Manager at Gravitational Inc. DBA Teleport. He specializes in Zero Trust implementation, identity security, and DevSecOps. He holds a degree in Computer Science from Texas A&M University (Texas, USA) and has extensive experience working with cloud providers, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

An active contributor to the cybersecurity community, Nivathan shares his expertise through Articles, webinars, and conferences, with a strong focus on identity threat detection and response (ITDR) and cloud infrastructure security. He is also a key contributor to the open-source VMware Carbon Black Harbor Adapter project. Nivathan can be reached at his profile on linkedin



Cybersecurity Starts with Behavior

Why Culture Is the Strongest Defense

By Yongmei Concepcion, Project Management Professional

What’s the first thing you do when you receive a suspicious email—click, delete, or report it? That moment says more about your organization's cybersecurity than any firewall could. Cybersecurity isn’t just a technology problem—it’s a human one. And the key to defending against threats often lies in everyday behaviors, both in and out of the office.

We tend to think cybersecurity starts with a tool—an antivirus, a firewall, or maybe a password policy. But if we’re honest, most cyberattacks succeed not because the tech failed but because someone got tricked into clicking something they shouldn’t have. We'll never build absolute security if we don’t address how people think and act.

While many companies invest in tools and training, they overlook something vital: how people behave daily. If someone uses weak passwords at home, ignores software updates, or overshares on social media, those habits will likely follow them into the workplace. Security doesn’t switch on when you enter the office, it’s a mindset shaped by consistency. They’re built over time—in how we manage our home networks, how we treat our devices, and whether we stop to think before clicking links on our personal email. If someone uses the same password for Netflix and work email, that’s a problem. But it’s also a teachable moment.

So how do we get there? Start small. Make cybersecurity personal. Instead of throwing jargon at employees, show them how secure habits help them protect their kids, bank accounts, or weekend vacation bookings. Offer tools and tips they can use outside of work—things like parental controls, phishing test emails, or password managers they can install at home. Once people feel the value in their everyday lives, they'll naturally carry those habits into the workplace.

And let's be real: no one remembers that hour-long training three months ago. People remember stories. They remember when their colleague caught a phishing scam, or the company held a "hack me if you can" day with prizes.

Leaders are key. Employees watch what leadership does more than what they say. So, if executives skip security training or reuse passwords, others will, too. However, it shifts the tone if leaders talk about security in town halls, recognize those who report incidents, and set clear expectations.

At the end of the day, a strong cybersecurity culture isn't about scaring people into compliance. It's about inviting them into the process. It's about saying, "You matter in this." Because when employees feel informed, valued, and empowered, security becomes second nature. That's how you go from hoping people do the right thing to knowing they will.

About the Author

Yongmei Concepcion, a Project Management Professional (PMP), recently graduated summa cum laude from Purdue University Global with a Bachelor of Science in Cybersecurity and Information Technology. As a military spouse, she is currently stationed with her husband in San Antonio, Texas. Prior to her marriage, she owned and operated children's playgrounds and a car-themed cafe. Now, she is pursuing a career in the rapidly expanding fields of cybersecurity and artificial intelligence. Yongmei can be reached at Yongmei.Concepcion@gmail.com.

AI, Deepfakes, and the War on Truth: Strengthening Emotional Firewalls in the Age of Manipulation

The Hidden Breach: When Emotion Becomes the Weakest Link

By Nadja El Fertasi, Founder, Thrive with EQ

It was 2008, and I was preparing to deploy to Afghanistan with NATO. The ISAF base was often on high alert—not because of technical intrusions, but because people were being manipulated. Skilled social engineers didn't need to breach a firewall; they simply breached trust. By exploiting emotions like fear, urgency, or loneliness, they accessed what even the best encryption couldn't protect—human decision-making.

What we once called "soft skills" proved to be the **hardest reality** in security.

Our training shifted: verify assumptions, question every narrative, and above all, understand your own emotional triggers. Emotional intelligence became as critical as situational awareness.

Fast forward to today: A financial employee wires millions to fraudsters after a deepfake video call from a fake CFO (CNN). The breach wasn't technical—it was emotional. This isn't science fiction. It's already happening. Our new battleground is not just digital—it's **psychological**. And yet we keep trying to fight emotional threats with technical tools alone.

The Evolution of Deception

A year ago, you might've spotted a deepfake with a closer look. Now, it's almost impossible. The pace of AI development has taken deception to an industrial scale.

From Europol to the FBI, the message is the same: Deepfakes, voice clones, and AI-generated personas are turning trust into a vulnerability. And these tactics don't target your network—they target your people.

Fake presidential speeches. Synthetic voices mimicking loved ones. AI-generated messages fine-tuned to trigger a sense of urgency or fear. These aren't edge cases anymore. They're the **new normal**.

What's changing isn't just the toolset. It's the **nature of the threat**.

Where Traditional Security Fails

Most cybersecurity frameworks are built around technical infrastructure. But attackers are bypassing the network and going straight to the human. Traditional defenses don't stop someone from clicking a link when they're scared or replying to a scam when they're under pressure.

Business Email Compromise scams, social engineering, and romance fraud are still raking in billions—not because our tech is broken, but because we continue to overlook the **emotional layer** of risk.

The "last mile" problem in cybersecurity has always been human. And when that human is overworked, unsupported, or afraid, they're the easiest point of entry - the path of least resistance to your data.

Emotional Manipulation at Scale

AI doesn't just generate fake content. It generates **emotionally targeted content**.

By harvesting data from our digital behaviour—likes, searches, habits—it creates a blueprint of our emotional triggers. Then it weaponizes them. (WIRED)

Emotionally resonant phishing. Deepfake voicemails from your CEO. Tailored misinformation campaigns designed to confuse, exhaust, and divide. What we're facing is not just disinformation. It's **disorientation**.

In NATO, I saw first-hand how cultural awareness and emotional resilience were essential during civil-military exercises—especially when cyber became an operational domain. Understanding emotion wasn't optional. It was strategic.

Today, the same principle applies to every cybersecurity team on the planet.

The Case for Emotional Firewalls

We need to stop treating emotional intelligence as a soft add-on. It's not. It's a **critical security skillset**.

Emotional firewalls are the psychological and cultural reflexes that help people pause before reacting, question before complying, and think clearly under stress. These aren't buzzwords—they're real capabilities built through deliberate practice and training.

Emotional intelligence frameworks provide the structure for developing these capacities. During my time leading within NATO's high-pressure environment, I used emotional intelligence as a foundational approach to manage ambiguity, pressure, and emotionally charged crises. It helped me stay grounded—and helped others around me do the same.

Because no firewall can stop a breach that comes through someone's emotions—unless that person knows how to spot it.

Integrating EQ into the Cyber Stack

Cybersecurity is no longer just a technical responsibility. It's a **leadership advantage**.

The cost of emotional manipulation is real: financial loss, reputational damage, team burnout, and disrupted operations. But when leaders invest in emotional intelligence, they don't just prevent incidents—they build **resilience across the board**.

Here's how it starts:

- **Emotionally-Aware Phishing Simulations** – Go beyond trick questions. Teach people to recognize the emotional tactics behind the message.
- **Scenario-Based Exercises** – Simulate stress, urgency, and uncertainty—so teams build real emotional reflexes, not just theoretical knowledge.
- **Resilience Coaching for Teams** – Give people a toolkit for navigating pressure, staying grounded, and making sound decisions under fire.

This is behaviour-driven cybersecurity. It doesn't replace your stack. It strengthens it.

The Future of Trust in the Age of AI

In a world where deepfakes can mimic anyone, trust is your most valuable asset—and your most vulnerable one.

The future of cyber defense won't be built on tools alone. It will be built on people who know how to think clearly when others are trying to make them panic. On leaders who prioritize culture, awareness, and resilience. On organizations that protect not just data, but **decision-making itself**.

Emotional intelligence isn't a luxury. It's a leadership skill, a security layer, and a competitive advantage.

Moving Forward with Emotional Intelligence

This is not just a call to CISOs. It's a call to **every leader** navigating the complexities of the digital age.

In this new era, your leadership isn't just measured by strategy or delivery—it's measured by how well you understand the emotional terrain your people are walking through. Burnout, fear, uncertainty, disinformation—these are not technical issues. They are human ones.

And they don't stay at work. They follow us home. They affect our families, our communities, and our ability to trust what we see and hear.

This is a new kind of leadership—one rooted in **clarity, empathy, and courage**.

Start with yourself. Develop emotional self-awareness. Create cultures where it's safe to speak up, to slow down, to think critically. Empower your teams to lead from the inside out.

If AI is accelerating the war on truth, then emotional intelligence is our way forward—toward resilience, toward trust, and toward a future where humanity leads the technology, not the other way around.

About the Author

Nadja El Fertasi is the Founder of Thrive with EQ.

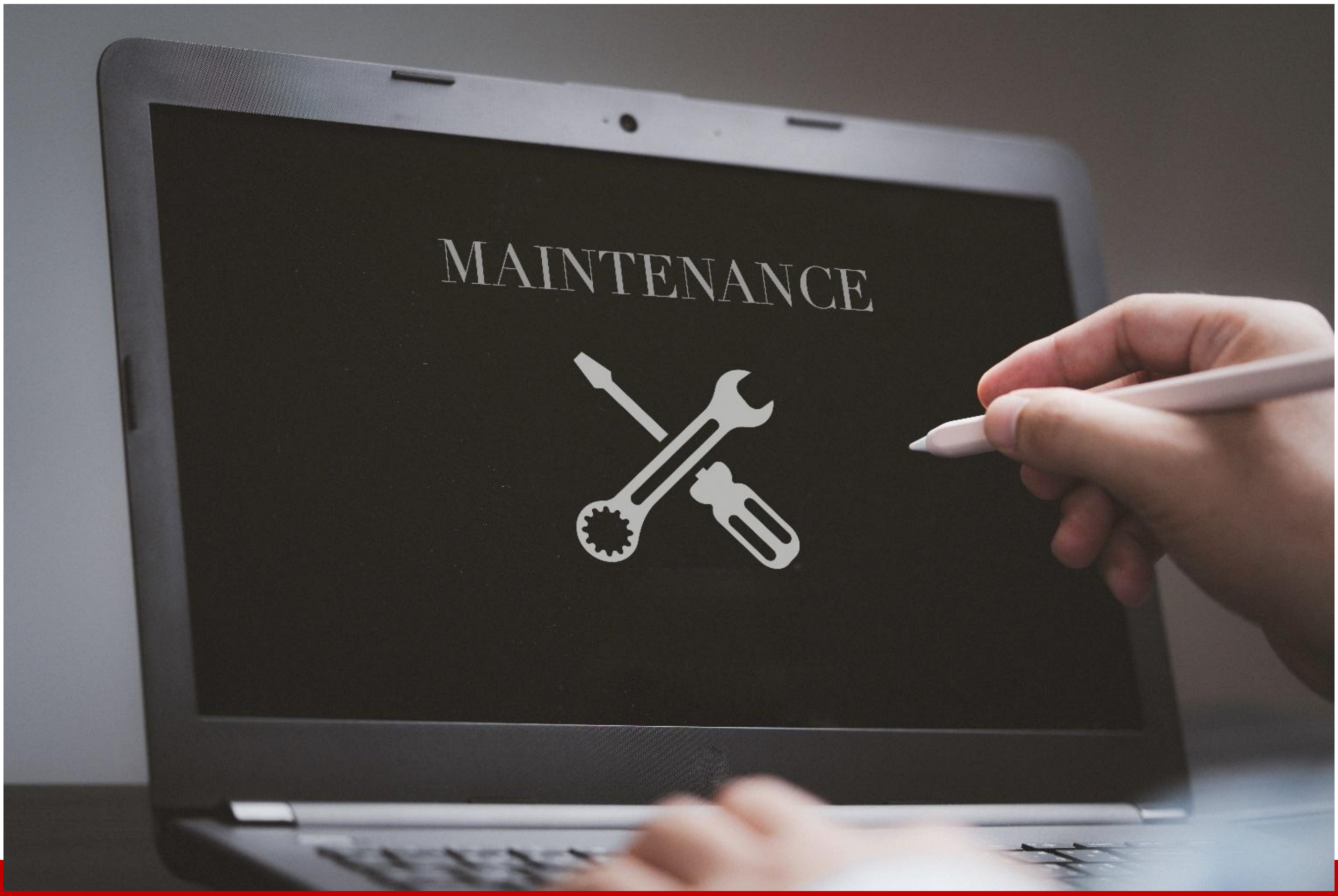
Nadja is a former senior NATO executive with nearly 20 years of experience advancing digital transformation, crisis leadership, and institutional resilience across 40+ nations.

At NATO's Communications and Information Agency, Nadja led high-impact initiatives that integrated secure cloud collaboration and multidisciplinary teams, always focusing on the human dimension of technology.

Nadja created the *Emotional Firewalls* framework to help leaders build emotional intelligence as a strategic defense against AI-driven manipulation and cyber threats.

As a global speaker and recognized thought leader, Nadja empowers organizations to lead with emotional agility and digital trust in a world where resilience is not optional — it's operational.

Nadja El Fertasi can be reached online at nadja@thrivewitheq.com, on LinkedIn: Nadja El Fertasi and at thrivewitheq.com.



Deferred Maintenance

A Hidden Opportunity in Quantifying Risk in IT

By John Kupcinski, CISO, PSEG Long Island

In traditional asset management, deferred maintenance (DM) is a well-established concept under Generally Accepted Accounting Principles (GAAP). It represents the cost of postponed repairs or replacements for physical assets such as elevators, lighting, and HVAC systems. Neglecting scheduled maintenance can reduce an asset's value and utility, impacting critical financial metrics like Operating Efficiency, Return on Assets (ROA), and Liquidity Ratios. Organizations often disclose deferred maintenance costs in financial statements, highlighting the estimated costs, affected assets, and risks of further deferral, such as operational disruptions or compliance violations.

An Overlooked Opportunity

Deferred maintenance also poses significant risks to IT systems, where the stakes are even higher due to rapid obsolescence, intricate interdependencies, and regulatory pressures. Unlike physical assets like buildings or HVAC systems, IT assets can quickly become obsolete or non-compliant, leading to severe consequences such as cyber breaches, system downtime, or regulatory fines. Despite these complexities, organizations can calculate deferred maintenance for IT systems through a structured approach tailored to their unique characteristics.

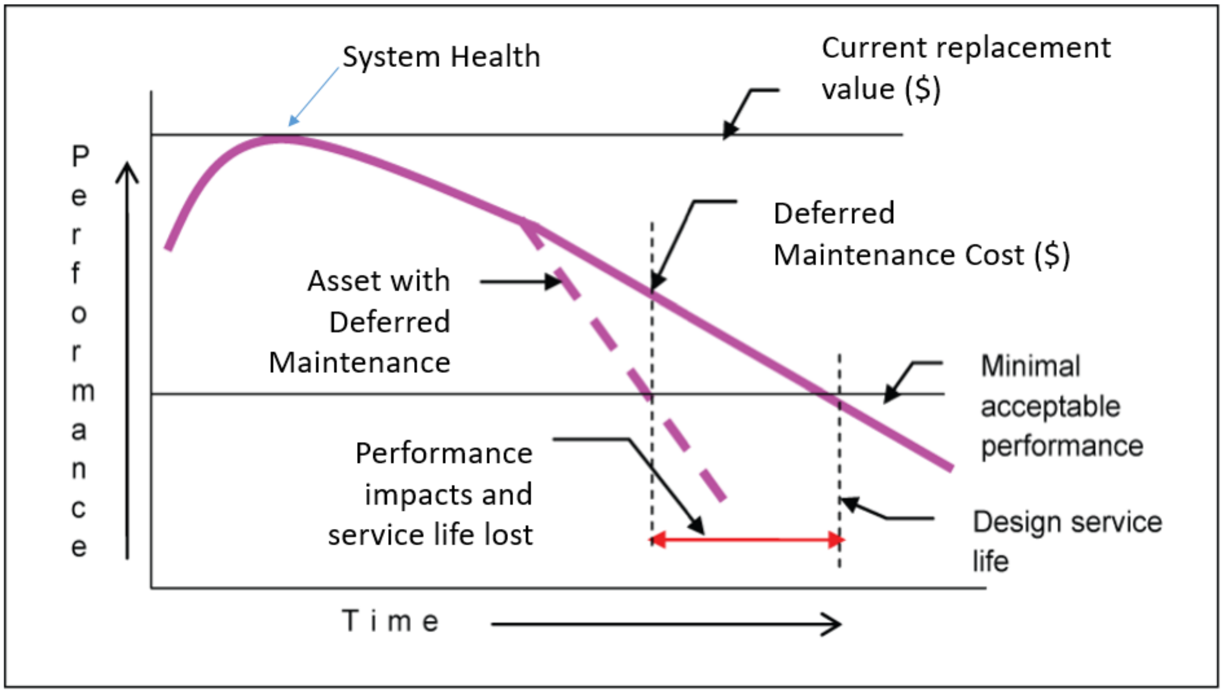

System Health
Current replacement value ($)
Performance
Deferred Maintenance Cost ($)
Asset with Deferred Maintenance
Minimal acceptable performance
Performance impacts and service life lost
Design service life
Time

Figure 1: Effect of Deferred maintenance on Asset Service

To assess an *IT system deferred maintenance*, organizations can use their existing asset inventory (CMDB) and combined with procurement & contract data to create a model that calculates an IT System Condition Index as well as Current Replacement Values (CRV). Estimating deferred maintenance costs for IT systems involves evaluating asset condition, estimating required resources for updates or repairs, and calculating the cost of delayed maintenance actions. The resulting Deferred Maintenance Cost (DMC) includes postponed tasks like hardware upgrades, software patches, and security updates. Note this data can change frequently, and regular reviews and data verification are essential to maintain accuracy and support the integrity of the assessment.

Unique Challenges of Deferred Maintenance in IT Systems

Calculating deferred maintenance for IT systems is inherently more complex than for traditional physical assets. The interconnected nature of IT systems means deferred maintenance in one layer (e.g., infrastructure) can cascade into failures across other layers (e.g., platforms or applications). Additionally, IT systems often become obsolete within a few years, requiring continuous updates and replacements. Unlike physical assets with predictable maintenance, IT maintenance costs grow logarithmically with scale (e.g. the cost of patching ten servers is less than 10x the cost of patching one server due to economies of scale & automation). As the need for maintenance on these systems expands, the costs of managing dependencies and addressing cascading issues increase significantly. Deferred maintenance can also lead to non-compliance with regulations like SOX, PCI DSS, or HIPAA, resulting in fines, legal liabilities, and reputational harm which should also be factored into the assessment.

Further complicating matters, IT operates in diverse environments—including cloud, on-premises, hybrid, and SaaS setups—each with unique deferred maintenance challenges shaped by shared responsibility models. Accurately tracking deferred maintenance costs requires accounting for overlapping responsibilities between cloud providers and third-party hosted applications.

The Business Case for Calculating Deferred Maintenance in IT

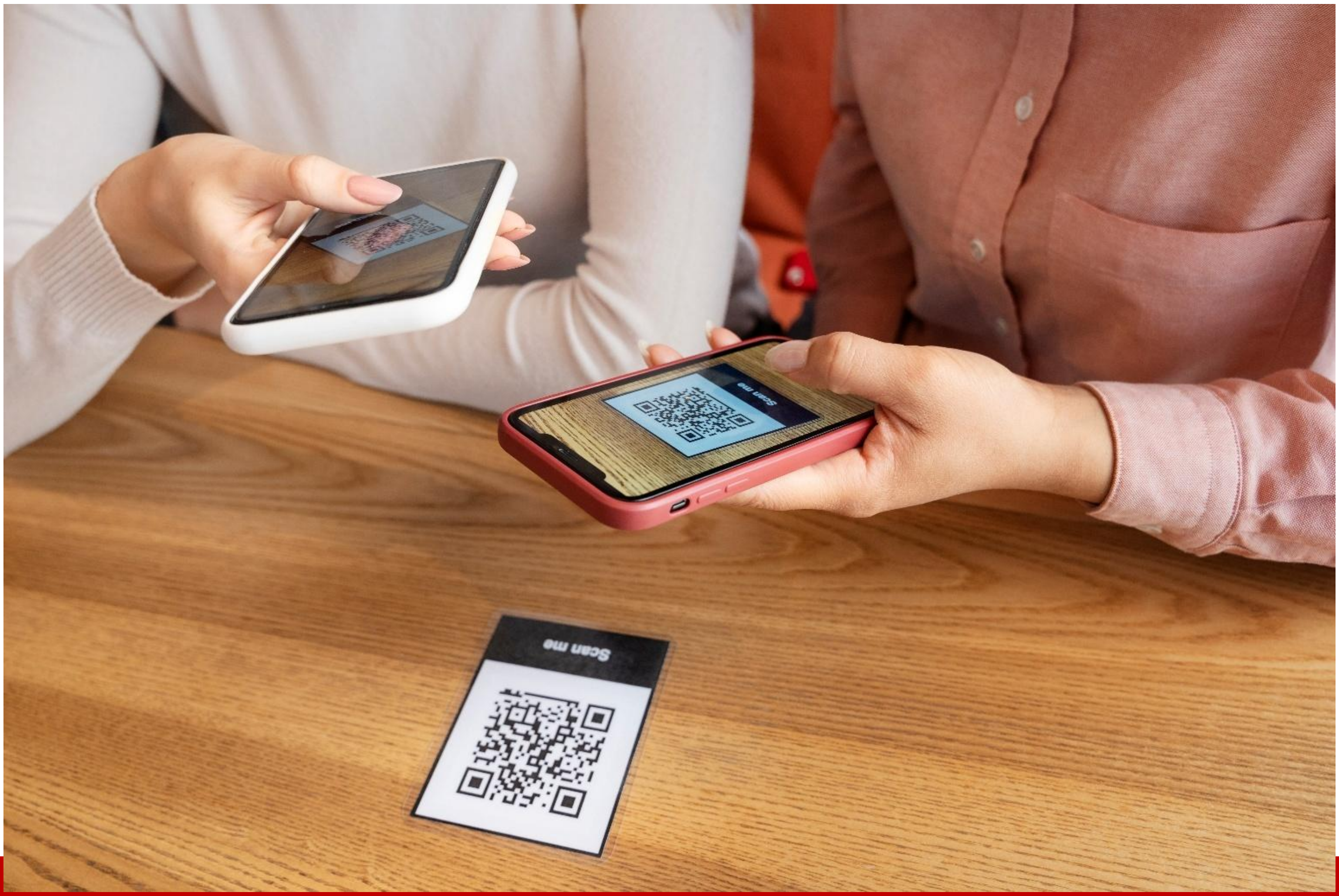
Despite these challenges, quantifying deferred maintenance for IT systems yields substantial benefits. It enables organizations to estimate future IT costs, prioritize investments, and mitigate risks related to asset impairment and regulatory non-compliance. Accurate calculations inform both operational (OPEX) and capital (CAPEX) budget forecasts. Metrics like the Replacement Value can support informed decision-making. Proactively addressing deferred maintenance reduces the likelihood of asset impairment, compliance violations, and cascading failures, protecting both financial performance and operational stability.

The unique challenges of assessing deferred maintenance in IT (e.g. rapid obsolescence, complex interdependencies, etc.) demand a tailored approach. Organizations can mitigate these challenges by implementing a program which includes processes to calculate fields. Ultimately having this data will provide organizations additional reference points to assist in prioritizing investments, navigating regulatory requirements, and maintaining a more secure, compliant, and efficient IT infrastructure.

About the Author

John Kupcinski is the Chief Information Security Officer (CISO) of the PSEG Long Island. He is a recognized cybersecurity executive and trusted leader in highly regulated industries with over 2 decades of experience designing and executing enterprise-wide information security programs.

John's expertise spans incident response, Security Operations, vulnerability management, identity and access management, and cloud security, with a proven track record of aligning cyber initiatives with organizational objectives. Throughout his career, John has held leadership roles at FreddieMac, KPMG, and IMF where he supported complex cybersecurity programs. He is passionate about advancing the cybersecurity field through strategic leadership, innovation, and workforce development. John can be reached online at https://www.linkedin.com/in/john-kupcinski-17985618



Awash In QR Codes, Bad Actors Are Pirating their Popularity

Once dismissed as a tech gimmick, QR codes are now a powerful tool—and a growing cybersecurity threat too often flying under the radar.

By Usman Choudhary, General Manager, VIPRE Security Group

QR (quick response) codes are no longer a novelty or a marketing cliche that faced a recent near-death experience. Instead, they have returned from the near grave as an excellent source for information exchange, especially as marketers and communicators attempt to uncover new ways to bring their messages to market.

Their use is pervasive, and hundreds of millions are expected to enter marketing efforts by the world's largest (and smallest) brands in the next year, according to Statisa. Despite this resurgence in power and popularity, QR codes are a threat vector weaponized with increasing sophistication in cyber dupes. As businesses rush to adopt QR codes, a new Trojan horse is sauntering to their gates. From these, cybercriminals are sneaking into the devices and data of their victims.

QR codes were created in 1994, the same year as the first PlayStation, by a Toyota subsidiary, as an inventory tracking tool, but by the start of this century's second decade, QR codes faced significant hurdles, and they nearly disappeared from the lexicon. The primary issue was the barrier to entry. Third-party apps were needed to read them, which turned many of us off.

In 2017, QR code readers were built into Android and Apple software updates. It was projected that by 2020, 91% of active iOS users would have access to in-built QR code scanners, eliminating the need for a separate app, and by 2022 one billion smartphones would have access to QR codes globally research by Fintech Futures suggested at the time.

Another frustration with them was an undefined use case. Their use was inconsistent and without purpose. They were usually integrated into marketing campaigns without optimization, leading to broken links, irrelevant content, or lack of mobile-friendly experiences, which is where the real value for scammers emerged. QR codes have always been exploited for malicious purposes, such as directing users to phishing websites or embedding malware. This undermined trust in the technology. As they surged in use, with earnestness during COVID-19, and were reimagined, threat actors evolved right alongside the technology.

Even with the development of dynamic QR codes, I'm currently less surprised by the adoption of the codes and more concerned by the sheer level of implicit trust users have begun to place in them. People are encouraged to use them—from celebrities working for their favorite brands telling us to use them by happenstance to stores collecting reward points and coupons to joining loyalty clubs and keeping up to date with news about our favorite sports teams, and even our employers using them to refer employees to update benefits packages and other corporate messaging.

As a fellow member of the cybersecurity community, you're aware of this, but your organization's users have been conditioned to identify traditional phishing cues in emails—misspelled domains, odd sender addresses, etc.—but a QR code bypasses all that. Users can't visually inspect a QR code's URL destination before scanning, creating a significant blind spot. Even experienced cybersecurity teams sometimes overlook this. Solutions exist that can run QR code phishing simulations to enable education to relevant users that click on the QR code of the perils of doing so, but without them, the protections are few.

The cybersecurity problem is not only the fact that scammers are slapping fake QR codes over legitimate ones in public spaces, but that the more sophisticated threat actors are employing tactics like dynamic QR codes to meet their objectives. This is important for security professionals to contemplate because these highly accessible codes are manipulatable once distributed to redirect users to risky URLs. We've seen this happen in spear-phishing campaigns targeting executives.

Quishing (phishing via QR codes) or QRLjacking possess potential harm because they can redirect payments from a legitimate account, for example, to an attacker's wallet without the user realizing it until it's too late. Given the irreversible nature of crypto payments and the difficulty of tracing the attacker, this is particularly effective when QR codes are used for cryptocurrency transactions. We're also seeing dynamic content injection developing into creative heists, where attackers create content and QR codes that, upon scanning, inject a malicious script into the user's devices.

What Can Be Done? Moving Beyond Basic Mitigations

Standard advice to train users to be cautious when scanning QR codes or to inspect URLs post-scan is not enough. We must push transformative shifts regarding how businesses deploy and monitor QR codes, but more importantly, we need real-time threat intelligence integration with QR code scanners. This is where we're focusing our innovation at VIPRE—building AI-driven threat detection engines that can assess the behavior of URLs in real time. We're talking about machine learning models that evaluate the destination URL for patterns, historical data, and geolocation or device type to stop malicious sites before they load. We're attempting to spearhead the creation of automatic buffers to protect against these threats without relying on user vigilance, which we know is a weak point. After all, how long have we been screaming at users to stop using "Password1234" as a password? If we rely on users as a line of defense, the war may already be over before the first shot is fired.

We also can't rely on any regulatory help. That landscape is woefully lagging in advancements of such technologies despite rapid adoption of QR code phishing and other such attacks. There's an absence of industry standards around secure deployment. For example, despite the surge in incidents, the NIST cybersecurity framework doesn't have specific guidelines for QR code use.

As an industry, we need to take the gloves off. We need to resemble the efforts of Mike Tyson in 1986, not the Tyson of 2024. We must push for security standards akin to PCI-DSS but tailored for QR code usage, particularly in financial services and healthcare, where the stakes are high. We also need integrated URL preview mechanisms in browsers and mobile OS-level protections that alert users to potential threats before they engage. Companies need to start looking at QR codes like any other endpoint or attack surface—monitoring, updating, and securing them as part of their broader cybersecurity strategy.

Since every kind of business has embraced QR codes, there is much room for opportunities for threat actors. The rapid, unchecked growth in these communication and engagement modalities has left gaping security holes that we've got to close. As cybersecurity professionals, we must challenge the narrative that QR codes are "safe enough " and treat them as a genuine attack vector. If we don't act, we're looking at a future where the next big data breach could begin with a single, innocent-looking scan.

So, when you engage in conversations about the potential threat of QR codes, keep this ammo at the ready: Threats to QR codes may be partially avoided, but implementing intelligent, proactive defenses is helpful because it's always about staying one step ahead of the attacks – and their innovation.

About the Author

As the general manager for VIPRE Security Group, Usman Choudhary is responsible for executing the company's product vision and strategy for advanced threat defense solutions. With contributions to several patented innovations in the early stages of the security space, he was instrumental in influencing the evolution of mission-critical cyber defense programs for the U.S. Navy (PROMETHEUS) and other government agencies and security programs at Microsoft and other large enterprises. Before joining VIPRE, Usman held several product leadership roles to develop identity and security businesses at NetIQ, Novell, and eSecurity. He previously served ten years in technology innovation for the global brokerage industry. Usman received his bachelor's degree in computer engineering from Rutgers University School of Engineering and his executive leadership education from Harvard Business School. In his personal time, Usman regularly contributes to several nonprofit service initiatives nationally and received the distinguished U.S. President's Call to Service Award in 2013.

Usman can be reached by email at Usman.Choudhary@vipre.com

Specialized Computer Vision vs. General AI: The Key to Fraud Prevention in Identity Verification

By Albert Roux, EVP of Product, Identity at Microblink

Artificial intelligence is transforming industries at an unprecedented pace, with large language models (LLMs) like ChatGPT and DeepSeek capturing headlines for their reasoning capabilities. However, when it comes to document verification and identity solutions, more specialized AI—particularly computer vision models optimized for specific tasks—outperforms general AI in both accuracy and efficiency. Nowhere is this more apparent than in high-stakes industries like travel and financial services, where fraud prevention and seamless user experience are critical.

The Accuracy Gap: Multi-Modal Machine Learning Models vs. Specialized Computer Vision

LLMs have impressive reasoning skills. They can process vast amounts of information and respond to requests more like humans. However, these models are generalists. They are designed to handle a wide range of tasks rather than optimizing for a specific one. When applied to identity verification, their accuracy lags behind dedicated computer vision models trained exclusively on analyzing visual patterns in documents and biometric data.

For example, an LLM can attempt to verify an ID by analyzing its text and structure. Still, it lacks the fine-tuned capabilities of a specialized computer vision model trained on millions of passports worldwide. This optimized model can detect what type of document it's viewing and minute details such as microprints, as well as security features that fraudsters attempt to manipulate. The result? A far lower error rate in identity verification reduces the risk of fraudulent transactions.

Why Computer Vision Excels in Identity Verification

Unlike LLMs, which rely on textual inference and reasoning, computer vision models are purpose-built to analyze and compare images, making them highly effective at tasks like facial recognition, document authentication, and detecting forged documents. Some of these models leverage a combination of deep learning and computer vision models. They train on extensive datasets of legitimate and fraudulent documents to become highly sensitive to discrepancies.

Computer Vision in Travel and Financial Services

Identity verification is a fundamental security measure across multiple industries. Cruise lines, hotels, car rental companies, and financial services firms all require stringent fraud prevention measures, and specialized computer vision models provide an effective solution. Computer vision models act much like a human brain, leveraging visual cues to detect anomalies in a document.

Identity verification in the hospitality sector has traditionally been a manual process. While airline gate agents or hotel staff visually inspect IDs, their ability to consistently detect sophisticated forgeries is limited. This is largely due to a lack of specialized training in document authentication - and just being humans. Humans get tired. Error and fatigue further contribute to potential security lapses.

In contrast, AI can run 24/7. It can be equipped with advanced computer vision and meticulously trained to identify even subtle indicators of fraudulent documents, providing a level of security far beyond what manual checks can achieve. The ability to process information rapidly and with high precision enables the industry to stay ahead of increasingly sophisticated fraud tactics, enhancing overall security.

Travel: Smoother Sailing for Cruise Operators and Passengers

Cruise operators handle thousands of passengers boarding and disembarking at multiple ports. Fraudulent IDs, whether stolen or manipulated, can pose security threats. Traditional verification methods, including manual checks and general AI solutions, often struggle to catch sophisticated document fraud. However, highly trained document verification machine learning models can quickly analyze travel documents, matching them against databases in real time to detect inconsistencies, ensuring that only legitimate passengers board the ship.

Furthermore, these models enhance passenger experience by reducing wait times to mere seconds vs. minutes. Instead of relying on human scrutiny or slow manual verification processes, passengers can move through security checkpoints seamlessly, minimizing bottlenecks when boarding or leaving the ship.

Car Rentals: Combating Identity Fraud and Stolen Vehicles

Fraud is a serious issue in the car rental industry, where stolen identities are frequently used to rent vehicles that are never returned. Fraudsters often manipulate driver's licenses, altering key details to evade detection. A general AI model might detect some inconsistencies, but a specialized computer vision system can perform precise authenticity checks in seconds. These models analyze security features, detect tampering, like photo face tampering (the most common form of document forgery), and even match facial biometrics against IDs to confirm a renter's identity.

By integrating computer vision into their verification processes, car rental companies can prevent fraudulent rentals and reduce vehicle theft, saving millions of dollars in losses annually. Additionally, automated verification improves customer experience, allowing legitimate renters to bypass lengthy manual checks.

Financial Services: Strengthening Fraud Detection in Banking and Payments

Financial institutions are a prime target for identity fraud, with cybercriminals constantly finding new ways to exploit vulnerabilities. General AI models may flag suspicious patterns in transaction data, but when it comes to document verification for account opening or loan applications, they lack the precision required to detect high-quality forgeries, especially font anomalies.

On the other hand, computer vision models augmented by data format and static rules can analyze minute document details, cross-referencing them with known fraud patterns. They can distinguish genuine government-issued IDs from sophisticated fakes that evade traditional detection methods. Banks and fintech companies that leverage this technology significantly reduce fraud-related losses while improving compliance with regulatory requirements.

The Role of AI in the Evolving Fraud Landscape

Fraud tactics constantly evolve, with criminals leveraging increasingly sophisticated tools to forge documents and bypass identity verification systems. General AI models may offer broad-based insights but lack the domain-specific expertise to counteract evolving fraud methodologies effectively.

Machine Learning models focused on computer vision can be easily retrained on the latest fraud attacks and quickly redeployed to curb the latest document forgeries. Moreover, these models integrate seamlessly with biometric verification, adding another layer of security by ensuring that the person presenting an ID is the rightful owner.

Striking the Right Balance with AI Collaboration

Leveraging both General AI and adopting specialized computer vision AI isn't just an option for businesses in high-risk industries, it's a necessity. These models' accuracy, speed, and adaptability make them the gold standard in identity verification, safeguarding companies and customers from the ever-present threat of fraud.

About the Author

Albert Roux, Microblink's EVP of Product, Identity, is a recognized industry expert with 20+ years of experience combating fraud and developing cutting-edge identity solutions. His extensive product management and R&D background spans fraud, identity verification, fintech, e-commerce, and adtech, with hands-on experience building and scaling successful products, platforms, and teams. Albert's expertise lies in large-scale fraud detection, honed through diverse roles at industry-leading companies like Microsoft, Criteo, and others. He is a sought-after speaker at prestigious events, including Money 20/20 and Gartner conferences, and has trained global law enforcement and intelligence agencies on advanced technical investigation techniques. His free newsletter is available via LinkedIn.

Ransomware's Escalating Toll Drives Demand for Ethical Hackers

As cyberattacks surge in scale and sophistication, ethical hackers are becoming indispensable in identifying vulnerabilities and defending critical infrastructure.

By Mark Moran, Chief Marketing Officer, Simplilearn

Ransomware has become a juggernaut, tearing through organizations with a ferocity that's hard to overstate. This year has already seen a flood of attacks from hospitals locked out of critical systems, city services stalled, leaving businesses scrambling to recover. Losses are quickly climbing, with estimates pointing to a $57 billion hit by the end of the year.

Cybercriminals aren't just encrypting files any more, they're raiding supply chains and wielding multi-pronged extortion tactics that leave little room for error. Given this situation, ethical hackers have become crucial in helping to take back control.

A Menace Growing Sharper

Ransomware incidents have grown rapidly since January of 2022, with reports noting a 388% growth of attacks in that time, turning what was once a manageable risk into a pervasive threat. In February 2025, a prominent Midwestern hospital chain grappled with a three-day outage, unable to access patient records as attackers demanded payment, while a Texas municipality saw its water treatment systems grind to a halt for nearly a week.

These aren't isolated setbacks, they're glimpses of a broader assault hitting healthcare, public services, and private firms alike, each incident amplifying the urgency for stronger countermeasures. Today's attackers move with precision, exploiting gaps before patches can roll out and amplifying damage by targeting backups or leaking stolen data. Standard security tools are essential but often lag behind this kind of agility.

Ethical hackers, known as white hats, offer a different approach. They dive into systems with a mindset borrowed from the adversaries they oppose. They scour web platforms for shaky code, test network barriers for cracks, and even stage phishing drills to spotlight human weak points. It's a hands-on, preemptive strategy proving its worth as the stakes climb higher.

Skills That Define the Job

Ethical hackers need a firm grip on networking essentials like protocols and server setups, paired with coding know-how in Python or C++. Certifications carry weight in these roles; the Certified Ethical Hacker credential and Offensive Security Certified Professional title often distinguish between a rookie and a professional.

What sets the best apart is an ability to stay current, with ransomware tactics constantly evolving, these professionals must track new vulnerabilities and countermeasures as soon as they emerge. It's a demanding balance of technical skill and relentless curiosity, a combination that's difficult to replicate.

Demand Outstrips Supply

The call for ethical hackers has hit its peak. With many cybersecurity jobs in the U.S. potentially remaining vacant by late 2025 and beyond, these specialists rank among the most coveted. Their dual-edged expertise in spotting flaws and fortifying against them makes them a rare commodity in a thin field.

Beyond filling a gap, their work carries real weight by thwarting attacks and shielding everything from patient care to public utilities, to offer protection far beyond server rooms. It's a role that marries technical grit with a broader sense of purpose.

Adapting to the Storm

Ransomware’s momentum isn’t fading, and neither can the response. Companies that once leaned on basic defenses are embracing tougher measures such as simulated breaches and deep system audits. Ethical hackers fuel this pivot, lending insight that turns weak spots into strengths.

The path is clear for those drawn to the challenge or leaders aiming to bolster their ranks. Programs like Simplilearn’s cybersecurity courses lay the groundwork, from network probing to countering social engineering ploys. As ransomware digs in, ethical hackers aren’t just a resource but a necessity, holding the line against a threat rewriting the rules.

About the Author

Mark Moran, Chief Marketing Officer at Simplilearn, is a passionate internet leader with over 25 years of marketing and line-management experience, Mark has successfully driven 9-figure revenue streams for emerging companies and divisions of Fortune 100 corporations. As the CMO, he oversees all aspects of the company’s global marketing initiatives, communications, and go-to-market efforts.

Previously, he headed marketing at Ebates and held executive positions with MyNewPlace, and Wells Fargo among others. Mark is a joint inventor of Patent 20080082426 for enabling image recognition and the enhanced search of remote content on partner websites and in ad units. Also, an angel investor and startup adviser, Moran holds a BA, from Pomona College and an MBA from Stanford Business School.

Mark can be reached online at mark.moran@fullstackacademy.com and at our company website https://www.simplilearn.com/

Closing Security Gaps with Attack Surface Scanning and Context-Aware Defense

An In-Depth Look at Why Traditional Scanning Falls Short in Today's Interconnected World

By Jeff Collins, CEO of Wanaware

The number of connected devices is growing at a rate that few could have imagined a decade ago—expected to surpass 32.1 billion globally by 2030. From smart thermostats in homes to complex IoT deployments in manufacturing, nearly every aspect of life and business now depends on interconnected systems. This explosion of connectivity, while enabling innovation and efficiency, has dramatically expanded the digital attack surface, and with it, the risks.

Today, security teams are tasked with safeguarding environments that span thousands of IP addresses and include countless shadow IT assets and third-party systems. Traditional vulnerability assessment methods simply weren't built for this scale. Legacy scanners tend to prioritize ease and speed, often focusing on fewer than 80 network ports. While that may have been sufficient in simpler environments, it's an increasingly dangerous gamble in today's distributed and dynamic networks.

Recent analyses show that this outdated approach only covers about 40% of the ports organizations actually use. The remaining 60%, which go unscanned, can harbor critical services and potential vulnerabilities that attackers are more than willing to exploit. The result is an incomplete picture of network exposure, and it leaves organizations flying blind.

To effectively reduce risk, we need a shift in how we think about vulnerability detection. That shift starts with expanding and contextualizing the attack surface scanning process.

The Case for Broader Attack Surface Coverage

One of the most immediate improvements organizations can make is to expand their attack surface scanning coverage to include the top 1,000 ports. These ports are responsible for hosting over 95% of the world's common network services and protocols, including HTTP, SSH, FTP, SMTP, and many others. By broadening the aperture of visibility in this way, security teams can catch a far greater share of misconfigurations, unpatched software, and rogue services before attackers do.

This doesn't mean scanning everything, everywhere, all the time, especially given the performance and bandwidth constraints that some networks face. But it does mean embracing smarter prioritization. The goal is to strike the right balance between thoroughness and efficiency, leveraging real-world threat intelligence to focus resources where they matter most.

Understanding the Context of Exposure

Equally important is moving beyond raw discovery to understand the context of each exposed asset or service. Not all vulnerabilities are created equal. A misconfigured FTP server in a segmented lab environment doesn't carry the same risk as one exposed directly to the public internet with administrator credentials. Without this context, security teams can drown in noise and miss the real threats.

That's where context-aware defense comes into play. This approach pairs attack surface scanning with insights about asset ownership, sensitivity, exposure level, and network topology. It transforms what would otherwise be a flat list of vulnerabilities into an actionable map of true risk. In practice, this means that a seemingly minor vulnerability can be elevated to a top priority if it resides on a critical asset or is easily accessible from the outside.

Context-aware defense doesn't replace other cybersecurity layers. In fact, it strengthens them. This type of defense provides the visibility and prioritization necessary to guide patching efforts, inform segmentation strategies, and even support incident response. When a breach attempt occurs, understanding the context of the targeted asset can accelerate containment and remediation.

Rethinking External Attack Surface Management

As organizations expand their use of cloud infrastructure, remote workforces, and third-party integrations, much of the attack surface now lives beyond the firewall. Internet-facing assets—some known, others long forgotten—can be deployed and exposed in a matter of minutes. These assets don't just increase surface area; they redefine the perimeter altogether.

Managing this shifting landscape requires more than asset discovery. It calls for a continuous, adaptive strategy that combines frequent scanning with real-time analysis. Instead of treating external exposure as a static inventory problem, the modern approach treats it as a fluid, high-frequency data stream—one where changes are tracked in near real time and automatically correlated with risk indicators.

Rather than reacting to every alert equally, smarter attack surface management prioritizes based on context: Which assets are active? Which are accessible from the public internet? Which tie into critical systems? Which ones have known vulnerabilities or fall outside existing controls? This kind of intelligent filtering enables teams to zero in on what matters, before attackers do.

Navigating IoT and Edge Complexity

Nowhere is the complexity of interconnectivity more pronounced than in environments rich with IoT and edge devices. These assets are often rolled out rapidly and at scale, with minimal security oversight. They run on diverse operating systems, may lack standard patching mechanisms, and are frequently deployed in remote or unmanaged environments.

Effective protection starts with simply knowing what's there. Attack surface scanning plays a crucial role in discovering these devices and cataloging the services they expose. From there, context becomes critical again—understanding which devices are connected to high-value systems, or which ones have known vulnerabilities but no path to remediation, can inform compensating controls.

IoT isn't going away. Neither is the cloud. Organizations need tools and strategies that can keep up; not just by scanning wider, but by thinking deeper.

Defending in Real Time, Not Hindsight

Security is ultimately about visibility. You can't defend what you don't know exists. As the digital perimeter continues to dissolve, organizations must take a more proactive and context-driven approach to understanding their exposure. That starts with expanding scanning coverage beyond outdated defaults and embracing the nuanced, risk-based prioritization that context-aware defense offers.

We are operating in a world of persistent threats and evolving vulnerabilities. Attackers don't limit themselves to the top 80 ports, and neither should we. To stay ahead, we must combine comprehensive visibility with real-world and real-time context. Only then can we close the gaps that legacy tools leave behind and truly defend our networks with confidence.

About the Author

Jeff Collins, CEO of WanAware, has over 25 years of experience driving profitable growth by transforming brands, companies, and cultures. He is passionate about leading disruption through insight-driven strategies that activate brands and companies, attract customers, inspire stakeholders, and create community. In 2020, Jeff began developing WanAware after recognizing the need for effective IT Observability solutions due to the limitations of outdated legacy tools and antiquated models. He also holds leadership positions at 21Packets (Chairman) and Lightstream (Chief Strategy Officer). Jeff serves on the boards of multiple technology companies, contributing his expertise in cybersecurity, AI, networking, and data transformation. Connect with Jeff on LinkedIn https://www.linkedin.com/in/jmcollins/ and learn more about WanAware on our company website https://www.wanaware.com/.

Credentials are Your Keys to the Castle - How to Keep Them Safe with a Security-First Culture

By Tim Eades, CEO & Co-Founder, Anetac

Organizations face a critical reality that many security professionals have long understood but too few enterprises have properly addressed: credentials remain the keys to the kingdom and cyber hygiene continues to be neglected. Despite advances in security technology, passwords remain the first line of defense and often the weakest links.

Passwords are just the visible edge of a much deeper problem: fragmented identity visibility. Behind every credential lies an identity, whether human or non-human, that may no longer need access, is overprivileged, or hasn't rotated credentials in years. At Anetac, we believe risk begins when you lose sight of who (or what) has access, why, and whether that access is appropriate.

The Fundamental Truth of Identity Security

Passwords alone cannot safeguard digital identities in today's hybrid environments, where employees access resources from multiple locations using various devices. According to recent industry reports, identity-based vulnerabilities have emerged as the primary attack vector for modern breaches, with compromised credentials involved in approximately 80% of all hacking-related data breaches. This alarming statistic underscores how critical proper credential management has become in our interconnected world.

Yet most organizations still treat this as a password strength problem instead of an identity context problem. Too many enterprises still lack visibility into who owns each credential, when it was last rotated, and whether the account behind it is even in use.

The Alarming State of Password Hygiene

At Anetac, we have uncovered concerning patterns in credential management across industries. In financial institutions, some passwords have remained unchanged for over 15 years, creating critical security blind spots in organizations handling some of the most sensitive financial data in the world. The healthcare sector shows equally troubling trends, with 74% of healthcare credentials remaining unchanged for more than 90 days, putting patient data and critical systems at significant risk. Critical infrastructure sectors demonstrate widespread credential sharing, with multiple employees using the same login information, violating basic security principles and making attribution nearly impossible when incidents occur. Across all industries, the average enterprise password remains unchanged for 180 days, well beyond security best practices, creating extended windows of vulnerability.

The true danger isn't just in stale passwords; it's in accounts that no one knows exist. Dormant service accounts and orphaned human accounts with outdated or weak passwords represent a treasure trove for malicious actors seeking entry points into corporate networks. These forgotten access points often retain privileged permissions and go unmonitored for months or years, providing perfect attack vectors.

Anetac helps organizations discover and surface these blind spots by analyzing credential age, tracking last password rotation, mapping access chains, and identifying unused or over-privileged identities across both human and non-human identities. We provide intelligence on when credentials were last rotated and how they are being used. This context enables organizations real, scalable remediation.

The Necessity of Cyber Hygiene in a Security-First Culture

Creating a security-first culture requires organizations to implement fundamental cyber hygiene practices regardless of industry. Even companies outside the cybersecurity sector must prioritize basic security protocols as part of their operational DNA. We recommend rotating credentials every 90 days at a minimum. This practice significantly reduces the window of opportunity for attackers who may have obtained credentials through various means, including phishing, brute force attacks, or dark web marketplaces.

Human error remains a significant vulnerability in the security chain. Organizations must invest in regular security awareness training to create vigilant employees who understand their role in protecting company assets. This education should cover:

- Phishing identification techniques, teaching employees to recognize suspicious email characteristics such as urgent language, unexpected attachments, and subtle domain spoofing.
- Social engineering awareness to help staff understand psychological manipulation tactics
- Proper reporting procedures to ensure that suspicious activity reaches security teams quickly, reducing the time between compromise and detection—a critical factor in limiting breach impact.

Keeping all devices and software current with security patches is essential for closing known vulnerabilities that attackers will exploit. Organizations should implement automated update systems to ensure consistency across the enterprise environment. Clear patch management procedures establish accountability and ensure critical updates aren't missed during busy operational periods. Regular maintenance windows provide predictable times for updates to minimize business disruption while keeping security prioritized. Critical security updates deserve special attention and expedited deployment, particularly for zero-day vulnerabilities that pose immediate threats.

The AI Threat Multiplier

The rise of artificial intelligence presents new challenges in the security landscape. What many organizations fail to recognize is how AI fundamentally changes the threat equation: A good threat actor becomes great with AI, and a great threat actor can scale with AI.

AI tools enable threat actors to generate more convincing phishing attempts by analyzing communication patterns and social media to create highly personalized messages that bypass traditional security awareness training. These systems can automate credential stuffing attacks at unprecedented scale, attempting millions of username and password combinations across multiple sites in hours rather than days or weeks. Pattern analysis capabilities help attackers identify vulnerable accounts and target them with precision. Sophisticated social engineering scenarios powered by AI can now mimic executive communication styles or leverage personal information to create highly convincing pretexts for accessing sensitive systems or transferring funds.

Enterprises relying on legacy cybersecurity solutions are in the digital dark ages, attempting to counter AI-enhanced threats with horribly outdated defenses. These organizations are fighting tomorrow's battles with yesterday's weapons, creating an asymmetric advantage for attackers who have enthusiastically embraced technological innovation.

The Identity Vulnerability Management Ecosystem

Modern security requires protecting both human and non-human identities with equal vigilance. Service accounts, API keys, application identities, and machine credentials often have even more privileged access than human users, yet receive far less security scrutiny. These non-human identities frequently operate with persistent, high-level permissions and minimal oversight, creating perfect targets for attackers seeking to establish persistent access to critical systems.

Comprehensive identity security includes several essential elements:

- Behavioral analytics to detect anomalous access patterns that might indicate compromise, even when credentials are valid.
- Lifecycle management to ensure that identities are properly provisioned, monitored, and deprovisioned as organizational roles change.
- Continuous verification to replace the outdated model of periodic authentication, ensuring that users remain who they claim to be throughout their sessions.
- Credential age to identify accounts with passwords that haven't been rotated passed organization standards

Beyond Password Management

Effective identity security requires capabilities beyond basic password management:

- Detection capabilities for aged credentials allow security teams to identify accounts that may have been overlooked in regular rotation schedules.
- Analysis of behavioral anomalies helps identify potentially compromised accounts even when credentials appear valid.
- Identification of lifecycle blind spots ensures that accounts aren't forgotten during employee transitions or project completions, preventing the accumulation of orphaned accounts with valid access.
- Advanced tools verify the actual identity behind the account through multiple factors, including location, device characteristics, and behavior patterns.

This comprehensive approach acknowledges that passwords aren't disappearing anytime soon, but contextualizes their importance within the broader identity ecosystem. Organizations must recognize that credential security represents a foundational element of their overall security posture, not just a compliance checkbox.

Credentials & Cyber Hygiene in the AI Age Matter More Than Ever Before

The uncomfortable truth is that password hygiene remains a cornerstone of effective cybersecurity. Despite advances in security technology, credentials continue to be a primary attack vector. Organizations must treat password management with the same seriousness given to any other critical security asset.

In today’s world, password hygiene is just one layer of defense. Identity vulnerability management, the ability to continuously discover, monitor, and reduce risks tied to every account, is the foundation.

In an era where identity is the perimeter, the ability to properly manage, monitor, and secure credentials over time represents the difference between security resilience and becoming the next breach headline. Organizations that create a security-first culture, implement proper cyber hygiene practices, and deploy modern identity security solutions position themselves to withstand the evolving threat landscape—where credentials remain both our greatest vulnerability and our most critical defense.

About the Author

Tim Eades serves as CEO and Co-Founder of Anetac, combining his deep cybersecurity expertise with a proven track record of building and scaling successful security companies. With over two decades of executive leadership, Tim has consistently delivered exceptional growth and successful exits in the enterprise software and security sectors.

Before founding Anetac, Tim served as CEO of vArmour for nine years and as CEO, led Silver Tail Systems to its successful acquisition by RSA (EMC's security division) in 2012. As CEO of Everyone.net, he drove the company's growth and eventual acquisition by Proofpoint. His executive experience also includes leadership roles at BEA Systems, Sana Security, Phoenix Technologies, and IBM, where he achieved the distinction of being the No. 1 salesperson in Europe. Beyond his operational roles, Tim serves as General Partner and Fellow Founder at Cyber Mentor Fund, where he actively invests in and mentors the next generation of cybersecurity entrepreneurs. His investment portfolio spans over 50 companies, reflecting his commitment to advancing innovation in cybersecurity. He currently serves on the board of Boxx Insurance, Enveil and Device Authority and holds advanced degrees in business, international marketing, and financial analysis from Solent University in England. Tim's approach combines rigorous business acumen with hands-on technical expertise, enabling him to identify and solve critical security challenges while building capital-efficient, high-growth companies.

Tim Eades and Anetac can be reached at our company website https://anetac.com/

Physical Network Isolation. The New Secret Sauce in Cybersecurity?

By Tony Hasek, CEO and Co-Founder, Goldilock

AI in cybercrime is no longer a distant threat; it's here. Going forward, organizations will encounter malware that learns, adapts, and operates autonomously. Unlike traditional malware, which executes a fixed set of instructions, these new threats can observe, evolve, and operate autonomously.

Yet, despite this leap in sophistication, many organizations continue to rely heavily on traditional, software-based defenses. While these remain important, they're no longer sufficient on their own.

It's time to start thinking in layers, combining intelligent detection, user training, and strategic planning with an old technique that has evolved into a modern form: physical network isolation. By cutting off all digital access, it removes critical systems from the line of fire – rendering them unreachable to even the most adaptive malware.

In an era where threats evolve faster than patches, this kind of hard disconnection is set to become the secret sauce of modern cyber defense.

A Surge in Sophisticated AI-Powered Threats

A recent Axios survey found that only 20% of companies feel prepared to handle AI-enhanced threats, and yet there has been a 300% increase in AI-powered cyberattacks over the past year alone, according to Restack. Meanwhile, Statista estimates that the annual global cost of cybercrime will rise from over $9 trillion in 2024 to nearly $14 trillion by 2028.

These aren't just statistics. They represent real financial damage, operational disruption, and erosion of public trust.

Unfortunately, too many organizations continue to rely heavily on reactive, software-based defenses. These tools, while useful, are outmatched when deployed on their own. AI-powered malware can now adapt in real-time, morphing its behavior to bypass detection systems and exploit previously unaddressed vulnerabilities.

So, by the time the alarms go off, the damage may already be done.

What Makes Physical Isolation So Effective?

This is why physical network isolation warrants more attention. Physical isolation cuts off access completely, creating a physical gap around the network, like a firebreak. When systems are physically disconnected from external networks – either automatically during an attack or as a default state when not in use – there's simply no path for intruders to follow.

This isn't the rigid air-gapping of the past. Today's approaches are smarter, more adaptable, and easier to deploy. Modern firebreak technologies allow systems to be disconnected remotely using out-of-band signals; communications that don't travel through the same networks they're meant to protect. This makes them immune to spoofing or hijacking by malware already inside the environment.

In other words, it lets organizations instantly sever a connection to proactively shield high-value targets without disrupting other systems or segment compromised networks to contain a breach and prevent data exfiltration.

Old Tactics, New Tricks?

The inspiration for physical isolation isn't new. In military operations, physically separating critical communications and control systems is standard practice. It's a proven strategy for preserving integrity in hostile conditions.

The same principle applies to cybersecurity: hardware-level isolation breaks the chain of connectivity completely. Unlike segmentation or firewalls that rely on software rules, this approach removes any remote access path altogether.

Some solutions can even be triggered with non-IP commands, leaving no internet-facing component for attackers to exploit.

And this is precisely where it beats AI-powered malware. These threats feed on access. They observe system behavior, probe defenses, and adjust tactics to slip past digital barriers. Physical isolation denies them that opportunity. It's the equivalent of pulling the plug – fast, effective, and absolute.

Still, no solution works in isolation (not even isolation), and physical network isolation works best as part of a layered security strategy.

Layered Defense: Where Isolation Fits In

The strongest defense is a layered one that blends human readiness with technical depth. That means regularly updating and testing disaster recovery plans, training employees to identify AI-powered phishing and social engineering attempts, and deploying intelligent detection tools that spot subtle, real-time anomalies, not just known threats.

Physical network isolation plays a critical role in this architecture. It's a precision tool as much as a blunt one, capable of both containing active threats and shielding critical assets. Used strategically as the foundational layer of a comprehensive security strategy, it works in conjunction with other solutions to empower organizations to act rather than react.

Instead of building ever-higher digital walls, organizations must create adaptable, resilient systems that know when to implement a firebreak at Layer-1 and disconnect completely dramatically reducing their attack surface in the process.

Preparing for the Autonomous Threat Era

The cybersecurity battlefield has changed. Threats learn, adapt, and target the humans behind the systems. Lone software defenses struggle to keep pace with evolving threats and AI has only exacerbated the issue.

Physical network isolation isn't a fallback. It's a frontline tool in a broader defense-in-depth strategy. Whether implemented as firebreak architecture, physical segmentation, or modern air-gapping, the goal is the same: create environments where critical systems can be instantly and definitively cut off from harm.

The bottom line is that systems that aren't online can't be hacked and it's very few systems where entire networks need to be 'always-on'. The level of control offered by physical network isolation may be one of the most important additions to the security stack in a long time.

And those who embrace it, not as a replacement for existing tools but as a critical layer within a unified defense, will be far better positioned to withstand AI-powered threats.

About the Author

Tony Hasek is the CEO and Co-Founder of Goldilock. Tony can be reached online at: https://www.linkedin.com/in/anthonyhasek/ and at our company website: https://goldilock.com/.

Orchestrating Secure Connections: Advanced Network Strategies for Hybrid Clouds

Addressing Key Network Security Challenges and Implementing Robust Solutions for Hybrid and Multi-Cloud Networks

By Harika Rama Tulasi Karatapu, Network Security Specialist, Google LLC.

As organizations increasingly embrace the dynamic and scalable nature of multi-cloud environments to drive innovation and agility, a significant shift is occurring in network security. While this distributed model offers compelling advantages, it fundamentally reshapes the network perimeter, dissolving traditional boundaries and demanding a more sophisticated, distributed approach to network security. Just like how “lift and shift” is not applicable for long-term applications, the same holds true for the underlying Network Architecture and the Security posture for the Cloud environment.

Network Security Challenges in a Multi-Cloud Environment:

Multiple Entry Points for the Attackers: While user-to-application traffic is considered North-South Traffic, the traffic between different workloads and services in a Cloud or multi-cloud environment is called East-West traffic.

With the adoption of multiple cloud environments, multiple entry points for the North-South traffic needs to be secured. However, multiple cloud providers offer different solutions to address, resulting in Inconsistent Network Security Policies and often prone to misconfiguration.

Inter-Cloud Connectivity: Establishing a secure and reliable path between Cloud Environments is a challenge. Traditionally Cloud VPN was the only option, however with the advancements of the technology Cloud providers now provide multiple options to connect almost anywhere to anywhere and that includes Interconnects, direct connects, Cloud WAN, or SD-WAN. While the reliable path solution is resolved with these options, security, monitoring, latency troubleshooting, and bandwidth requirements are still applicable.

Securing Traffic between Cloud Platforms: East-West traffic is critical to be protected from different attacks. Usually, native firewall rules that operate on layer 3 or 4 on each Cloud platform will help control the traffic based on the 5-tuples (Source address, destination address, Source port, Destination Port, Protocol). However, we also need to be able to block the traffic on layer 7, i.e., Application layer, and thus need some important features like SSL/TLS inspection, Deep packet Inspection(DPI), stateful inspection, URL filtering, data loss prevention(DLP), etc., to cater to the increase in demand.

Centralized Visibility and Control: While taking advantage of multi cloud, a unified dashboard to view the Network Traffic is a major challenge. Each cloud provider offers very clear and most advanced Networking tools for the monitoring capabilities, and common dashboards are not available for multi cloud environments, which makes it even more difficult in enforcing consistent Security policies.

Best Practices for a robust Multi-Cloud Network Security from Google Cloud Platform:

To effectively secure multi-cloud networks, organizations should follow best practices:

Principle of Least Privilege: Adhere to the **Principle of Least Privilege** by meticulously restricting network access for users (principals), Compute Engine instances (devices), and applications (services) strictly to the minimum set of permissions and network paths required for their designated roles and functions. Leverage **Identity and Access Management (IAM)** for user and service account permissions, and **VPC Firewall policies** along with **network tags** to precisely control network connectivity at the instance and application level. This minimizes the blast radius of potential security incidents.

Identity-Centric Security: In Google Cloud, move beyond traditional network location-based access control and base network access decisions on **v**erified user and service account identities (leveraging Cloud IAM), device posture (potentially through integration with endpoint management solutions), contextual factors (such as user location inferred through BeyondCorp Enterprise or Context-Aware

Access), and application attributes (like service accounts or workload identity), for a more dynamic and secure environment.

- **Centralized point of entry:** The **Global Load Balancer** acts as a single, resilient entry point for your globally distributed applications. Its key capabilities in mitigating the risk of multiple entry points include:
- **Centralized Traffic Management:** By directing all incoming traffic through a single IP address (or set of addresses), the Global Load Balancer reduces the attack surface and simplifies security policy enforcement.
- **Integration with Cloud Armor:** Directly integrating with **Cloud Armor**, Google Cloud's Web Application Firewall (WAF) and DDoS protection service, the Global Load Balancer allows you to apply consistent security rules and mitigations at the edge, inspecting traffic before it reaches your backend services, regardless of their location. This single point of defense protects against a wide range of web-based attacks.
- **Scalable Certificate Management:** Supporting **millions of SSL/TLS certificates**, the Global Load Balancer simplifies the management and deployment of encryption across your global footprint, ensuring secure connections for users regardless of the entry point they access.
- **Hybrid Backend Services:** The Global Load Balancer can seamlessly route traffic to **hybrid backend services** spanning multiple environments. This includes backends within different Google Cloud regions, on-premises infrastructure, and even other cloud providers. **Internet Network Endpoint Groups (NEGs)** further extend this capability by allowing you to directly address internet-reachable endpoints as backends. This centralized control ensures consistent security policies are applied even to traffic destined for diverse backend locations.

Google Kubernetes Engine (GKE) Gateway provides a powerful solution for managing external access to your Kubernetes clusters, including those in hybrid and multi-cloud scenarios. Its relevance to mitigating multiple entry points includes:

- **Unified Ingress Control:** GKE Gateway offers a standardized way to manage ingress traffic to your GKE clusters, regardless of where they are running. This provides a consistent control plane for external access, reducing the complexity of managing individual ingress controllers per cluster.
- **Multi-Cloud and Hybrid Connectivity:** GKE Gateway is designed to support **cluster services from multiple cloud providers**, including on-premises Kubernetes clusters. This allows you to present services running across different Kubernetes environments through a unified set of access policies, managed centrally.
- **Enhanced Security Features:** While not directly a WAF like Cloud Armor, GKE Gateway integrates with Kubernetes Network Policies and can be further enhanced with third-party security solutions. Its centralized management of ingress rules helps to define and enforce consistent security boundaries for your containerized applications, regardless of their cloud provider.

East-West Security with Google Cloud: With the evolution of Cloud platforms, many advancements have been made in firewalls, and we see that security options like **NGFW Enterprise** by Google Cloud are one great example.

It helps in Advanced Threat Prevention Powered by Palo Alto Networks, protecting against Intrusion Prevention System (IPS), Anti-Malware and Anti-Spyware, Command and Control (C2) Blocking, Vulnerability Protection, Real-time Threat Intelligence, Deep Packet Inspection (DPI) and Layer 7 Visibility, TLS Inspection and Decryption, Micro-segmentation with IAM-governed tags, and Centralized and comprehensive Logging and Monitoring options.

NGFW Enterprise integrates with Google Cloud's Identity and Access Management (IAM) and leverages **IAM-governed Tags**. This powerful combination enables granular micro-segmentation down to individual Compute Engine instances or workloads.

However, while working with a multi-cloud environment, NGFW will incur lack of Centralized Control, potential for Policy Gaps on multiple cloud providers, Vendor Lock-in Concerns.

Centralize Network Security Monitoring and Management with Integrated 3P Visibility:

Establish **unified visibility** by integrating network logs and telemetry generated within your Google Cloud environment (from VPC Flow Logs, Firewall Rules Logging, Cloud NAT Logging, etc.) or by using Network Security Integration Out-of-band 3P integration. This provides a centralized and holistic view of network activity alongside insights from your other cloud and on-premises environments, enhancing threat detection and analysis.

Implement **automated anomaly detection** within your integrated 3P solution by leveraging its AI and machine learning capabilities to analyze aggregated Google Cloud network traffic patterns. This enables the identification of deviations indicative of potential attacks, triggering alerts and facilitating automated or semi-automated responses orchestrated through the 3P solution, potentially interacting with Google Cloud APIs for remediation.

Ensure **continuous configuration monitoring** of your Google Cloud network resources (VPC networks, firewall rules, routes, etc.) by leveraging the monitoring capabilities of your integrated Network Security Integration 3P out-of-band solution. Configure it to detect configuration drift and identify potential misconfigurations against your security baselines, generating timely alerts and, where possible, initiating automated remediation workflows through API integrations with Google Cloud.

Conclusion:

The move to multi-cloud setups brings flexibility and innovation, but it also creates complex network security problems. The traditional idea of a network's edge is disappearing, leaving a spread-out environment with many points of vulnerability. This demands a more advanced and unified security strategy. Businesses struggle with inconsistent security rules across different clouds, the difficulty of setting up secure connections between clouds, the crucial need to protect traffic within cloud environments (East-West traffic), and the challenge of getting a single, clear view and centralized control of their scattered networks.

Adopting a robust set of best practices is paramount to navigating this evolving terrain. Strategies such as enforcing the Principle of Least Privilege through meticulous access controls and moving towards an Identity-Centric security model are foundational. Centralizing traffic management and defense using tools like global load balancers with integrated web application firewalls can effectively mitigate risks associated with multiple entry points. For containerized workloads, solutions like GKE Gateway can provide unified ingress control across hybrid and multi-cloud Kubernetes deployments.

Furthermore, advanced threat prevention for internal East-West traffic, for example, through Next-Generation Firewalls, is crucial, although considerations for centralized management in multi-cloud settings remain. Ultimately, achieving comprehensive security requires centralizing network monitoring and management, often by integrating Network Security Integration 3P out-of-band platforms to enable holistic visibility, automated anomaly detection, and continuous configuration oversight across the entire multi-cloud and hybrid landscape. By proactively addressing these areas, organizations can harness the power of multi-cloud environments while maintaining a strong and resilient security posture.

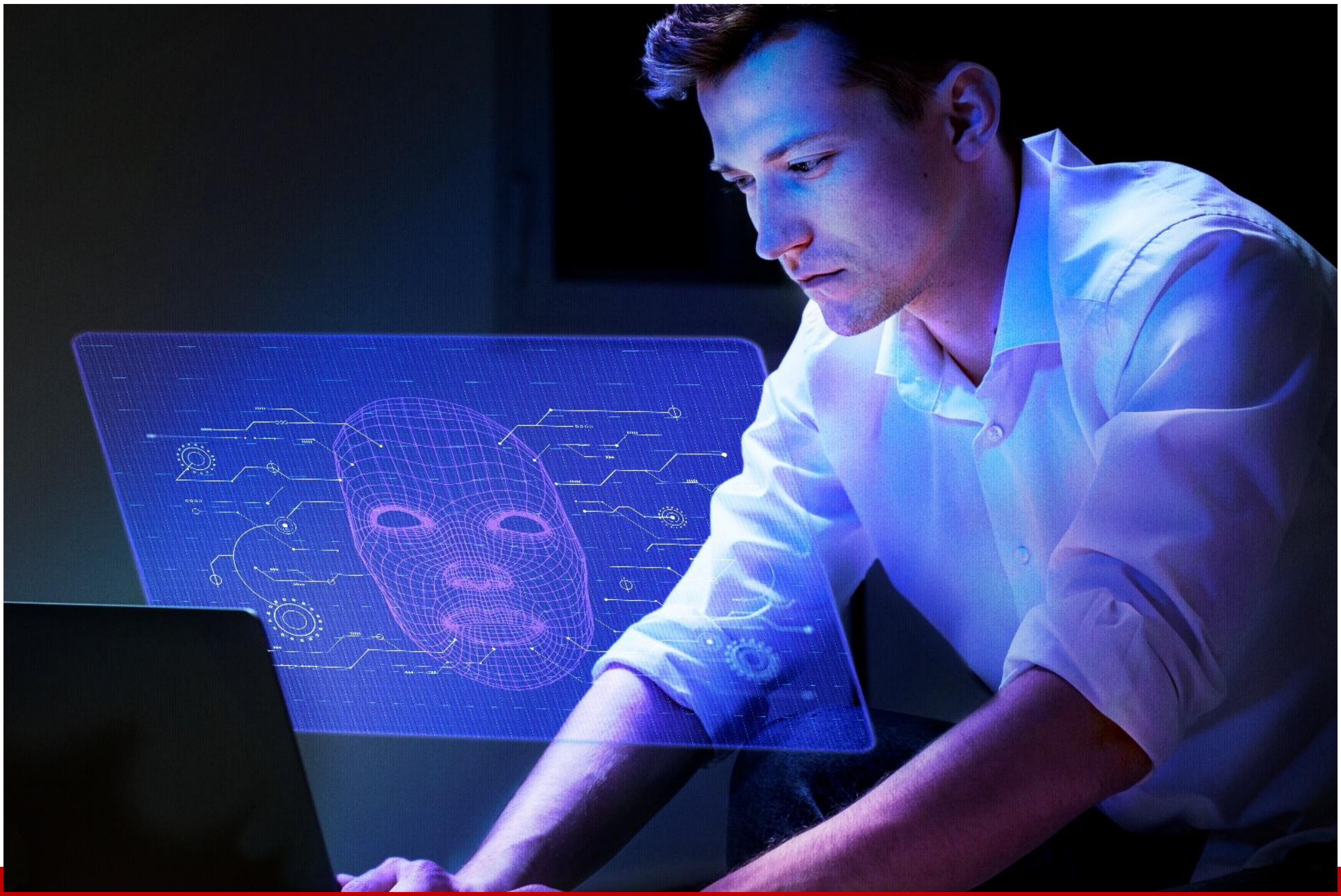
About the Author

Harika Rama Tulasi Karatapu is a seasoned Network Solutions Architect with over 13 years of experience in cloud and traditional networking. With a strong technical foundation and a results-driven approach, she specializes in designing and implementing secure, high-performance networking solutions across Google Cloud Platform (GCP) and Amazon Web Services (AWS).

Currently working as a Network/Network Security Specialist, Customer Engineer at Google LLC, she architects cloud-native and hybrid networking solutions for enterprise clients, optimizing cost, performance, and security. She also collaborates with C-suite executives on cloud adoption strategies, leads the Network Architecture for Google Cloud SaaS Accelerator Program, and contributes to Google Cloud for Startups as a technical Mentor.

Prior to Google, Harika worked at Juniper Networks, Amazon Web Services, and Infosys, working on network architecture, troubleshooting, automation, and security. A JNCIE-ENT, JNCIE-DC certified Juniper expert. Harika did her Masters from San Jose State University in Electrical Engineering with Computer Networking as specialization.

Harika can be reached online at harika.karatapu@gmail.com, https://www.linkedin.com/in/harikakaratapu/ and at our company website https://sites.google.com/view/gfsa-ca-2025/google-mentors?authuser=0



Cybersecurity for AI Systems: Protecting AI Models and Data

This article explores advanced strategies for fortifying the future by securing AI models and data against emerging cyber threats.

By Bhashwanth Kadapagunta, Specialist Leader, Deloitte AI & Engineering

Artificial intelligence (AI) systems are increasingly central to critical infrastructure, business operations, and national security. As their adoption accelerates, so do the sophistication and frequency of cyber threats targeting AI pipelines. This article presents original research and a synthesis of the latest methods for securing AI systems, focusing on three core challenges: data poisoning prevention, model theft protection, and secure model deployment.

Securing the AI Pipeline: Threat Landscape and Attack Vectors

AI pipelines are exposed to unique threats at each stage:

I. **Data Ingestion and Preprocessing**: Vulnerable to data poisoning, where adversaries inject malicious samples to corrupt model behavior.
II. **Model Training**: Susceptible to unauthorized access, theft of proprietary algorithms, and adversarial manipulation.
III. **Model Deployment and Inference**: Exposed to prompt injection, model inversion, denial-of-service, and exfiltration attacks.

I. Data Poisoning Prevention

A) Threat Overview

Data poisoning involves the deliberate introduction of malicious or manipulated data into training sets, aiming to degrade model performance or induce specific misclassifications. The stealthy nature and scale of modern datasets make detection and remediation challenging.

B) Original Research: Adaptive Provenance-Based Filtering

An adaptive provenance-based filtering system is proposed that leverages cryptographically signed data lineage and real-time anomaly detection. Each data sample is accompanied by a verifiable provenance record, ensuring traceability from source to ingestion. The system employs:

- **Schema validation and cross-validation** to enforce structural integrity.
- **Anomaly detection using ensemble models** to flag suspicious patterns in high-dimensional data streams.
- **Outlier detection with robust statistics** to automatically quarantine anomalous samples for human review.

C) Best Practices

- Implement strict access controls and encryption for all training data.
- Regularly retrain and test models on clean, verified datasets to detect and mitigate poisoning.
- Foster security awareness among data engineers and establish clear incident response protocols.

II. Model Theft Protection

A) Threat Overview

Model theft (also known as model extraction or stealing) occurs when adversaries reconstruct or exfiltrate proprietary model parameters, architectures, or weights, often via API probing or insider threats.

B) Original Research: Differential Query Monitoring

A differential query monitoring framework is introduced that profiles legitimate user interaction patterns and flags anomalous query sequences indicative of model extraction attempts. Key features include:

- **Rate limiting and behavioral analysis** to detect high-volume or systematic probing.
- **Output perturbation**: Adding controlled noise to model outputs for untrusted queries, balancing utility and security.
- **Watermarking model responses**: Embedding imperceptible signatures within outputs to trace stolen models.

C) Best Practices

- Encrypt model weights at rest and in transit; store them in hardware security modules (HSMs) or isolated enclaves.
- Restrict access to models via zero-trust principles and role-based access control (RBAC).
- Apply adversarial training and model hardening to increase resilience against extraction and inversion attacks.

Secure Model Deployment

A) Threat Overview

Deployed models face risks from prompt injection, unauthorized API access, supply chain compromise, and runtime tampering.

B) Original Research: Continuous Integrity Verification

A continuous integrity verification protocol is proposed that combines:

- **Cryptographic hashing of model binaries and configurations** at release, stored in tamper-proof vaults.
- **Automated monitoring of model behavior, architecture, and configuration** for unauthorized changes.
- **Human-in-the-loop failover mechanisms** for rapid rollback and incident containment.

C) **Best Practices**

- Secure all exposed APIs with strong authentication, authorization, and encrypted communication (e.g., HTTPS/TLS).
- Validate and sanitize all user inputs to prevent prompt injection and adversarial manipulation.
- Store all source code, infrastructure-as-code, and artifacts in version control with strict access and audit trails.

Comparative Summary of Key Security Controls

Security Control	Data Poisoning	Model Theft	Deployment Attacks
Data provenance & validation	✓		
Anomaly/outlier detection	✓	✓	✓
Encryption (data, weights)	✓	✓	✓
Access control (RBAC, MFA)	✓	✓	✓
API authentication & rate limiting		✓	✓
Adversarial training	✓	✓	✓
Continuous monitoring & rollback	✓	✓	✓

Conclusion and Future Directions

Securing AI systems requires a holistic, multi-layered approach that integrates provenance tracking, robust access controls, adversarial resilience, and continuous monitoring. The original frameworks proposed-adaptive provenance-based filtering, differential query monitoring, and continuous integrity verification-offer a blueprint for advancing the state of AI cybersecurity.

Future research should explore automated supply chain risk assessment, federated learning security, and formal verification of AI model integrity. As AI systems become more autonomous and interconnected, proactive and adaptive cybersecurity will be essential to safeguard their trustworthiness and societal impact.

About the Author

Bhashwanth Kadapagunta is a distinguished Architect and Delivery Leader at Deloitte’s AI and Engineering practice. With over 15 years of industry experience, he is a trusted advisor to Fortune 500 clients, helping them navigate complex digital transformations and leverage cloud and AI technologies to achieve business objectives. As a strategic thinker, he blends deep technical expertise with a strong understanding of business goals, to enable long-term growth for organizations. Bhashwanth can be reached at https://www.linkedin.com/in/bhashwanth/

Email
Firewall
The latest version is ready to install now.
Please update to continue.
Update
Not now
Details

Cybersecurity Solutions for Small Businesses: Cost-Effective Strategies to Stay Secure

By Vishal Vasu, Chief Technology Officer, Dev Information Technology Ltd

In today's fast-paced digital landscape, small businesses are increasingly becoming prime targets of cyber-attacks. While large enterprises invest heavily in security infrastructure, many small and medium-sized businesses (SMBs) operate with limited resources and lower awareness of cyber risks. However, the reality is that no organization is too small to be compromised. Adopting tailored, affordable cybersecurity strategies is a mandate in the modern era.

This blog is specifically targeted for a cost-effective cybersecurity services and solutions tailored for small businesses, ensuring the operations are not disrupted.

Cybersecurity Challenge for Small Businesses

Small businesses often believe they're too small to be noticed by hackers. Unfortunately, that belief can be costly. According to research by Kaspersky, nearly 43% of cyberattacks target small businesses. From phishing scams to ransomware, the range of cyber threats is both broad and damaging.

Understanding the threats is the first step to create a stronger defense. They are as follows:

- **Phishing attacks**: Fake emails or websites trick employees into sharing sensitive data.
- **Ransomware**: Malicious software that locks systems or data until a ransom is paid.
- **Insider threats**: Employees, either malicious or negligent, who compromise security.
- **Data breaches**: Unauthorized access to confidential customer or business data.

Each of these can have devastating impacts in the form of lost revenue, reputational damage, and potential legal penalties.

Why is the focus on SMBs?

The hackers view them as easier targets, often due to weak security posture, legacy applications, or lack of in-house expertise. In order to avoid loss of data or financial fraud, proactive measures should be made beforehand.

Most Common Cyberattacks on Small Businesses

Attack Type	Percentage of Incidents
Malware	18%
Phishing	17%
Data Breaches	16%
Website Hacking	15%
DDoS Attacks	12%
Ransomware	10%

Affordable Cybersecurity Strategies That Work

Despite having a constraint in the budget, SMBs can still implement effective security measures. There are several affordable cybersecurity strategies that strike the right balance between protection and cost. Effective, budget-friendly practices aligned with the five pillars of cybersecurity.

1. Know What You Have and Who's Using It

Before you can protect your assets, you need to understand what is residing in your environment.

- Implement a centralized Inventory of Assets (hardware, software, cloud resources).
- Use Identity and Access Management (IAM) to control who accesses what.
- Establish a "source of truth" system for tracking users, devices, and applications (e.g., Azure Active Directory).
- Audit user privileges regularly to reduce unnecessary access.

2. Safeguard Your Assets

Once you know what protection needs, build defense layers accordingly.

- Use Antivirus and Endpoint Detection & Response (EDR) tools like Microsoft Defender for Business or CrowdStrike.
- Enable Multi-Factor Authentication (MFA) across all business applications.
- Encrypt sensitive data (Data at rest and transit) using built-in tools (BitLocker, Thales CTE).
- Apply security patches and software updates consistently with automation tools.

3. Identify Threats Before Damage Happens

Early detection limits the scope of damage and shortens response time.

- Set up real-time alerting through open source SIEM solution like Wazuh
- Monitor user and device behavior to flag anomalies.
- Schedule regular log reviews or use managed detection services that offer alerts.

4. Act Quickly When Incidents Occur

A good response plan minimizes confusion and speeds up containment.

- Create a Cybersecurity Incident Response Plan (CIRP) using free templates from NIST or ISO27001.
- Designate incident response roles and responsibilities ahead of time.

- Use predefined playbooks to guide containment and communication steps.

5. Bounce Back Stronger After an Attack

Resilience is the key. Be ready to restore operations promptly.

- Use Azure Site Recovery to replicate workloads and ensure quick business continuity.
- Regularly test backup and restore procedures to validate readiness.
- Document post-incident lessons learned to improve future defenses.

The ROI of Investing in Cybersecurity

Many SMBs still perceive cybersecurity as a cost center. But it's really an investment in resilience. A single breach can cost over $120,000—enough to bankrupt many small firms.

Strong IT security for SMBs helps ensure:

- Customer trust remains intact.
- Operations continue without costly disruptions.
- Regulatory and legal standards are met.

Effective cybersecurity services and policies help small businesses thrive in an increasingly hostile digital environment.

Final Thoughts: Building a Resilient SMB

Cybersecurity is no longer a luxury; it's a necessity. With a thoughtful approach grounded in the five pillars: Identify, Protect, Detect, Respond, and Recover

The small businesses can establish a solid defense posture that scales with them.

Whether you're investing in employee training, managed services, or cloud-based Cybersecurity Service and Solutions, the key is action. Don't wait for an incident to be your wake-up call.

By implementing the strategies outlined above and aligning them with a layered security framework, even the leanest SMB can stand strong in the face of evolving cyber threats.

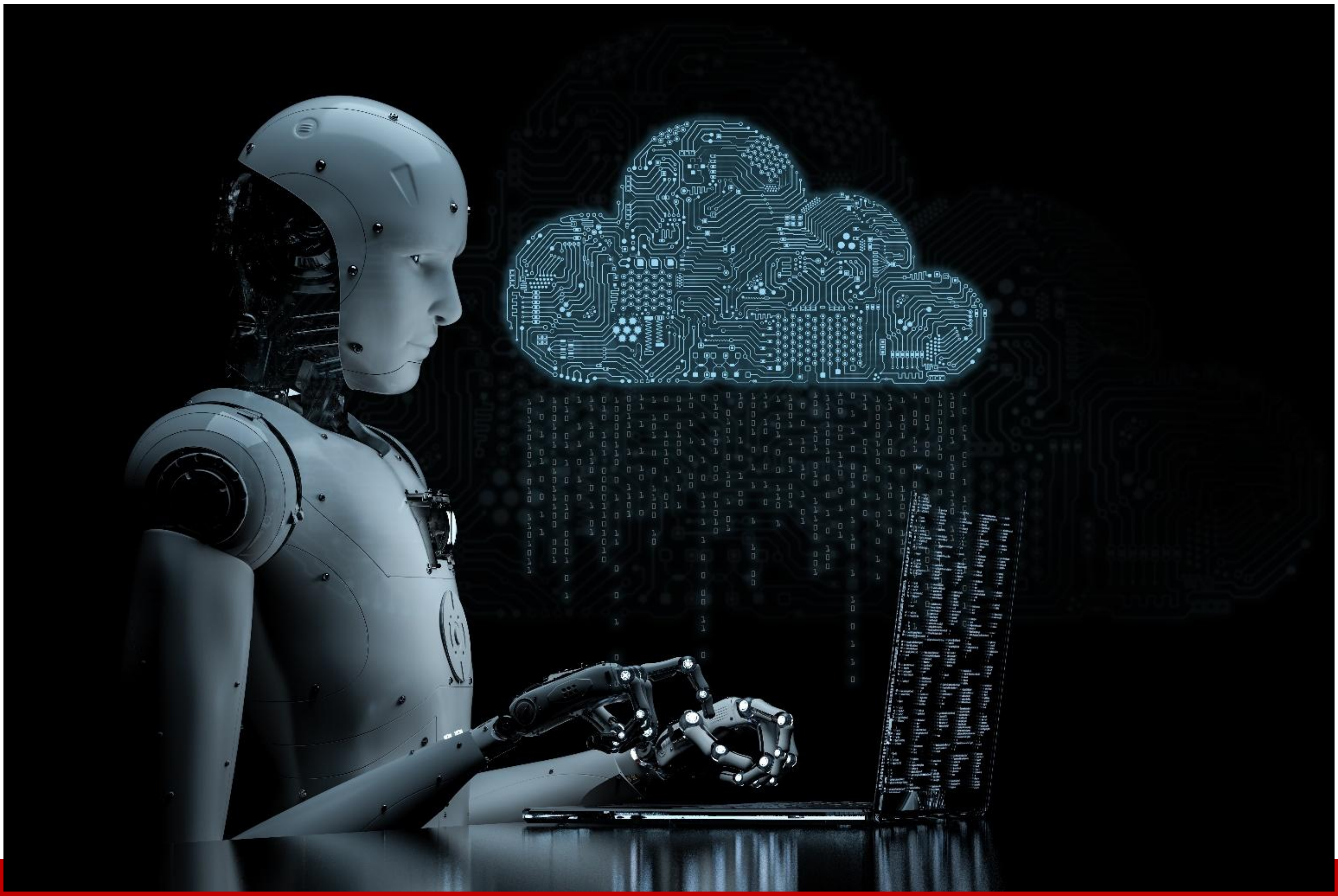
Leveraging cloud-based tools, today's IT security for SMBs doesn't have to be expensive to be effective.

Staying secure is no longer optional: it's a core part of doing business in the digital age.

About the Author

Vishal Vasu is Director and Chief Technology Officer (CTO) at Dev Information Technology Ltd (DEV IT) and leads the company's Technology and Innovation ecosystem. He is responsible for managing DEV IT's innovation portfolio and creating new growth drivers for the company. In addition to planning and executing DEV IT's technology roadmap and strategy, he is also fanatic about driving innovation through Research & Development activities in DEVLabs (internal R&D division). Vishal also provides technical direction across the company in areas of managed services, architecture designs, software technology, and cybersecurity supporting project development and business growth. Along with this, he also leads the Information Technology function at DEV IT, including its infrastructure, systems, processes, and security

Vishal can be reached online at https://www.linkedin.com/in/vishalvasu/



Securing AI at Its Core: Protecting Data and Models with Fully Homomorphic Encryption

By Luigi Caramico – CTO and Founder, DataKrypto

Organizations today are rushing to adopt AI without fully appreciating the profound cybersecurity risks involved. The reality is stark: accidental data leaks, sophisticated adversarial attacks, and the theft or reverse engineering of proprietary AI models are not distant possibilities—they are immediate threats.

AI's greatest strength is its insatiable appetite for data, but each data point it absorbs simultaneously becomes a vulnerability. As AI systems become more intelligent, they also become increasingly valuable—and thus increasingly targeted.

Addressing this emerging security landscape requires more than conventional perimeter defenses and access controls. Organizations must rethink their cybersecurity approach to prioritize protecting the AI models themselves and the sensitive data these models consume.

The Paradox of AI Data Management

The effectiveness of AI models depends entirely on the data they process. Yet, the datasets fueling these models often include highly sensitive information such as medical records, financial transactions, intellectual property (IP), and personally identifiable information (PII).

One significant yet frequently overlooked risk arises when proprietary data—trade secrets, source code, product strategies—is directly integrated into AI models during training or fine-tuning. Without robust security measures, these critical assets may inadvertently become embedded in a model's structure, leaving them exposed to extraction through model inversion attacks, prompt leakage, or reverse engineering.

Such data leaks can inflict severe competitive damage, erode investor trust, and trigger regulatory repercussions. These risks aren't theoretical; businesses across sectors have already begun experiencing their consequences.

Why Traditional Security Isn’t Enough for AI

Current cybersecurity measures, like endpoint security, identity management, and perimeter firewalls, remain crucial, but they were never designed for the unique operational characteristics of AI systems.

Traditional methods adequately protect against known threats like malware or unauthorized access, but fall short in securing AI's distributed and data-dependent environments.

A new security paradigm is essential—one that secures the AI lifecycle end-to-end, safeguarding the integrity of data and models rather than merely the infrastructure around them.

Introducing Fully Homomorphic Encryption (FHE)

Fully Homomorphic Encryption (FHE) represents a revolutionary shift in data security. Unlike traditional encryption, FHE allows data to remain encrypted throughout the entire computation process. As a result, AI models can train, learn, and infer without ever exposing sensitive data.

By combining FHE with hardware-backed Trusted Execution Environments (TEE), it is possible to create an unparalleled secure computing framework:

- **TEE-Enforced Encryption:** Encryption keys exist exclusively within the TEE, never exposed externally.
- **Always Encrypted Models:** AI models remain encrypted at every stage, from initial training to ongoing inference.
- **Encrypted Processing:** Intermediate results, model gradients, and outputs never appear in plaintext, even internally.

This approach ensures a zero-trust, zero-knowledge environment where sensitive information remains completely secure, even across distributed or cloud-based infrastructures.

Benefits of End-to-End AI Encryption

This integrated approach offers numerous strategic benefits:

- **Isolation of Proprietary Data:** Critical IP and sensitive information remain continuously protected throughout the AI lifecycle.
- **Controlled Key Management:** Keys are securely stored within TEEs, preventing potential leaks through memory exploits or insider threats.
- **Model Protection:** Encrypted AI models are unusable if exfiltrated, safeguarding against theft and unauthorized usage.
- **Regulatory Compliance:** Compliance with stringent standards like GDPR and the EU AI Act is achieved seamlessly, without sacrificing operational efficiency.
- **Secure Collaboration:** Enterprises can collaborate across external platforms without risking exposure of internal datasets or proprietary model logic.

Combining New Technologies with Proven Practices

A secure AI strategy doesn't replace traditional cybersecurity—it complements it.

Enterprises must integrate foundational cybersecurity measures such as endpoint protection, access management, and network monitoring with advanced encryption techniques to achieve comprehensive protection.

Incorporating FHE transforms sensitive data from a potential vulnerability into a continuously secure asset, enabling organizations to innovate without fear of exposure or compromise.

Building Trust: Essential for AI's Future

Trust is fundamental to successful AI deployment. Regulators, partners, and customers must have absolute confidence in the security and integrity of AI systems. Demonstrating responsible AI management by protecting sensitive data and proprietary models strengthens trust, enabling greater innovation and collaboration.

Industries such as healthcare, finance, and critical infrastructure require uncompromising data security. FHE enables secure AI-driven services like fraud detection, personalized medicine, and infrastructure protection without sacrificing data privacy. As global regulations tighten, secure-by-design AI isn't merely beneficial—it's indispensable.

The Future: The Encrypted Enterprise

As AI continues evolving into a central repository of organizational knowledge and decision-making processes, it becomes critical to treat AI as a core operational asset. Protecting AI through FHE today lays the groundwork for a broader application of encryption throughout the enterprise—extending secure computing practices to analytics, search engines, contract negotiations, simulations, and decision-making systems.

The encrypted enterprise represents the future of secure digital transformation, and that journey starts now—by securing AI at its very core.

About the Author

Dr. Luigi Caramico is the Founder and CTO of Datakrypto. He holds a research doctorate with a degree in computer science. Moving to Silicon Valley in 2000, where he currently lives and works, he is the founder and CTO of Datakrypto, Inc. Information on the company is posted at https://www.linkedin.com/company/datakrypto

Detecting and Defeating Synthetic Identity Fraud

By Husnain Bajwa, Senior Vice President, Product, SEON

Synthetic identity fraud is one of the most complex and challenging threats facing financial institutions today. Unlike traditional identity theft, synthetic identity fraud combines real and fabricated information to create entirely new, fictional identities that can bypass conventional security measures.

Synthetic identity scams exposed lenders to approximately $3.1 billion in potential losses in 2023, and the Federal Reserve raised alarms last month about its rapid acceleration. Exact costs are difficult to isolate but many sources believe this form of fraud is responsible for somewhere between $20 to $40 billion dollars. As fraudsters leverage increasingly sophisticated techniques, including generative AI, organizations must understand this evolving threat landscape and implement strong, multi-layered defense strategies to protect their operations and customers alike.

The Elusiveness of Blended Identities

Synthetic identities present unique detection challenges precisely because they operate in a gray area between real and fake. Fraudsters carefully craft these “frankenstein IDs” by combining stolen legitimate information, typically Social Security numbers, with fabricated names, birthdates, addresses and other contact details. This blending of information creates identities that appear authentic enough to pass initial verification checks while remaining disconnected from any real person’s complete profile.

Their ability to evade traditional fraud monitoring systems make these synthetic constructs particularly dangerous. Unlike stolen identities that trigger alerts when a real person reports unauthorized activity, synthetic identities have no corresponding victim to flag any of the suspicious behavior. This gap allows fraudsters to operate undetected for extended periods, sometimes years, as they methodically build credit profiles and establish legitimacy before executing their end goal fraud schemes.

Business Ramifications Beyond Financial Losses

The consequences of synthetic identity fraud extend beyond immediate monetary losses. Organizations that fall victim to these types of schemes face multilayered impacts that compound over time. Financial institutions often lose the direct value of fraudulent loans and credit lines and incur significant operational costs associated with investigating complex fraud cases that lack clear victims.

In addition, synthetic identity fraud can create regulatory exposure and compliance challenges as organizations struggle to explain how fictitious customers passed their Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols. As fraudsters typically abandon their synthetic identities after maximizing their illicit gains, financial institutions face charge-off rates that damage their credit portfolio performance and undermine investor confidence. The reputational damage from widespread synthetic fraud can be particularly devastating in an industry where trust forms the foundation of customer relationships.

Advanced Detection Strategies for Modern Protection

To combat this form of fraud, organizations today must implement advanced machine learning and artificial intelligence (AI) systems capable of analyzing behavioral patterns and identifying anomalies that might indicate synthetic identity use. These systems can detect subtle inconsistencies across application data, transaction history and account activity that humans might miss.

Document and biometric verification technologies provide another critical protection layer against synthetic identities. While fraudsters can fabricate personal details that pass basic credit checks, they typically cannot produce genuine identity documents matching their synthetic personas. Implementing robust document verification alongside biometric confirmation creates barriers for fraudsters. Cross-referencing data across multiple sources and establishing consortium models for sharing fraud intelligence among industry participants can further strengthen detection capabilities and reduce fraud exposure.

Building Organizational Resilience Against Synthetic Fraud

Creating effective organizational defenses against synthetic identity fraud requires balancing security with operational efficiency. Security teams must implement continuous monitoring systems that track account activity over time, not just at the point of application. This longitudinal approach helps identify the telltale patterns of synthetic identity "nurturing," where fraudsters gradually build credit profiles before exploitation.

Employee training represents another critical component of defense. Customer-facing staff and risk analysts need specific education about synthetic identity red flags, such as thin-file credit applicants with inconsistent documentation or unusual application patterns. By combining technological solutions with human expertise, organizations can create a more resilient system to fight against these types of sophisticated fraud schemes to better protect financial assets and maintain customer trust.

The Answer: Technology & Humans

As synthetic identity fraud continues to evolve, cybersecurity professionals must stay ahead of fraudsters by implementing comprehensive detection strategies that combine advanced technologies with human expertise. By understanding the unique challenges these blended identities present and deploying multilayered verification approaches, organizations can significantly reduce their vulnerability to this turbulent threat landscape.

About the Author

Husnain Bajwa is a fraud and risk technology leader with over 30 years of experience in cybersecurity, enterprise cloud platforms, and critical infrastructure. As SVP of Product - Risk Solutions at SEON, he drives innovation in fraud prevention and compliance. Previously, he held leadership roles at Beyond Identity, Hewlett Packard Enterprise, Aruba Networks, and Ericsson, focusing on secure, scalable solutions. Husnain is a recognized voice in risk management, advocating for data-driven, adaptive strategies to combat digital fraud while ensuring compliance in an evolving threat landscape.

Domain Generation Algorithms (DGAs) and Fast Flux DNS: Evasive Tactics in Modern Malware

By Abiodun Adegbola, Security Engineer, Systal Technology Solutions

Modern malware programs employ sophisticated techniques to maintain persistent command and control (C2) communication with infected hosts while evading detection by security measures. Among these techniques, Domain Generation Algorithms (DGAs) and Fast Flux DNS stand out as particularly effective in establishing resilient and highly available communication channels. These two techniques represent a significant challenge for defenders, as they create a highly dynamic and evasive infrastructure that can bypass static blacklists and IP-based blocking mechanisms. Understanding the intricacies of DGAs and Fast Flux DNS is, therefore, crucial for developing effective detection and mitigation strategies against contemporary malware threats.

Understanding Domain Generation Algorithms (DGAs)

DGAs function as an algorithm embedded within malware, designed to dynamically generate a vast number of seemingly random domain names. The primary purpose of employing a DGA is to provide attackers with an agile and unpredictable set of domain names that can be used for their command and control (C2) infrastructure. This constant flux of potential communication endpoints makes it exceedingly difficult for defenders to block malware communication by simply blacklisting specific domain names. By the time a malicious domain is identified and added to a blacklist, the malware may have already switched to using a different, newly generated domain. This necessitates a shift in defensive strategies from reactive blocking to more proactive and analytical approaches. Various types of DGAs exist – PRNG, Character, Dictionary, Adaptive - each with its own unique characteristics and level of sophistication.

Fast Flux DNS: A Cloaking Technique for Cybercriminals

Fast Flux DNS is another significant evasive technique employed by malware authors to conceal C2 infrastructure and subsequent malicious operations. The Fast Flux network concept was first introduced in 2006, with the emergence of Storm Worm malware variants. It is characterized by a single domain name that has multiple IP addresses associated with it, and these IP addresses change very rapidly and frequently. The primary role of Fast Flux is to hide the actual location of malicious activities, such as C2 servers, by distributing them across a large and dynamic network of compromised hosts, often forming part of a botnet. This rapid rotation of IP addresses makes it exceedingly difficult for defenders to block access to the malicious infrastructure based on IP addresses, as any identified and blocked IP address is likely to be replaced by a new one within a short period.

There are variations of the Fast Flux technique. **Single flux** involves a single DNS A record associated with multiple IP addresses that change frequently. This is the most basic form of Fast Flux. **Double flux** provides an additional layer of obfuscation by rapidly changing not only the A record but also the Name Server (NS) records associated with the domain. This makes it more challenging to track the authoritative source of DNS information for the malicious domain. The dynamic nature of both the IP addresses and the authoritative name servers significantly increases the resilience of the malicious.

Mitigations

Combating the evasive tactics of DGAs and Fast Flux DNS requires a layered security approach employing various countermeasures. These include:

- **Machine learning-based detection:** Utilizing machine learning models trained to identify patterns indicative of DGA and Fast Flux activity.
- **Threat intelligence:** Leveraging feeds of known malicious domains and IP addresses associated with these techniques.
- **Protective DNS solutions:** Filtering DNS requests to block access to identified malicious domains and IPs.

- **Sinkholing:** Redirecting DNS requests for DGA-generated domains to controlled servers for analysis.
- **Enhanced logging and monitoring:** Increase logging and monitoring of DNS traffic and network communication to identify domains with an unusually high frequency of IP address updates, characteristic of Fast Flux.
- **Monitoring DNS records for short TTL (Time-To-Live) values:** Detecting the use of very short TTLs, often employed in Fast Flux configurations.

Conclusion

DGAs and Fast Flux DNS are powerful evasive techniques used by malware for command and control communications. Their dynamic nature, involving constantly changing domains and IP addresses, makes traditional security measures less effective. To safeguard their infrastructure and mitigate the evolving threats of DGAs and Fast Flux DNS, organizations must implement a robust DNS security strategy that integrates threat intelligence and leverages machine learning alongside advanced detection technologies.

About the Author

Abiodun Adegbola is a Security Engineer at Systal Technology Solutions, a global specialist in managed network, cloud and security services. He brings over seven years of various experience into the global security operations team within Systal. He is certified across various technologies and holds a BTech in Computer Engineering from LAUTECH, Nigeria and MSc in Advanced Security & Digital Forensics from Edinburgh Napier University, UK. Abiodun can be reached online at https://www.linkedin.com/in/abiodunadegbola/ and at company website https://systaltech.com/

Drowning In 130 Tools: Security's Real Resource Gap

Security teams are shrinking. Threats are not.

By Shai Mendel, Co-Founder & CTO, Nagomi Security

The global cybersecurity workforce is short 3.5 million people with more than 750,000 open roles in the U.S. alone. Even government agencies like CISA are cutting budgets and staff. Yet despite having fewer hands on deck, most teams are seeing more threats, not fewer: 72% of CISOs say the volume of attacks has increased in the past year.

On top of this, the average enterprise now runs 130 security tools at once. Instead of clarity, teams face complexity. And instead of confidence, they face fatigue.

This isn't just a staffing or budget issue. It's a strategy problem. Teams don't need more tools – they need to get more from what they already have.

Start With the Threat, Not the Tool

Security strategies too often begin with technology: a new tool, a new dashboard, a new capability that promises better coverage. In fact, security spending has climbed from 8.6 percent to 13 percent of total IT budgets over the past five years. But when teams lead with tools instead of threats, they end up managing noise, not risk.

To break the cycle, teams need to flip the model. Start by identifying the actual threats your organization faces whether it's phishing, ransomware, a specific seen in the wild campaign, or something else entirely. Then map those threats to your existing controls. What's covered? What's redundant? Where are the blind spots?

This threat-to-control mapping gives teams a clearer picture of what matters and reveals where their stack is working *against* them by creating alert fatigue, friction, or false confidence.

Action step: Build or refresh your threat model, then align each major security control to a specific tactic or technique you're trying to defend against. If you can't draw a clear line from tool to threat, it's time to reassess. Then take it a step further: map coverage and (mis)configurations to each control. That extra layer of visibility is where real differentiation happens.

Once teams have mapped their controls to real threats, the next challenge is scale. Doing this once is helpful. Operationalizing it across dozens, or hundreds, of tools is where the real value lies.

Continuous threat exposure management helps make that possible. It brings visibility into how well your existing controls align to the threats you've identified, across your entire environment. Instead of switching between platforms or managing tools in isolation, teams can get a unified, up-to-date view of what's covered, what's misconfigured, what's vulnerable, and where critical gaps remain.

That kind of clarity is often what separates a near miss from a major breach. In many attacks, the defenses needed to stop the threat were already in place, but they weren't actively managed, tuned to the threat, or surfaced in time to take action. Continuous threat exposure management helps organizations move from passive coverage to active assurance.

Cut Complexity Before You Cut Headcount

Once you've mapped your controls to real threats, chances are some tools won't hold up. But that doesn't mean you start slashing immediately. Cutting tools without a plan can create more gaps than it closes.

130 tools means 130 places to look when something goes wrong. It also means siloed data, duplicated capabilities, and wasted time switching between systems. Simplifying the environment starts with identifying where effort and value don't align: where are teams spending the most time for the least impact?

Instead of slashing budgets or downsizing blindly, organizations should invest in rationalizing workflows: assess the ROI of each security tool, maximize their coverage and optimize their effectiveness.

Action step: Rationalize your tool stack based on deployment, configurations and vulnerabilities. What tools are not covering key assets? What tools are not properly configured? Which capabilities do I actually have but I don't use?

Prove Impact with Clarity, Not Scale

Boards and business leaders want to know: are we safer? Security teams need to answer that question without defaulting to more spend or more dashboards.

That means shifting the conversation from "how many alerts we closed" to "what threats we prevented." The sheer volume of activity - escalations, scans, detections - doesn't reflect effectiveness. Clear, outcome-driven metrics tied to threat reduction give teams the leverage to defend their strategies, secure budgets, and avoid reactive investments.

But proving impact requires a language the business understands. Rather than overreporting on technical activity - like alert counts or log volume - security leaders should focus on the risks they've actually reduced, their preparedness to real threats, and how coverage is evolving.

What this looks like in practice:

- % of MITRE ATT&CK techniques actively covered
- Increased effectiveness of security controls - in terms of coverage, configurations and vulnerabilities
- Reduction in overlapping or underutilized tools
- Ratio of preventive to reactive spending across the security budget

These kinds of metrics help leadership see what matters: how controls are closing gaps, reducing exposure, and improving resilience over time. They also give CISOs a stronger position when making hard decisions: what to streamline, where to invest, and how to stay focused under pressure.

Fewer tools and people, less security debt: these aren't signs of weakness. If what remains is strategic and measurable, it's a sign of maturity. In a constrained environment, clarity is the new scale and the best-performing teams will be those who can show exactly how they're defending what matters most.

Action step: Identify three metrics your team reports on today that measure *activity*, and replace them with metrics that measure *impact*, specifically tied to threat mitigation, dwell time, or risk reduction. Bring those to your next board or budget discussion.

The Bottom Line

Security teams don't need more tools, more dashboards, or more noise. They more than likely have what they already need and simply need to make it effective.

In a landscape defined by resource constraints and rising threats, the strongest programs won't be the most complex, they'll be the most aligned. Aligned to the threat landscape. Aligned to what actually reduces risk. Aligned to metrics that matter.

Resilience today isn't about scaling up. It's about stripping away what doesn't serve a purpose and doubling down on what does.

About the Author

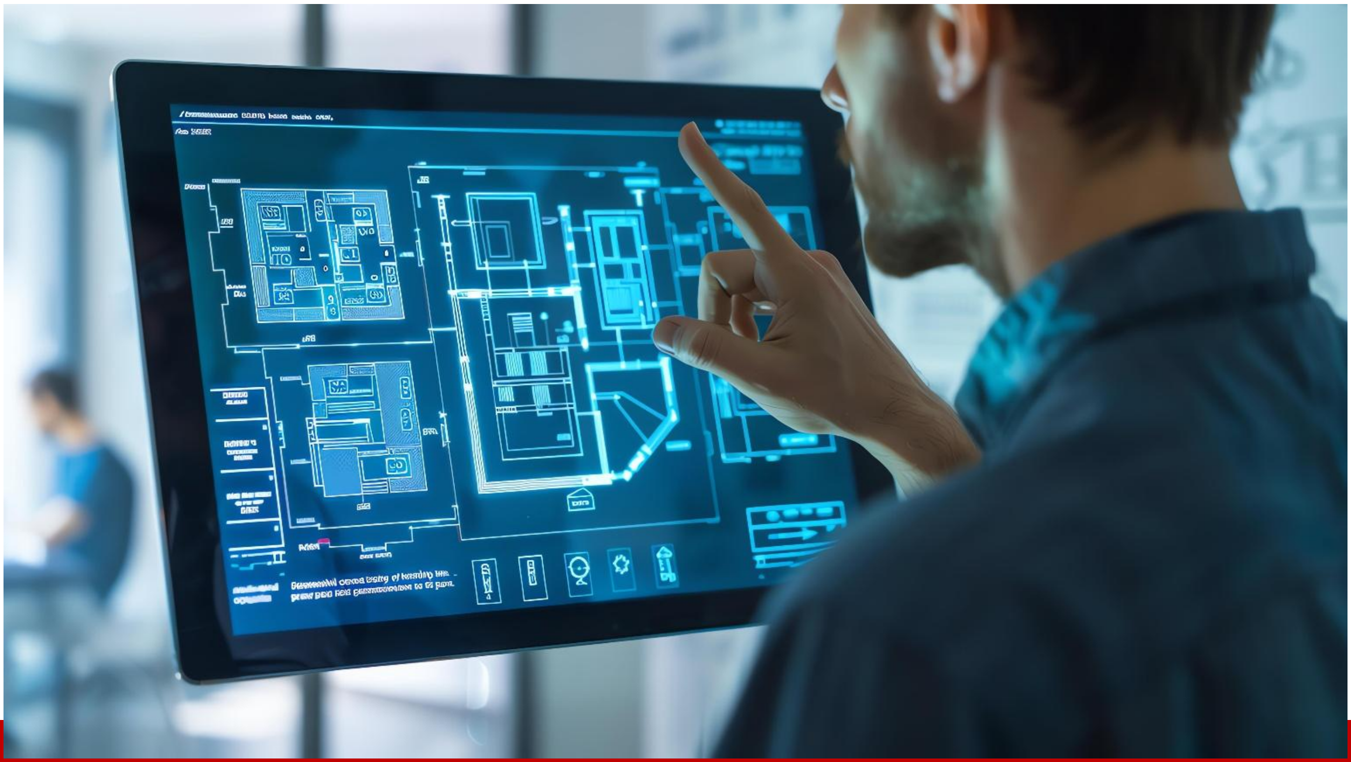
Shai Mendel, Co-Founder & CTO, Nagomi Security, brings over a decade of deep technical expertise and leadership experience in cybersecurity. He began his career as a software engineer and researcher in the Prime Minister's Office, where he worked for six years, contributing to high-level national security projects.

Shai's entrepreneurial journey took off when he joined XM Cyber as the first engineer, where he played a pivotal role in building the product from the ground up. As the company's first Engineering Manager, Shai also spent 25% of his time in customer-facing roles, ensuring that the product aligned with real-world needs and solving complex cybersecurity challenges.

Later, Shai joined Snyk to build its second product focusing on Containers and Kubernetes security. Starting as an Engineering Manager and later advancing to Director of Engineering, he grew his team to dozens of engineers and architects, directly contributing to approximately 20% of Snyk's revenue at the time.

Shai holds an M.Sc. in Computer Science from Tel Aviv University, and his technical acumen, combined with his leadership product development, drives Nagomi's mission to deliver innovative effective cybersecurity solutions.

Shai can be reached online at LinkedIn and at our company website https://nagomisecurity.com/.



Engineering Challenge: Smart Positioning System

By Milica D. Djekic

Transitioning from intelligent to smart technologies has been a long way as it has taken decades of dedication. Navigating industry posture and refining technical endeavors in ever-evolving surrounding have played a pivotal role. With intelligent systems development, it is possible to govern solution, using feedback control that is well-researched concept in control theory. On the other hand, smart technologies are next-generation enhancements, balancing between technological requirements and security challenges.

Positioning systems have always provoked engineering communities through time, suggesting even the simplest control architectures needed to be innovated in era of their applications. Innovation is crucial for making anything sophisticated ever, unlocking heaps of opportunities to those who are prepared to invest into such explorations. Designing smart positioning system is an ultimate goal nowadays. Such research could serve in civilian, defense and even space industries, embracing immense convergence of Internet of Things (IoT) and Artificial Intelligence (AI) paradigms, usages and security needs.

IoT and AI go hand-to-hand and give some hope in many fields of human activities. Making IoT networks is a high demand, while dealing with AI might assure better effectiveness, faster data processing and more reliable defense in everyday routines. Challenge with AI is it is still dependent on accuracy of input information, providing less qualitative outcomes if incoming data is inadequate. Also, this means stronger bolster in case of wireless transmission of information, as well as more developed and deployed cloud computing. Smart positioning systems deeply rely on these concepts as age of novel technological frontiers is anticipated to arrive.

The Recent Challenge: Intelligent Positioning System

Intelligent positioning systems have begun developing about a couple of decades ago, streamlining completely new concept in control engineering. These systems have invoked feedback control, using some wired proximity sensors that can quite accurately determine position of rotating device. Such systems could deal with three elementary positions such as in, out and over, making an angle of up to 60 degrees between one another. Appeal for such improvement has come as the previous ON-OFF control needed to be replaced with something handier. This innovation at its very basic level includes:

- **DC Motor Setup**

DC motor is actuator of such feedback control system, giving driving force to mechanical part to move. As segment of feedback control, actuator usually serves as plant, receiving signal from its controller to perform as wanted.

- **DC Motor Controller**

This is only a purchased part, being in compliance with the rest of control system kit. It can govern behavior of actuator in real-time. When installing this testbed, it is very important to adjust all parts carefully – otherwise control system will not operate.

- **Wired Sensor's Network**

Usually, some smart switches and potentiometers are used to provide feedback information to controller. In addition, wiring issue is not resolved in this case as an entire setup still deals with many wires and cables, causing wireless transmission of information and control signal a bit trickery.

- **Signal Convertor's Testbed**

These systems apply digital-to-analog and analog-to-digital interface, looking for well-researched and developed AC/DC and DC/AC convertors.

- **Computer Application**

Good coding might seem as critical phase in making final solution as computer software is something that can guarantee a user-friendly experience.

Intelligent positioning systems are step forward in development and deployment of open-loop control technology. Yet, these systems are significantly improved, using wireless networking that might promise more convenient experience. In such case, smart positioning systems are that next generation, mainly relying on IoT approach.

- **The Ongoing Remark: Smart Positioning Solution**

With arising needs for copper and its reserves limitations, wiring issue has become a central concern. Even a few decades back, one of the greatest engineering challenges has been wireless transfer of information and energy. Smart technologies have overcome such problem, applying mid-range internet connectivity at homes and businesses. Such solution is very inexpensive, somewhat reliable and still pretty unsafe. In today's world of interconnected objects, wiring issue is highlighting two challenges such as limitation of resources and well-protected wireless systems. Apparently, some differences between intelligent and smart positioning systems might cover:

- **Wireless Sensor's Grids**

Cordless sensing networks have become top requirement for modern interconnected technologies, resolving packaging remarks and wiring issues. These networks truly innovate smart positioning systems that now communicate and send control signals at quite quick pace. Only drawbacks with these systems could be interference, range and coverage challenges, opening up totally new arena in science and engineering.

- **Cloud Computing**

Cloud computing infrastructures are still something extremely new in cyber industry, unlocking limitless options in both – data storage and information transmission field. These assets count on reliable and safe web connections, dealing with vast amount of data being managed by them. Computer programs might cope with cloud advancement in extremely bullish manner, streamlining smart positioning systems to spot of IoT networks and other smart technologies.

- **Feedback Control**

In closed-loop control, controller must be adjusted to desired value as plant could receive control signal and behave in wanted fashion, providing output information from wireless sensor's grid. This information is further compared with desired value at input and if error is zero, system operates with accuracy. Such new challenge if applying Wi-Fi signal for data exchange, is mostly implementation of IoT network to feedback control.

Encompassing smart positioning systems with IoT excellence is ongoing challenge nowadays. Smart positioning systems look for more innovations and better performances that could enhance their operability, functionality and security. This is strongly possible with new class of cutting-edge solutions.

The Overall Shift: Signal Processing Enhancement

In modern digital systems such as IoT network, it is necessary to put accent on much faster and more accurate signal processing. Enhancing these capabilities in binary data processing is from vital significance in sustaining such assets. With cloud technologies, large portion of data can be monitored, analyzed and detected, unleashing very comprehensive area to play in.

- AI-Powered IoT Networks: Opportunities and Open Questions

AI is good as long as input data are good, otherwise it can make a mess. On the other hand, if everything works flawlessly, some advantages of this technology can be considered. Applying AI in IoT grids is very critical as it can offer a lot of opportunities, as well as open up some questions. Synergy between AI and IoT can bring some feasibilities such as:

- Prompt data processing: It can accelerate signal analytics, accuracy and exchange.
- Better high-tech security: Some signal anomalies can be detected, analyzed and removed.
- Higher efficiency and effectiveness: Systems work smarter, not harder.

The Key Rally: Physical and Virtual Security Concerns

Physical challenges with smart positioning system can occur if factors like interference, space noise, vibrations and harsh working conditions are present. Therefore, virtual security is needed for better technical operability as hacked systems might get malfunctional. Assuring more reliable and better trusted functioning of smart positioning systems is central question that seriously corresponds with IoT network security.

Tips and Tricks for Further Research: Need of Long-Term Commitment

Here are some ideas how tomorrow’s smart positioning systems could be tackled:

A. Smart investment in both – software and hardware engineering.
B. Better and effective physical and cyber security assessments.
C. Long-term dedication in deserving innovations.
D. Intelligent selection of science and technology talents.
E. Meeting extremely high environmental safety and security requirements.

Final Thoughts

Positioning systems have challenged engineers, researchers and inventors over time. At present, making such systems is matter of emerging IoT paradigm. Indeed, these technological endeavors still need a commitment to be functional and cost-effective, liberating a plenty of safety and security challenges, too.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas press, and she is also the author of the books *"The Internet of Things: Concept, Applications and Security"* and *"The Insider's Threats: Operational, Tactical and Strategic Perspective"* being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology, and business. Milica is a person with disability.

Evolving Browser Security: Defending Against Advanced Phishing Threats in the Age of AI

By Sahil Dhir, Senior Risk and Security Manager, Amazon

Introduction

As we progress through 2025, the nature of phishing attacks has dramatically evolved. What was once limited to simple email scams has expanded into highly advanced, multi-faceted threats, leveraging artificial intelligence (AI) and deep fake technology to trick users. Modern phishing campaigns are now more complex, often spanning multiple channels and utilizing techniques that bypass traditional defenses. This growing sophistication means organizations must reassess their approach to browser security, as browser-based phishing attacks become a more prevalent and dangerous risk.

The Changing Face of Phishing

Phishing has evolved far beyond the traditional email scam. Today's attackers harness AI and deep fake technology to create highly realistic phishing attempts, often mimicking trusted organizations with astonishing accuracy. These campaigns use various methods, such as progressive web apps (PWAs), malicious browser extensions, and deceptive web components, to deliver their attacks. With these tools, attackers can embed threats within websites and browser notifications, which makes detection even more challenging.

What's more, these attacks are no longer confined to just one method. Modern phishing threats often combine multiple attack vectors, including fake login pages, fraudulent push notifications, and compromised browser extensions. The seamless integration of these tactics means that users are more likely to fall victim to phishing attempts before traditional security measures even have a chance to react.

Advanced Browser Security Strategies

To counteract these evolving threats, organizations are implementing cutting-edge security strategies within browser environments. The most widely adopted defense framework is the zero-trust model, which operates on the principle that no one, regardless of their location, should be trusted without continuous verification. This approach is being integrated directly into modern browsers, allowing for constant evaluation of users, devices, and sessions to ensure they are legitimate.

Additionally, browsers have been outfitted with advanced security features powered by AI, such as real-time URL reputation checks, dynamic content verification, and behavioral anomaly detection. These tools allow security systems to identify phishing attempts in real time, even as attackers use new tactics to bypass traditional defenses. By analyzing user behavior patterns and cross-referencing them with known threat intelligence, browsers can now offer more reliable protection from phishing and other malicious activities.

Global Implementation Barriers

While these advanced security measures offer significant protection, their implementation varies widely across regions, creating challenges for global cybersecurity efforts. Different countries and regions have distinct regulatory requirements, which can complicate the deployment of standardized security protocols. For example, in North America, organizations must navigate complex privacy laws, while in Europe, GDPR and other data protection regulations add another layer of complexity to any security strategy.

Moreover, in Asia-Pacific, organizations face challenges in managing cross-border data flows, while emerging markets often contend with infrastructure and resource limitations that prevent the widespread adoption of advanced security technologies. As a result, security strategies need to be tailored to specific regulatory environments, requiring businesses to remain flexible and adaptive.

Recommended Security Practices

For organizations looking to strengthen their defenses against browser-based phishing attacks, a multi-layered security approach is essential. The following practices should be integrated into every organization’s browser security strategy:

1. **AI-Powered URL Filtering**: Utilize AI-based tools to evaluate URLs in real time, ensuring that users are not directed to fraudulent or compromised sites.

2. **Behavioral Monitoring**: Continuously track user interactions to detect unusual patterns that may indicate phishing attempts.

3. **Contextual Authentication**: Implement multi-factor authentication (MFA) systems that assess not just the user's credentials but also contextual data such as device and location to determine the legitimacy of login attempts.

4. **Real-Time Threat Intelligence**: Integrate real-time threat feeds to stay updated on the latest phishing tactics and vulnerabilities.

5. **Automated Incident Response**: Establish systems that can automatically block malicious sites, notify users, and sync across browsers to ensure uniform protection.

By implementing these strategies, organizations can better anticipate and mitigate phishing attacks, even as they grow more advanced and sophisticated.

Preparing for the Future of Browser Security

Looking ahead, the future of browser security is shaped by several emerging technologies. Browser isolation, for instance, involves opening potentially dangerous websites in isolated virtual environments, preventing them from affecting the user’s system or accessing sensitive data. This method adds an extra layer of security by containing the threat.

Moreover, cloud-based security services and edge computing are revolutionizing how data is processed and analyzed for threats. These technologies allow for faster detection and response times, which are critical for combating the speed and scale of modern phishing campaigns.

Another crucial aspect of future-proofing browser security is user education. Organizations should implement ongoing security awareness training to help users recognize phishing attempts. Interactive modules simulated phishing campaigns, and real-time alerts can all contribute to creating a more security-conscious workforce, reducing the likelihood of successful phishing attacks.

The Role of Emerging Technologies

As we look to the future, several innovative technologies will continue to shape the direction of browser security:

- **Quantum-Resistant Cryptography**: As quantum computing becomes more powerful, organizations must adopt cryptographic methods that can withstand quantum-enabled attacks.

- **Decentralized Identity Verification**: This technology may eliminate the need for centralized password management systems, reducing the attack surface for phishing.

- **AI-Driven Threat Detection**: As AI and machine learning continue to improve, their ability to identify phishing threats will become more precise, using advanced pattern recognition and predictive analytics.

- **Extended Reality (XR) Security**: With the rise of virtual and augmented reality, new security challenges will emerge as phishing threats begin to target XR environments, requiring novel defense techniques.

Organizations must also remain mindful of changing regulations and compliance requirements. As new laws around AI and privacy emerge, security systems will need to adapt to ensure compliance, especially in regions with stringent data protection standards.

Conclusion

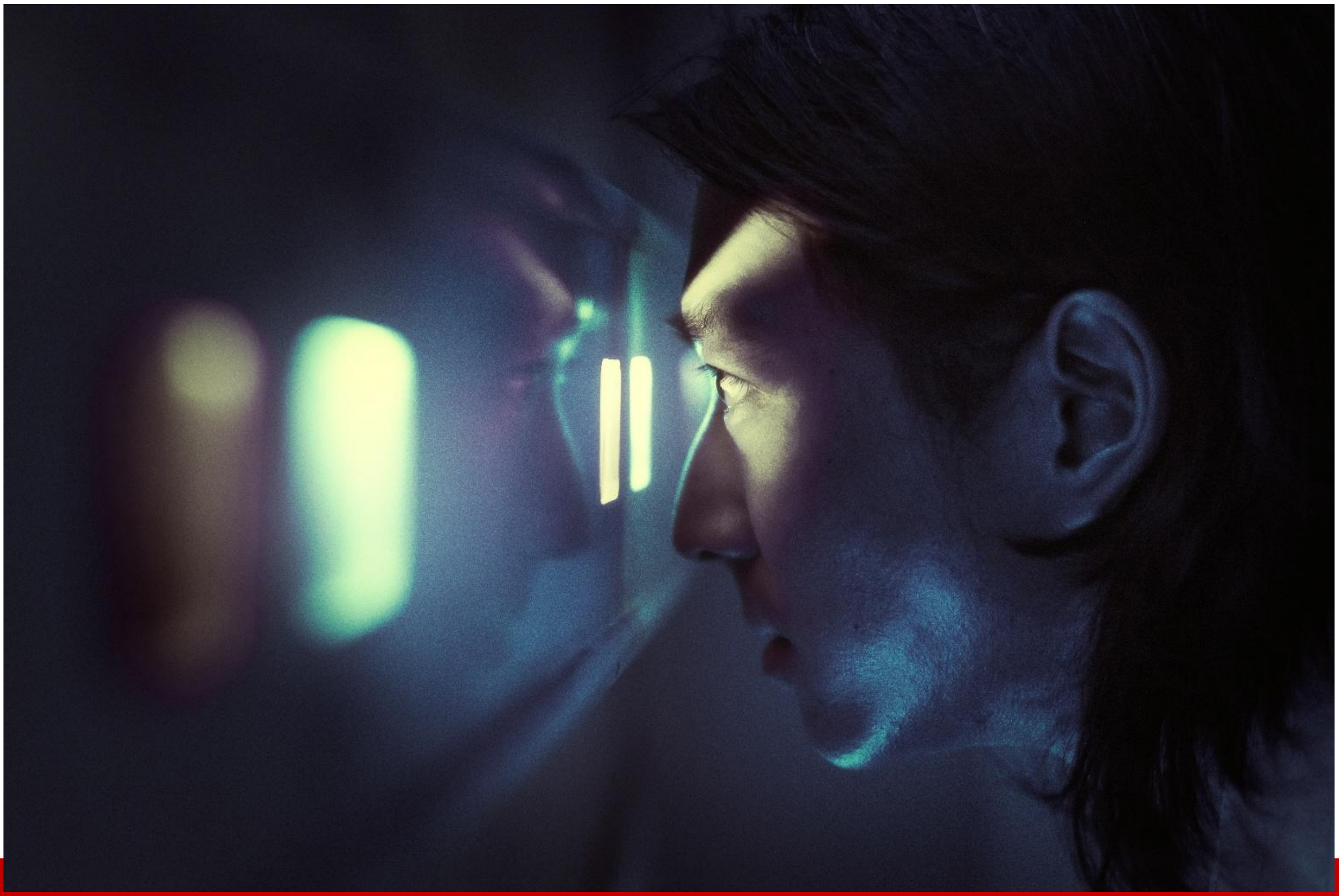
Phishing attacks are becoming more sophisticated, utilizing AI and multi-channel strategies to bypass traditional defenses. In response, organizations must adopt advanced browser security solutions, combining AI-driven technologies with user education to create a robust defense framework.

The road ahead will require continuous innovation in both security tools and organizational processes to combat these evolving threats. By maintaining a proactive, multi-layered security strategy, organizations can stay one step ahead of attackers and protect their users and data from increasingly complex phishing schemes.

About the Author

Sahil Dhir is a cybersecurity governance risk and Compliance leader with 14+ years of experience. Sahil has implemented and scaled GRC programs for multiple Fortune 500 companies during his tenure at Deloitte. Currently working as a Senior Risk and Security manager at Amazon, Sahil is spearheading the development and implementation of an enterprise-wide GRC tool. His expertise also extends to security assessments, security operations management, and security policy development, leveraging data-driven decision-making to address potential threats and vulnerabilities and to ensure company complies with relevant regulations including SOX, PCI and GDPR. Sahil enjoys staying up-to-date with offensive strategies used by attackers and building proactive risk management programs that serve as business enablers.

Sahil can be reached at https://www.linkedin.com/in/sahil-dhir-9370a238/



Think you’re Too Small to Be Hacked? Think Again. 5 Cyber Threats SMBs Need to Watch in 2025

By Tushar Sharma, Cyber Security Specialist, Cyber Guardians LLP

Running a small or mid-sized business is no joke. You wear every hat: sales, marketing, HR, operations—sometimes all before noon. But there’s one hat no one wants to wear: cybersecurity.

Here’s the thing: hackers know that. They know most SMBs don’t have security teams or the latest tech defenses. That makes you a target—not by accident, but by design.

Let’s talk about the real threats headed your way this year. No buzzwords. No scare tactics. Only what actually matters.

1. Ransomware Is Now DIY

You don't need to know how to code to launch ransomware anymore. With Ransomware-as-a-Service, bad actors can rent out attack kits like Netflix subscriptions. It's cheap, effective, and terrifyingly easy.

What you can do:

Have backups—real, working ones. Keep them offline. Also: don't give everyone admin rights. Seriously.

2. Phishing Scams You'll Actually Fall For

We're not talking about those laughable emails from a fake prince. Today's phishing scams are polished. They mimic your coworkers. Your boss. Even your vendors. And yes, some use AI and deepfakes.

What you can do:

Train your team. Run fake phishing tests. If you do one thing this year, let it be enabling MFA.

3. Cloud Blunders That Leave Your Data Hanging

Cloud platforms are amazing—until they're misconfigured. One small mistake, and sensitive files are publicly accessible. No hacker needed.

What you can do:

Review your cloud settings regularly. Use alerts for weird access. And don't give blanket permissions to everyone.

4. Your Partners Might Be Your Weakest Link

Let's be honest: you trust your payroll provider, your IT consultant, your software vendors. But what if they're compromised? That's how many breaches start.

What you can do:

Ask your vendors about their security practices. Put it in writing. And keep an eye on any third-party access to your systems.

5. AI Isn't Just for the Good Guys

Hackers are using AI to find vulnerabilities, automate attacks, and outpace defenses. It's not sci-fi anymore—it's happening now.

What you can do:

Invest in tools that don’t just scan for known threats—look for behavior anomalies. And more importantly, stay curious. Awareness is your first line of defense.

One Last Thing...

You don’t have to be a cybersecurity pro. But ignoring it? That’s not an option anymore.

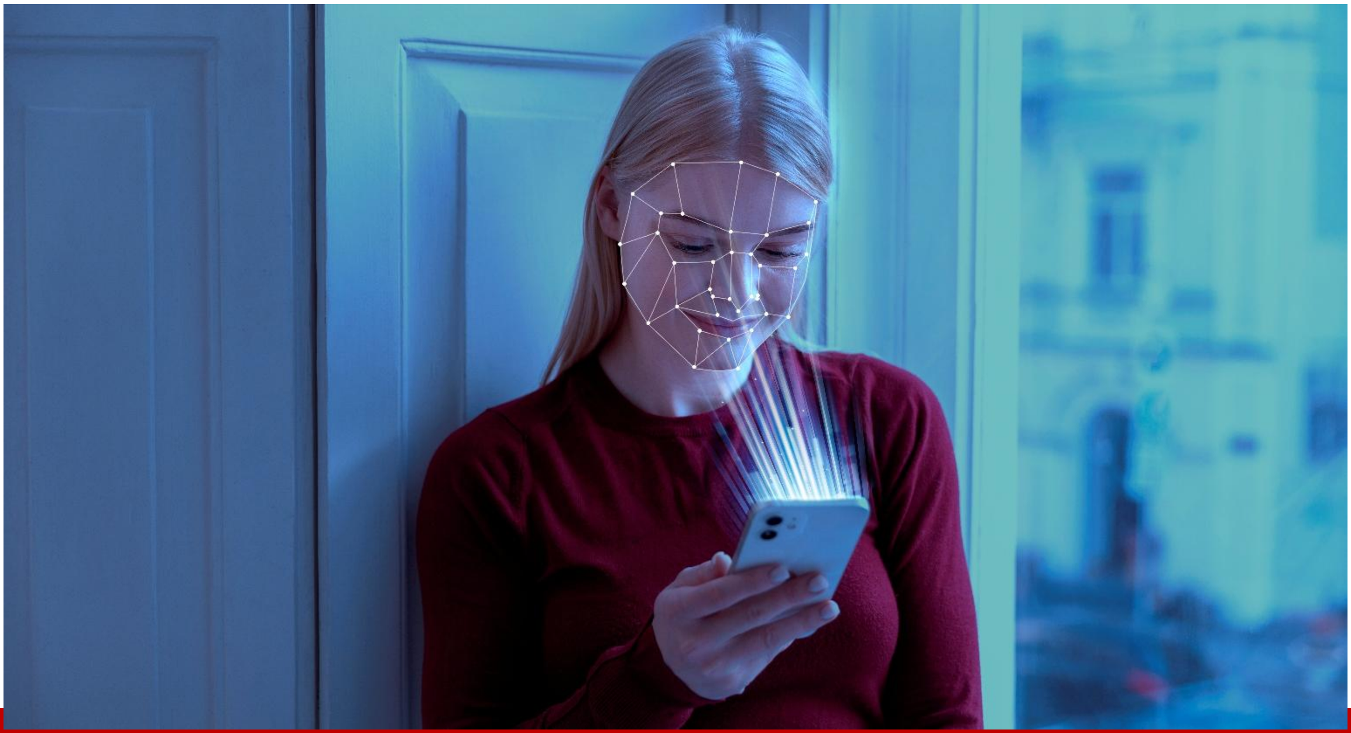
Start small. Secure your basics. Talk to your team. And remember: being a harder target than the next business might be enough to make attackers move on.

You’ve got this.

About the Author

Tushar Sharma is a Cyber Security Specialist at Cyber Guardians LLP, where he helps small and mid-sized businesses strengthen their digital defenses. He focuses on threat detection, cloud security, and practical risk reduction strategies

Tushar Sharma can be reached online at Tushar@cyberguardians.in and at our company website https://cyberguardiansglobal.com



Fortifying Digital Frontlines for a Post-Quantum World

By Bhagwat Swaroop, President, Digital Security Solutions at Entrust

Quantum computing is rapidly moving from theory to reality – and with it comes the power to break today's cryptographic systems. The timeline for viable quantum machines is accelerating, with Google recently revealing it could be as little as five years before practical quantum applications become a part of everyday life. While the potential of quantum computing is exciting, it also yields significant risks. As the post-quantum future nears, the window for enterprises to address those risks is rapidly closing.

The urgency is compounded by the rise of generative AI, growing digitization, and our increasing dependence on mobile-first ecosystems – where 92% of apps still rely on insecure encryption. At the same time, cryptographic sprawl has taken root: encryption keys, certificates, and secrets are scattered across decentralized, cloud-heavy environments with little visibility or governance.

In this complex new environment, enterprises face a stark choice: evolve or fall behind. Preparing for the quantum shift begins with rethinking cryptographic management, starting with visibility, centralization, and agility. The time to act is now.

Combating the Cryptographic Sprawl

Before defending against quantum threats, enterprises must tackle a more immediate challenge: cryptographic sprawl.

As digital transformation accelerates, cryptographic assets – including keys, certificates, and secrets – have spread across cloud environments, mobile devices, and internal systems. Many remain unmanaged, untracked and forgotten. Most companies lack real-time visibility into where these credentials live, whether they're still valid, or if they comply with internal policies. For example, machine identities currently outpace the human workforce by a ratio of 45 to 1, generating a large attack surface that leaves organizations vulnerable to cyberattacks. This explosion of digital identities has dramatically expanded today's attack surface, making visibility into the cryptographic estate essential.

The ability to protect your environment starts with understanding it. Without a comprehensive inventory of cryptographic assets, organizations can't identify vulnerabilities or prepare for a seamless migration to post-quantum cryptography. Closing the visibility gap is the first and most critical step toward crypto-agility — and long-term resilience.

Achieving Crypto-Agility

With visibility into cryptographic assets established, organizations can shift gears to prioritize crypto-agility. This refers to an organization's ability to rapidly pivot encryption methods and key management processes as new vulnerabilities emerge or regulations change. In a world where quantum threats evolve faster than most companies can react, crypto-agility is no longer optional – it's essential.

At the heart of agility is automation. Manual processes simply can't keep up with today's threat landscape. Automated key rotation, algorithm swaps, and policy enforcement are now the foundation of a resilient cryptographic strategy.

But agility alone isn't enough. It must be paired with cyber resilience – the ability to anticipate, withstand, and adapt to disruptions, whether powered by AI technologies, quantum computing, or sophisticated state-sponsored attacks. Together, agility and resilience give organizations the speed and stability needed to thrive in an increasingly volatile digital world.

Integrating Siloed Cybersecurity Tools

Even with visibility and agility in place, many enterprises are held back by fragmented security infrastructures. Siloed cybersecurity tools are no longer enough in a world where cryptographic assets are increasingly being targeted by AI-enhanced attacks.

Fragmented tools and decentralized management not only hinder visibility but also slow the enterprise's ability to adapt to evolving threats and regulations. Modern adversaries — often armed with AI-enhanced attack methods — are targeting these gaps, exploiting unmanaged keys and mismanaged certificates buried in decentralized systems. To close those gaps, organizations need a unified approach to cryptographic management, especially as the cryptographic sprawl continues to grow, expanding the attack surface across cloud environments, mobile endpoints, and IoT devices.

Fortunately, emerging platforms now offer comprehensive visibility across the entire cryptographic estate, allowing teams to monitor keys, certificates and encryption methods in real time. Centralizing control not only streamlines policy enforcement and compliance, but also simplifies the transition to post-quantum cryptography.

By breaking down operational silos and automating key management, organizations can reduce risk, improve agility, and stay ahead of the rapidly shifting threat landscapes.

Preparing for Q-Day isn't about reacting – it's about restructuring. Quantum computing will disrupt the cryptographic foundations that enterprises rely on today. The only way to stay ahead is to start now.

The preparation begins with visibility. Organizations must conduct a full audit of their cryptographic assets – keys, certificates, and secrets – across all systems. From there, automation becomes critical. Tools that enable key rotation, algorithm updates, and policy enforcement will reduce manual errors and accelerate readiness.

Quantum disruption is inevitable. The question is not if your cryptography will be tested, but when. Will you be ready?

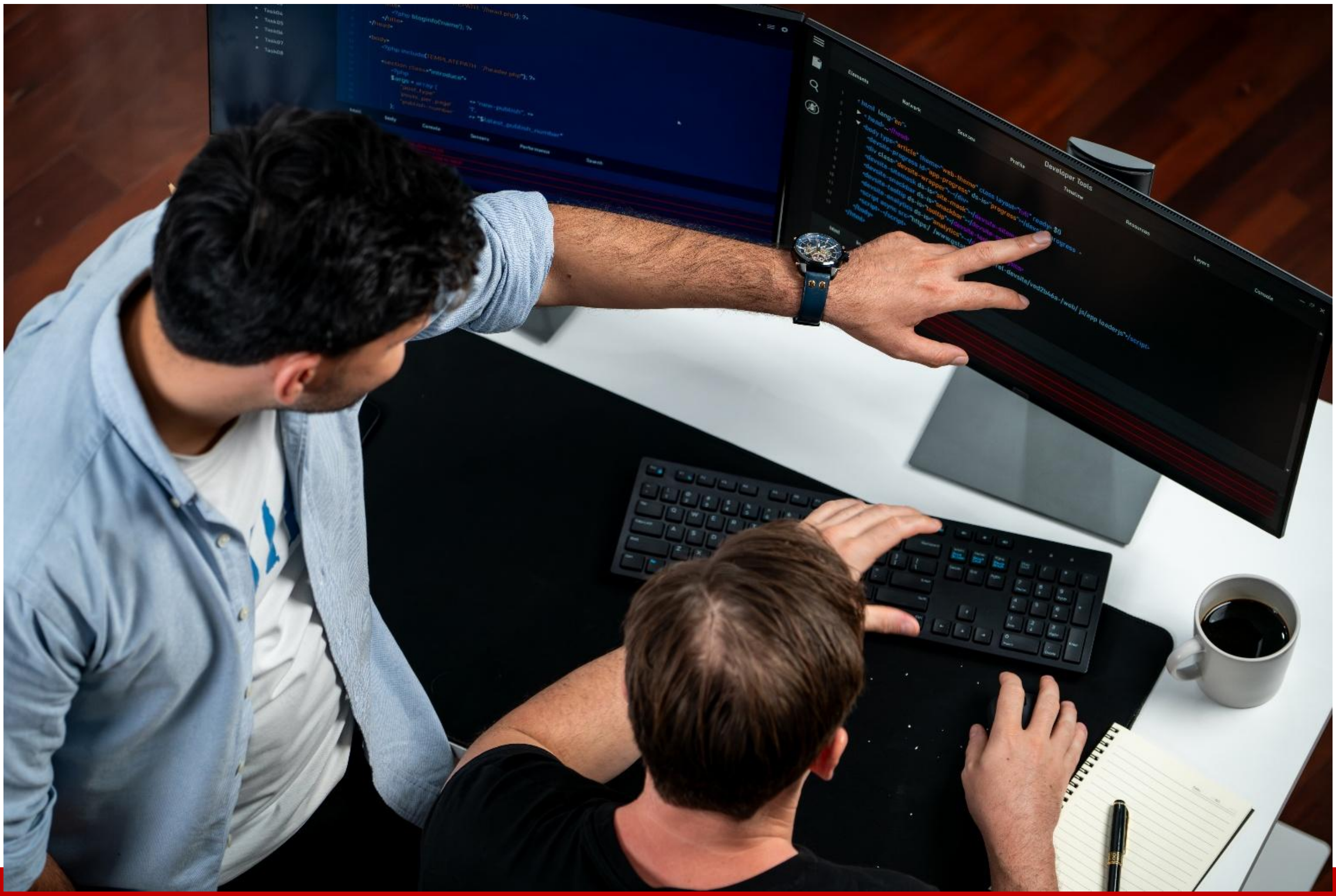
About the Author

Bhagwat Swaroop is President, Digital Security Solutions at Entrust. He leads the evolution, growth, and expansion of the Entrust Digital Security portfolio. This portfolio is foundational for enabling crucial enterprise security initiatives for Zero Trust architectures supported by identity and data security, and they underpin secure digital interactions around the world.

Swaroop has more than 20 years of leadership experience driving growth in global high-tech companies. He was most recently President and General Manager of One Identity, a cloud-based cybersecurity company. Prior to One Identity, Swaroop was Executive Vice President and General Manager of Proofpoint, leading the company's email security business; and led the Enterprise Security Solutions product management and product marketing teams at Symantec. Previously he held leadership positions at NetApp, McKinsey, and Intel.

Swaroop holds a BE degree from Delhi Institute of Technology, an MS in Electrical Engineering from Arizona State University, and an MBA from the Wharton School at the University of Pennsylvania.

Bhagwat can be reached at LinkedIn and our company website https://www.entrust.com/.



From NMAP TO CSV How Experience and Management Skills Improve Data Analysis for Security Professionals

By Jordan Bonagura, Senior Security Consultant, Secure Ideas

The other day, I found myself reflecting on my career and how things have evolved as I age. In doing so, I realized how fortunate I am to have started my career at such an early age. I can still remember being fascinated by using BBSs *(Bulletin Board Systems)*, patching motherboards, working with Windows 3.11 and NT, as well as using ICQ and various other systems and operating systems. By the way, just mentioning these applications makes me feel like my beard has gained a few more white hairs.

I strongly believe that everything we learn in life contributes to the abilities and knowledge we carry with us — our knowledge is built brick by brick. Sure, sometimes some of those bricks fall on our heads, but we pick them up and keep building. Unfortunately, one of these cases where bricks fall is when people try to see the technical and the management as separate ideas instead of combining the skills and such to improve both.

While my career has been centered on technical work, I've also gained experience working with management, which has taught me the importance of regulations, compliance, and clear communication with stakeholders. Presentations often rely on KPIs, graphs, and Excel to demonstrate risks and impacts. I've learned to apply these management skills, like simplifying complex information, to my technical tasks, especially in research and penetration testing.

As many know, a crucial phase of penetration testing involves collecting data, and the volume of data can be overwhelming, especially when dealing with medium to large-sized companies that have thousands of devices. During the reconnaissance process, a widely used tool is Nmap. However, even with the current data output options *(-oA)*, the sheer volume of information can still be challenging to analyze effectively.

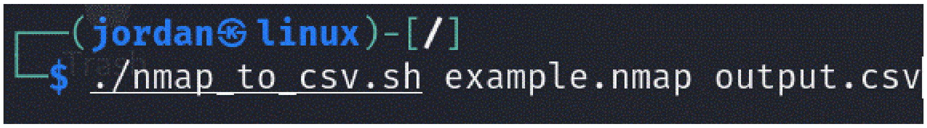
So, why not simplify things and leverage Excel's dynamic features? By creating filters, sorting for ports, services, status, and more, we can make the data much easier to identify and then dive deeper into our engagement.

Aiming to streamline the process while presenting the information more clearly to clients, I decided to develop the following bash script that parses data from an Nmap-style file (*.nmap*) and converts it into a CSV format that can be easily imported into Excel.

```
#!/bin/bash

# Check if input file is provided

if [ "$#" -ne 2 ]; then

        echo "Usage: $0 <input_nmap_file> <output_csv_file>"

        exit 1

fi

# Input and Output files

input_file=$1

output_file=$2

# Check if the input Nmap file exists

if [ ! -f "$input_file" ]; then

        echo "Error: Input file does not exist."

        exit 1

fi

# Create the CSV file and add the header
```

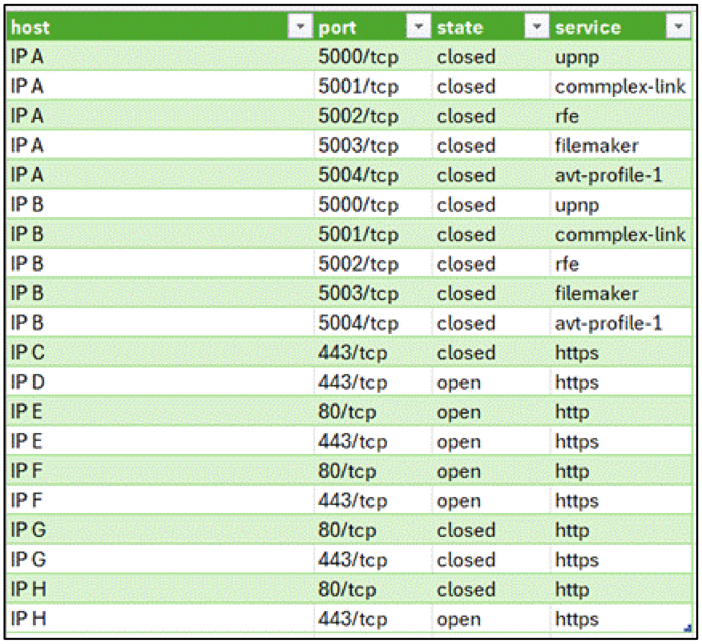
```
echo "host,port,state,service" > "$output_file"


# Parse the Nmap file
host=""
while IFS= read -r line; do
    # Check if line starts with "Nmap scan report for" (indicating a new host)
    if [[ $line =~ ^Nmap\ scan\ report\ for\ (.*) ]]; then
    host="${BASH_REMATCH[1]}"
    echo "Found host: $host"  # Debugging: print host when found
    fi
    # Check if line contains port info (TCP/UDP ports)
    # Adjust the regex to ensure matching is more flexible with spaces and tabs
    if [[ $line =~ ([0-9]+)/(tcp|udp)[[:space:]]+(open|closed)[[:space:]]+([a-zA-Z0-9\-]+) ]]; then
    port="${BASH_REMATCH[1]}"
    protocol="${BASH_REMATCH[2]}"
    state="${BASH_REMATCH[3]}"
    service="${BASH_REMATCH[4]}"
    # Debugging: print port, state, service
    echo "Found port: $port/$protocol, state: $state, service: $service"
    # Write the host, port, state, and service to the CSV file
    echo "$host,$port/$protocol,$state,$service" >> "$output_file"
    fi
done < "$input_file"
echo "CSV file created at $output_file"
```

After setting up the correct permissions to execute it, you can simply type the following:



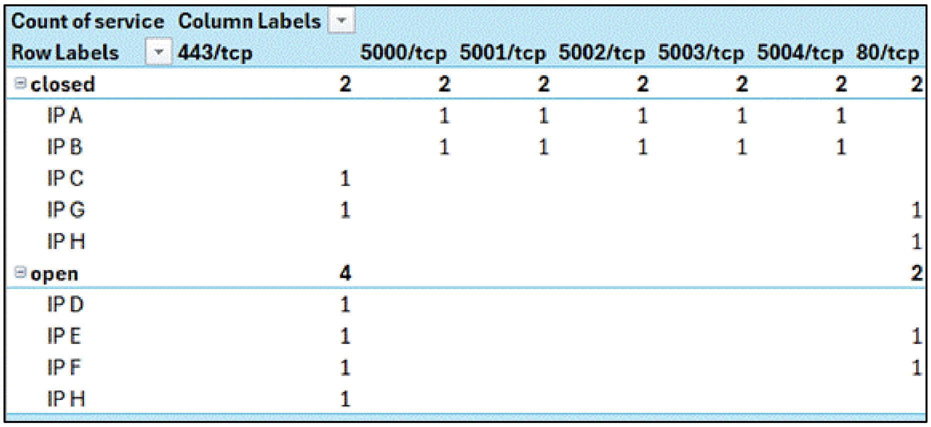
```
┌──(jordan㉿linux)-[/]
└─$ ./nmap_to_csv.sh example.nmap output.csv
```

In addition to the on-screen display, you will have generated an *output.csv* file that, once processed, may have a graphical representation as below.



host	port	state	service
IP A	5000/tcp	closed	upnp
IP A	5001/tcp	closed	commplex-link
IP A	5002/tcp	closed	rfe
IP A	5003/tcp	closed	filemaker
IP A	5004/tcp	closed	avt-profile-1
IP B	5000/tcp	closed	upnp
IP B	5001/tcp	closed	commplex-link
IP B	5002/tcp	closed	rfe
IP B	5003/tcp	closed	filemaker
IP B	5004/tcp	closed	avt-profile-1
IP C	443/tcp	closed	https
IP D	443/tcp	open	https
IP E	80/tcp	open	http
IP E	443/tcp	open	https
IP F	80/tcp	open	http
IP F	443/tcp	open	https
IP G	80/tcp	closed	http
IP G	443/tcp	closed	https
IP H	80/tcp	closed	http
IP H	443/tcp	open	https

Now it will be much easier to organize it by host, sort by port, filter by status or anything else that you want to do with the data. As a basic example, I created a pivoted table as follows:



Count of service	Column Labels						
Row Labels	443/tcp	5000/tcp	5001/tcp	5002/tcp	5003/tcp	5004/tcp	80/tcp
⊟ **closed**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
IP A		1	1	1	1	1	
IP B		1	1	1	1	1	
IP C	1						
IP G	1						1
IP H							1
⊟ **open**	**4**						**2**
IP D	1						
IP E	1						1
IP F	1						1
IP H	1						

To wrap it all up, this simple yet effective tool allows us to streamline the process of analyzing Nmap data, making it far more manageable and easier to present to clients or stakeholders. By converting raw data into a structured CSV format, we can leverage Excel's powerful features to quickly identify patterns, sort information, and generate meaningful insights. This not only simplifies our daily work, but also improves communication, enabling us to focus more on the critical aspects of our penetration testing and vulnerability assessments. Ultimately, it's a small innovation that makes a big difference in both the efficiency and clarity of the entire process.

If you're interested in exploring ways to improve the analysis and handling of large volumes of data in penetration testing, I invite you to visit and contribute to this project on our GitHub page *(https://github.com/ProfessionallyEvil/)*. Your insights and contributions would be greatly appreciated as we continue to refine and enhance the tools and techniques used in this field.

About the Author

With more than 20 years of experience in information security, Jordan is passionate about helping companies and clients protect their data and applications from threats and vulnerabilities. As a Principal Security Researcher, he led teams in conducting vulnerability management, risk assessments, penetration tests, and setting up boundaries to comply with standards for companies in different segments.

He contributed to significant projects, such as developing an integrated GNSS positioning system and an encryption communication protocol between ground and satellite at the Brazilian National Institute of Space Research. He also had the opportunity to speak at important security conferences around the globe, be a professor and course coordinator at colleges, and consult for the Brazilian police in crime solving.

Jordan can be reached online at https://www.linkedin.com/in/jordan-bonagura and at our company website https://www.secureideas.com

Futureproofing Next-Gen Network Security with Advanced Observability and Proactive Anomaly Detection.

By David Olufemi, PMP, S-IEEE, B-Yond Inc.

As the world stands on the cusp of a new technological era, the transition to next-generation networks, including 6G, is poised to revolutionize industries across the globe. These networks will bring about faster speeds, ultra-low latency, and enhanced connectivity, creating the foundation for innovations in autonomous systems, smart cities, the Internet of Things (IoT), and much more. However, as the complexity and interconnectivity of these networks grows, so do the security risks. With increasing reliance on highly automated systems, such as Industry 4.0 manufacturing, connected transportation systems, and smart grids, ensuring the safety, security, and resilience of these infrastructures becomes paramount. This article delves into the security challenges inherent in next-generation networks, the crucial role of observability, and the application of proactive anomaly detection to safeguard the future of our hyper-connected world.

The Rise of Advanced Network Infrastructures

Next-generation networks (NGNs) like 6G are expected to deliver on the promise of seamless, ubiquitous connectivity across a wide variety of industries. From autonomous vehicles to smart cities, and from robotic manufacturing to energy grids, advanced network infrastructures will form the backbone of an intelligent, interconnected world. However, as the complexity of these networks increases, so do the potential vulnerabilities.

Among the key sectors driving the transformation are:

Connected Roads and Autonomous Vehicles: The advent of connected vehicles and smart transportation networks will allow for real-time communication between cars, traffic systems, and infrastructure. While this promises enhanced safety and efficiency, the integration of autonomous vehicles and connected road networks creates new avenues for cyberattacks, where adversaries can exploit vulnerabilities in communication channels to cause accidents or disrupt traffic.

Smart Grids and Energy Infrastructure: The energy sector is undergoing a transformation with the integration of smart grids, renewable energy sources, and IoT-enabled energy systems. These advancements provide real-time data for efficient energy management, but they also create an extensive attack surface for hackers. Vulnerabilities in these interconnected systems can lead to service disruptions, damage to critical infrastructure, and potential financial losses.

IoT-Driven Environments: The Internet of Things (IoT) is increasingly becoming the backbone of modern infrastructures, enabling devices to communicate and operate autonomously. In smart homes, healthcare, industrial automation, and even agriculture, IoT systems are playing a crucial role. However, the widespread use of interconnected devices introduces security challenges, including the risk of unauthorized access and data manipulation.

Telecommunication Networks: The telecom industry will also play a significant role in the next generation of connectivity. 5G networks are already enabling high-speed communication for smart cities and IoT devices. As 6G and future networks emerge, the security of telecommunications infrastructure will need to evolve to protect against increasingly sophisticated cyber threats.

These interconnected systems have one thing in common: their reliance on seamless, real-time communication across vast networks. This makes them highly susceptible to security breaches if not properly protected.

Security Risks in Next-Generation Networks

While the promises of next-generation networks are vast, they also come with a host of security risks that could have far-reaching consequences. As more systems become interconnected, the potential for cyberattacks increases. Some of the key risks include:

Distributed Attack Surfaces: The complexity of next-generation networks leads to expanded attack surfaces. In sectors like smart cities and IoT, individual devices and components communicate across vast networks, creating numerous entry points for attackers. A vulnerability in one part of the network could allow adversaries to exploit others, creating a cascading effect that compromises the entire system.

IoT Vulnerabilities: Many IoT devices are low-cost, with minimal built-in security. Their widespread deployment in critical infrastructures such as healthcare devices, home automation systems, and industrial equipment can serve as easy entry points for hackers. A compromised IoT device could provide attackers with access to sensitive data or control over critical systems.

Data Integrity Risks: With the vast amount of data flowing through next-generation networks, maintaining data integrity becomes a significant challenge. Malicious actors could manipulate or intercept data, leading to incorrect decisions in automated systems. For example, falsifying sensor data in a smart grid could disrupt power distribution, causing service outages or equipment damage.

Supply Chain Attacks: As organizations adopt new technologies, they increasingly rely on third-party vendors to provide software, hardware, and services. However, vulnerabilities in third-party components or software can expose organizations to supply chain attacks, where attackers gain access to networks through trusted suppliers.

AI and Machine Learning Vulnerabilities: Artificial intelligence and machine learning systems are critical to the operation of next-generation networks, providing automation and intelligence. However, these systems are vulnerable to adversarial attacks, where malicious actors can manipulate algorithms or training data to achieve their objectives. This is especially concerning environments like autonomous vehicles, where the failure of AI systems can have life-threatening consequences.

The Importance of Observability in Network Security

To secure next-generation networks, observability is essential. Observability refers to the ability to monitor and understand what is happening across a complex network in real-time, enabling security teams to quickly identify and respond to potential threats.

Comprehensive Visibility: Observability tools provide full visibility into every component of a network, from IoT devices to cloud infrastructure. This visibility allows security teams to track network activity, performance, and security events, identifying unusual patterns that may indicate a breach.

Real-Time Monitoring: Advanced observability enables real-time monitoring of both traffic and data flows. In sectors like connected transportation or smart grids, where any delay or disruption can have significant consequences, real-time monitoring allows for quick identification of anomalies and rapid incident response.

Data Correlation: Observability tools allow organizations to aggregate data from various network components, correlating events across devices, applications, and systems. This provides a comprehensive view of the entire network, making it easier to detect cross-system threats. For example, unusual patterns of data exchange between autonomous vehicles or devices in a smart grid can be detected before they result in widespread damage.

Predictive Insights: By continuously monitoring network traffic and system behavior, observability tools can provide predictive insights that help organizations prepare for potential threats. These tools can detect subtle deviations from normal behavior, such as slow network traffic in specific areas, which might indicate a targeted cyberattack.

Proactive Anomaly Detection: The Key to Mitigating Security Risks

Proactive anomaly detection is the process of identifying irregularities or abnormal behavior in a network before they escalate into full-blown security incidents. Unlike traditional security measures that react to known threats, proactive anomaly detection looks for signs of potential risks, allowing organizations to address them before they can cause significant harm.

Machine Learning and AI: Anomaly detection systems increasingly rely on machine learning and AI to analyze vast amounts of network data. These algorithms learn what constitutes "normal" network behavior and can identify new, previously unseen threats. This is particularly important in environments where systems evolve rapidly, such as connected vehicles or smart cities.

Real-Time Detection: Proactive anomaly detection systems are designed for real-time analysis, making them highly effective in dynamic environments. For example, in smart grids, these systems can detect abnormal fluctuations in energy consumption or communication patterns that might indicate a cyberattack or technical malfunction.

Reducing False Positives: One of the challenges in traditional anomaly detection is the occurrence of false positives alerts that appear as threats but are not actual security incidents. By leveraging machine learning, modern anomaly detection systems reduce false positives, ensuring that security teams are not overwhelmed by irrelevant alerts and can focus on real threats.

Early Incident Response: With early detection, organizations can deploy automated responses to mitigate the impact of security breaches. For example, a connected vehicle network might automatically isolate a compromised vehicle from the larger traffic system, preventing it from causing accidents or disruptions.

Integrating Observability and Anomaly Detection Across Industries

In the context of Industry 4.0, smart cities, autonomous vehicles, and energy grids, integrating observability and proactive anomaly detection will be essential to securing the complex infrastructures of the future. Here's how:

Scalable Infrastructure: As these technologies expand, organizations will need scalable security solutions that can grow alongside them. Integrating observability and anomaly detection allows for continuous monitoring and protection, regardless of how large or complex a network becomes.

Automated Responses: The future of security will involve automated responses triggered by real-time insights from observability and anomaly detection systems. In autonomous vehicle systems, for example, AI-driven anomaly detection can trigger automated steering adjustments if a vehicle is compromised, while in smart grids, it can reroute power to prevent outages.

Cross-Sector Collaboration: To ensure robust security, collaboration across sectors is essential. For example, sharing threat intelligence between transportation, energy, and telecom sectors will allow for better identification of common vulnerabilities and quicker responses to attacks.

Possible Challenges and a Path Forward

While observability and anomaly detection hold tremendous promises for securing next-generation networks, challenges remain, and are mentioned below:

Data Privacy and Compliance: With the vast amounts of data being collected, privacy concerns and regulatory compliance must be prioritized. Adhering to GDPR and similar regulations will be critical in sectors like healthcare and energy.

Legacy Systems Integration: Many existing systems, particularly in critical infrastructure sectors like energy, are not designed with modern observability and anomaly detection tools in mind. Integrating these systems with new technologies will require careful planning and investment.

Evolving Threats: As cybercriminals become more sophisticated, organizations must continuously evolve their security strategies to stay ahead of new threats.

The future of connectivity promises a world of unprecedented opportunities, but it also introduces new and more complex security challenges. By integrating advanced observability and proactive anomaly detection into next-generation networks, industries can ensure that they are prepared to safeguard critical infrastructure, protect data, and minimize downtime. As we move toward the deployment of 6G and the continued expansion of IoT, autonomous systems, and smart infrastructure, proactive security measures will be the key to ensuring the safe, efficient, and resilient operation of these transformative technologies.

About the Author

David Olufemi is a seasoned expert in Communications Networks, currently serving as a Lead Engineer in 5G Observability Development at B-Yond Inc. He is a PhD candidate in Computer Science and Engineering at the University of Fairfax, USA and holds a master's degree in information and Telecommunications Systems from Ohio University. He is a Senior Member of the IEEE, a Fellow of the Nigeria Institute of Professional Engineers, and a Fellow of the Institute of Management Consultants.

David can be reached online on Gmail, david.olufemi@ieee.com and on LinkedIn.

Getting Out of the Silo

The Importance of Business Context for Security Teams

By Esteban Gutierrez, Chief Information Security Officer & VP of Information Security at New Relic

According to Gartner, GenAI-enabled cyberattacks will continue to spike enterprise investment in information security resources, leading to a 15% increase in security software spending in 2025. As security teams prepare for this emerging threat landscape, it is worth pausing to reevaluate IT best practices for any potential improvements that can help enterprises in an era of increased cyber activity.

Security in Isolation

One common pitfall facing security teams is that they often work in a silo because of their very specialized roles. While having deep expertise in their company's security posture and the threat landscape, security resources are often too far removed from the company's business function and its departments (i.e., sales, go-to-market, engineering, customer service) when these areas should inform their work. This arrangement can lead to their isolation in a company's larger organizational structure. Unless silos are proactively guarded against, security resources can drift too far away from the company's core operations, finding themselves flatfooted at critical steps during an outage or security incident.

“We Have a Problem”

During a security event, security teams missing the business context to fully comprehend how outages impact their company will be out of step and lacking preparedness. Further, suppose they lack critical technical expertise or critical relationships with key subject matter experts (SMEs) in other areas of the business. Security pros will have the unenviable task of mapping out and learning system functionality to determine the affected infrastructure and services, potentially slowing incident response times. This is no small matter when adding up the cost of outages, wherein the wrong move could lead to financial ruin. With so many critical touch points and services involved, security teams may fail to prioritize their response in line with business objectives.

In short, beginning research into the technical aspects, business priorities, critical points of contact, and customers affected only after something has already happened will leave security teams scrambling, significantly reducing their effectiveness. Instead, an organization’s security team must understand every aspect of the business beyond a basic, default high-level conceptualization.

The Customer Perspective

In that same security silo, important customer context that can round out the impact of an outage is also missing. Knowledge of specific customers and how they will be affected should also inform the work of security professionals. The customer perspective is not just a matter for other departments. Security teams should also have a tangible understanding of who or what is affected during a potential event or incident. For example, in a B2B (Business to Business) company, can this incident potentially impact a critical deal with a major customer or does this incident involve regulated customers that often require specific terms for notifications. When the system blinks red and alerts pop up, who is on the other side of these?

Further, what customers consider most important often differs from what one might expect. Being in the loop with customers might help the security team reprioritize the order of tasks. Pushing back against the detached, insular, and cordoned off approach, when IT pros know the company’s top customers and their concerns before an incident, it will improve their incident response outcomes.

Getting Out

Security teams that lack full integration with their broader organization miss the opportunity to reach full preparedness in advance. While an incident can be an opportunity for critical relationship-building and cross-team collaboration, these relationships must be permanent and ongoing. Haphazardly reaching out to work together when the clock is ticking leaves considerable room for improvement. Instead, security resources should establish close relationships with the people their work impacts every day across the company. This includes proactively collaborating with engineering teams instead of instigating communication during a crisis. It also means identifying subject matter experts and contacts across the company should the need arise.

However, closing the gap by working more closely with other teams across the organization to inform other departments of their work and understand what is critical to the business cannot be achieved by a single team alone. There must be reciprocity and an overall interdepartmental collaborative spirit in the company. The move to a more vertical, tightly integrated organization needs to be instituted top-down or the promise of closer proximity will wither on the vine.

Security teams that establish close cross-functional relationships and expertise across the organization by cultivating ongoing collaboration with other teams across IT — like infrastructure, DevOps, and site reliability engineers (SREs) — will develop a stronger understanding and improve efficiency when it matters most. To promote awareness, knowledge, and informed security practices, these teams should be in constant communication with the goal of full integration. When security teams have the technical expertise, product knowledge, customer understanding, business context, and cross-department contacts in place, they will be ready to address their organization's cybersecurity needs efficiently.

About the Author

Esteban Gutierrez is Chief Information Security Officer & VP of Information Security at New Relic. Esteban's preferred pronouns are the/them.

They are passionate about reshaping information security to enable people to do the work they value in balance with business goals, best practices, technical constraints, and pragmatic risk management strategies.

Esteban can be reached online at Esteban Gutierrez | LinkedIn and at our company website https://newrelic.com/

Self-Hosted AI: Enabling Secure Innovation Across the Federal and Defense Sandors

By Joel Krooswyk, Federal CTO at GitLab

Many government agencies operate under restrictions that limit their use of cloud technology for software development. This limits their ability to realize AI's transformative potential because most cutting-edge AI solutions are cloud-based. The risks of external data processing and limited control over AI environments require them to take a more secure approach.

Simply avoiding AI is not an option. Agencies need to integrate AI into software development to enable efficient software modernization. But how can they take advantage of powerful AI tools to enhance productivity, strengthen security, and drive innovation, without exposing themselves to the risks entailed by cloud-based AI solutions?

Self-hosted AI models offer a strategic solution. By deploying and managing large language models (LLMs) and other advanced AI capabilities within their own secure infrastructure, whether on-premises data centers or private cloud environments, agencies gain the control needed to leverage AI while maintaining strict compliance standards and advancing mission-critical applications.

Key Benefits of a Self-Hosted AI Strategy

I've spent many years working with federal agency tech leaders, so I know that a statement like "let's just host it ourselves" might raise some eyebrows. It's not always straightforward, especially with a technology as new as AI. But there are signs that federal agencies and defense organizations are ready for a different way.

For example, the Pentagon is actively working on a "fast pass" approach to securing software components, aiming to onboard approved software more quickly by using existing standards such as Software Bill of Materials (SBOM), the NIST Secure Software Development Framework (SSDF), and other common attestation methods and risk assessments.

Meanwhile, the House Oversight and Government Reform Committee has been exploring ways to use IT modernization to make the government more efficient. And there's a broad groundswell of interest in finding ways to leverage AI in government.

To name just a few more examples from the U.S. military:

- The Defense Information Systems Agency is working on a new data strategy that integrates data, analytics, and AI into all aspects of defense operations via a secure, self-hosted platform.
- The Army is building two new self-hosted AI tools, CamoGPT and NIPR GPT, to assist with predictive maintenance, analysis of adversaries' communications, logistics optimization, and analysis of different proposed courses of action.
- The Air Force Research Lab is developing an open-source platform, the Air and Space Force Cognitive Engine, a flexible, single IT platform for operationalizing AI within the Air Force.

There are several clear benefits to government organizations hosting LLMs within their own secure infrastructure:

- **Data Sovereignty:** When handling sensitive national security information, the risks associated with external data processing and limited control over AI environments demand a more secure approach—one that keeps critical data within protected boundaries. Self-hosted environments help guarantee that level of security.
- **Compliance Alignment:** Federal agencies operate under complex regulatory frameworks, including the Federal Risk and Authorization Management Program (FedRAMP), International Traffic in Arms Regulation (ITAR), Federal Information Security Modernization Act (FISMA), and agency-specific mandates. Self-hosted environments provide the granular control needed to implement specific security controls, audit trails, and governance frameworks that meet these strict requirements.

- **Enhanced Security Posture:** Self-hosted models significantly reduce potential attack vectors by removing dependencies on external APIs and third-party infrastructure. Agencies maintain complete control over access management, network segmentation, and vulnerability patching within their AI systems.
- **Mission-Specific Customization:** Unlike pre-configured cloud solutions, agencies can select from a list of supported AI models using specialized datasets to align with their unique use cases and environments. This enables more effective, purpose-built AI solutions that directly support mission objectives—whether enhancing intelligence analysis, optimizing resources, or strengthening cybersecurity. This customization extends to integration with legacy systems, a common challenge in the public sector.
- **Predictable Resource Management:** While initial setup requires investment in infrastructure and expertise, self-hosted AI models can provide more predictable long-term cost structures than variable subscription-based cloud models. This approach offers greater flexibility for large-scale deployments and leverages existing infrastructure and personnel. Additionally, self-hosted AI can provide a secure environment for modernizing legacy systems while keeping sensitive code under direct oversight.

Fostering Innovation Within a Trusted Framework

Deploying AI in a secure, self-hosted environment doesn't restrict innovation—it nurtures it within a foundation of trust and control. Agencies can use open-source AI advances while maintaining security, compliance, and performance standards. This flexibility empowers government developers and data scientists to build next-generation critical applications with security and compliance as foundational principles rather than afterthoughts.

It’s clear from the examples I cited above that the U.S. government, and the Department of Defense in particular, are serious about embracing the potential of AI for making their work more effective, efficient, and innovative. This movement is already well underway.

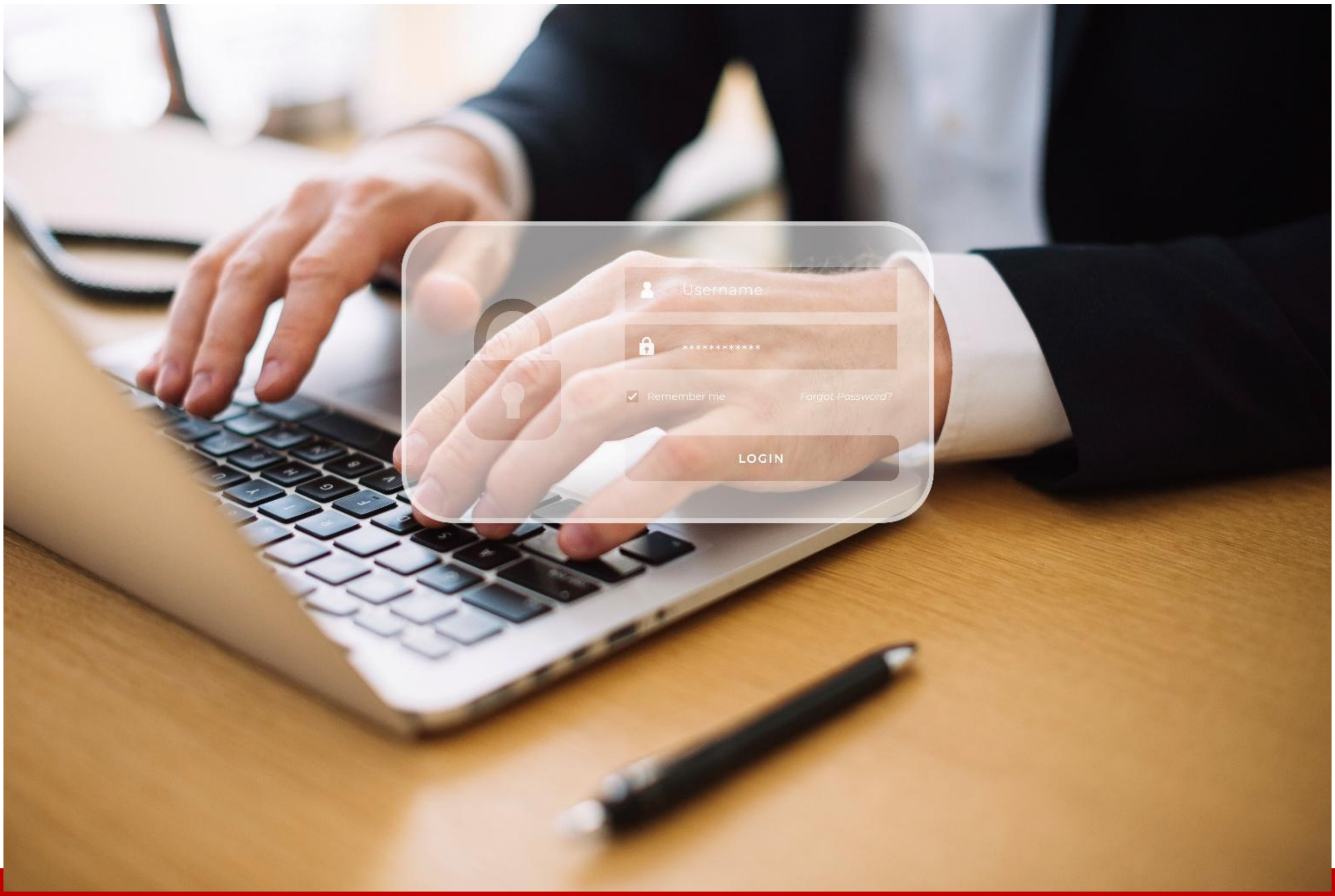
For federal agencies, integrating self-hosted AI models into software development workflows is essential for navigating the intricate web of security regulations while fostering innovation. Self-hosting enables AI to reach its full potential throughout the software development lifecycle. That, in turn, enhances operational effectiveness, fortifies security, and accelerates the creation of more intelligent applications to safeguard national interests in an increasingly complex digital environment.

A secure, technologically advanced future for the federal government depends on its ability to innovate with AI while upholding strict regulations and maintaining complete control over sensitive data. Self-hosted AI models are the way to do just that.

About the Author

Joel Krooswyk is the Federal CTO at GitLab. Joel has actively been involved in GitLab's growth since 2017. His 25 years of leadership experience span not only the U.S. Public Sector, but also small, mid-market, and enterprise businesses globally. Joel combines deep government policy expertise with a wealth of experience in technology, software development, AI, and cybersecurity. He is frequently called upon by industry and agencies alike for policy commentary and response.

Follow Joel Krooswyk on LinkedIn https://www.linkedin.com/in/joelrkrooswyk/ and learn more about GitLab at https://about.gitlab.com/solutions/public-sector/.



Governing The Ungoverned: Securing Kerberos Keytabs in Modern Enterprises

How to Bring Visibility, Control, and Post-Quantum Readiness to One of the Most Overlooked Credentials in Cybersecurity

By Durgaprasad Balakrishnan, Independent Cybersecurity Researcher and Director of Cybersecurity – Identity and Access Management at a Leading Global Fintech Company

Kerberos keytabs are among the most powerful yet invisible credentials in enterprise infrastructure. These files silently authenticate service accounts, allowing critical systems to run uninterrupted. But their very convenience has created a gap in visibility, one that attackers increasingly exploit. Mismanaged keytabs have become backdoors for lateral movement and privilege escalation, often with little to no detection.

In many environments, keytabs are created manually, distributed informally, and rarely tracked. Administrators generate them using command-line tools, then move on, leaving no audit trail, expiration policy, or ownership mapping. Over time, these credentials accumulate across servers, backups, and forgotten scripts. They don’t rotate. They don’t expire. And most importantly, they are not governed like passwords or tokens. This creates a hidden attack surface that can be difficult to detect but devastating when breached.

Addressing this risk begins with changing how keytabs are provisioned. Rather than relying on one-off commands and ad-hoc transfers, keytab issuance should flow through formal IAM workflows. Each request should be linked to a specific service, include business justification, and assign ownership to a team. Once approved, the keytab should be tagged, encrypted, and logged into an identity governance system for traceability. This brings keytabs into the same control plane as privileged user credentials, making them visible, justifiable, and auditable.

Discovery is often the next challenge. Most organizations have keytabs scattered across environments, created long ago and never retired. Scanning file systems for .keytab files and using Kerberos utilities to extract metadata is a useful start. These findings should then be correlated with existing service accounts, applications, and infrastructure records to determine whether they are still valid. Building an authoritative inventory enables policy enforcement and compliance monitoring, transforming static files into manageable assets.

Security hardening of keytab storage is equally important. These files contain cryptographic keys that can be used to impersonate services. Basic hygiene, like setting strict file permissions, encrypting storage, and avoiding inclusion in code repositories, can drastically reduce exposure. Production, staging, and development environments should each maintain their own segregated keytab controls, limiting scope and blast radius in case of compromise.

Lifecycle management is often overlooked. Keytabs, like user accounts, need a structured joiner-mover-leaver process. When services are introduced, keytabs should be issued and linked to owners. If a service is migrated, the associated keytab should be rotated and ownership reassigned. And when systems are decommissioned, the keytab must be removed, and the Kerberos principal deleted. Integrating this lifecycle into IAM tooling ensures keytabs do not outlive their purpose or disappear into shadow infrastructure.

Some organizations are exploring certificate-based authentication to replace static keytabs altogether. Using PKINIT, services authenticate using X.509 certificates instead of stored secrets. This approach aligns better with smartcards, HSMs, and MFA policies, adding cryptographic agility and revocation controls. While PKINIT requires initial investment in PKI infrastructure, it offers a more secure foundation, especially for sensitive or regulated workloads.

Keytabs have featured prominently in breach investigations. Attackers have extracted them from memory, recovered them from backups, and used them to forge Kerberos tickets that bypass detection. These incidents highlight why regular rotation, proper encryption, and governance are not optional. A forgotten keytab is a latent vulnerability waiting to be weaponized.

Modern identity platforms now include features to govern non-human credentials like keytabs. With the right integrations, IGA systems can link keytabs to business applications, include them in access reviews, and trigger revocation based on lifecycle events. This is especially valuable during audits, where being able to demonstrate control over service accounts and automation credentials strengthens overall security posture.

Looking ahead, post-quantum cryptography may impact parts of the Kerberos ecosystem, particularly those using public key mechanisms like PKINIT. Organizations that inventory their keytab landscape today, implement AES-256 where possible, and prepare for algorithm upgrades will be better positioned for a secure transition.

Keytabs no longer belong in the shadows. They are part of the identity fabric and must be treated with the same diligence as passwords, certificates, and API keys. Governance, visibility, and lifecycle automation are essential to ensuring these powerful credentials don't become the weakest link.

About the Author

Durgaprasad Balakrishnan is an independent cybersecurity researcher and Director of Cybersecurity – Identity and Access Management at a leading global fintech company. With over 16 years of experience in identity architecture, access governance, and secure automation, he has led enterprise-scale IAM transformations and contributed to multiple peer-reviewed cybersecurity initiatives. He actively participates in research communities and helps organizations design identity-centric security strategies for regulated and high-risk environments.

He can be reached via LinkedIn.

How AI is Reinventing the Security Operations Center

By Shahar Ben, CEO and Co-Founder, Radiant Security

The typical SOC team can be presented with thousands of security alerts every day. While most turn out to be false positives, each needs reviewing, and, nevertheless, creating a to-do list that is almost impossible to complete. Unsurprisingly, security professionals are often in the position of having to firefight. Picking which alerts to focus on and which ones to leave can mean missing a true positive. The idea of taking proactive stance that everyone in the industry aspires to can be an impossible ideal.

This all-too-common scenario isn't just an operational nuisance; it can bring the very real risk of missing genuine threats while also contributing to a much broader issue: burnout. A recent industry study, for example, revealed that nearly three-quarters of SOC analysts experience some level of burnout, caused by issues such as understaffing and increased workloads. As a result, nearly two-thirds say they are likely to switch jobs in the next year. – a situation which is simply unsustainable over the long term.

Adding to the sense of pressure is the nature of today's attacks, with threat actors using AI to create highly adaptive, fast-moving threats. The big problem here is that traditional security tools and manual processes simply don't scale in this environment. Without the ability to understand and act on threats at machine speed, even well-resourced SOCs risk being outpaced, leaving critical systems exposed and teams constantly stuck in reactive mode.

The case for SOC automation

This puts some organizations into a perfect storm scenario, where their adversaries are ideally placed to exploit gaps in coverage before stretched security teams can respond. Thankfully, the situation is far from one-way traffic, with AI-driven platforms also having a transformational effect on how SOCs go about various key processes, from automating routine tasks to helping analysts identify and prioritise high-priority threats.

Take automated triage, for example, where AI can be used to process enormous volumes of alert data in near-real time. In this context, its role is to filter out the false positives that can drain SOC resources and, instead, escalate only the genuine threats for expert human review. Crucially, the best solutions can triage any alert, regardless of type, source or format to provide a level of responsiveness that manual processes can no longer match.

Instead of wading through a backlog, analysts are presented with a curated shortlist of credible threats, each with contextual insights and recommended next steps. Investigation times are cut from hours to minutes, and the team is no longer stuck in reactive mode. Released from the associated impact of alert fatigue, analysts can focus their efforts more effectively on potentially critical and emerging incidents.

AI also transforms response times. By automating investigative steps and generating dynamic remediation recommendations, analysts can quickly understand the scope of a threat and act immediately, often with a single click. In contrast to rigid, rule-based workflows, this introduces much-needed flexibility into SOC operations.

Elsewhere, AI is changing the economics of log management. With affordable, scalable and vendor-neutral solutions, SOCs can now store and query vast archives of security data efficiently, supporting long-term compliance and, when required, forensic investigations. In particular, integrated log management across multiple systems and sources makes it easier to unify this information and identify meaningful patterns or anomalies that might otherwise go unnoticed.

The benefits aren't just technical, they're human. By reducing the volume of repetitive tasks and improving working conditions, AI can help stem the tide of burnout and attrition seen across SOC teams. It also lays the foundation for a more strategic role, where analysts spend less time juggling immediate priorities and more time focused on improving security posture.

These represent a compelling set of capabilities, but even with automation in place, AI isn't a silver bullet. While it excels at automating repetitive tasks and processing large volumes of data, there are still critical areas where human judgment remains essential. From assessing the context of a threat to making strategic decisions about incident response, experienced analysts play a vital role in ensuring that SOC operations remain accurate, ethical and aligned to business risk.

There are also important questions to consider around data quality, model transparency and the potential for bias, all of which require careful oversight to avoid unintended consequences. The point is, AI can enhance SOC performance, but it must be deployed with a clear understanding of its limitations.

Overall, however, the case for increasing the role of AI within contemporary SOCs has, for many across the industry, already been made. The question is, how quickly can organizations deliver on the undeniable benefits?

About the Author

Shahar Ben-Hador is the **co-founder and CEO** of **Radiant Security**, an AI-powered security platform designed to modernize **Security Operations Centers (SOCs).** Before founding Radiant Security in **2021**, he held key leadership roles at **Exabeam,** where he served as **CIO** and later as **VP of Product Management,** helping to develop the company's first **SaaS product**. His cybersecurity journey began at **Imperva,** where he progressed from **IT Administrator** to become the company's first-ever **Chief Information Security Officer (CISO).**

Shahar Ben-Hador can be reached via marketing@radiantsecurity.ai and at www.radiantsecurity.ai

How Artificial Intelligence Is Shaping the Future of Cyber Threat Detection

How AI Tools Make Cyber Threat Detection Easier

By Sujan Sarkar, Cofounder, aitools.xyz

Hackers are constantly evolving their strategies to outsmart traditional security measures, even through the use of AI. In response, AI-driven companies are continuing to develop smarter, more powerful tools to fight back against evolving cyber threats.

In February 2025, **CrowdStrike** recorded **470.20K total web traffic visits**, reflecting a growing awareness among businesses to safeguard digital systems against increasingly sophisticated cyberattacks—including AI-driven threats, ransomware, and state-sponsored hacking.

Meanwhile, **Abnormal AI**—known for its Behavioural AI platform that delivers robust email protection—saw **218.70K total web traffic visits** during the same period.

In addition, with **3.80K total web visits** in February 2025, **ZeroThreat** is pushing cybersecurity even further by helping businesses stay ahead of advanced risks—such as model tampering, data manipulation, session hijacking, and zero-day vulnerabilities.

In this article, we'll explore how AI tools are transforming cyber threat detection by using advanced techniques like machine learning, behavioral analysis, anomaly detection, natural language processing, and real-time threat intelligence.

1. AI Detects Threats Faster

Traditional cybersecurity tools rely on pre-set rules and known attack patterns to detect threats. However, these tools often struggle to identify new, unknown threats, or sophisticated attacks. This is where AI comes in.

AI-powered tools, such as machine learning algorithms, can analyze vast amounts of data and recognize patterns that might go unnoticed by traditional systems.

Example

Vectra AI focuses on metadata, allowing it to recognize abnormal behavior patterns that may go unnoticed by traditional systems. It can identify new attack techniques, such as lateral movement or insider threats, and raise alerts for immediate action.

2. 24/7 Threat Monitoring

AI tools can continuously monitor networks and systems for any signs of suspicious activity, without the need for manual intervention. They operate 24/7, ensuring that threats are detected immediately, no matter the time of day.

Example

AI-driven tools like Darktrace and CrowdStrike use advanced algorithms to track and analyze data across an organization’s network.

If they detect any unusual behavior—like a sudden spike in data transfer or unauthorized access to sensitive files—they can immediately alert security teams and take action to block the threat.

3. Automated Responses

One of the key advantages of AI in cyber threat detection is its ability to automate responses to potential threats.

Once AI detects a threat, it can trigger predefined actions without waiting for human intervention. This is particularly important when it comes to stopping threats before they escalate.

Example

AI tools like Palo Alto Networks Cortex XSOAR can automatically isolate compromised devices, block malicious IP addresses, or trigger an alert for the security team.

This automated response speeds up the reaction time, which is critical in preventing the damage that can be caused by cyber attacks.

4. Forecast Potential Attacks

AI tools are not just about detecting threats that are happening right now—they can also predict future risks. By analyzing past data and trends, AI tools can forecast potential vulnerabilities and attack strategies, allowing organizations to strengthen their defenses before an attack occurs.

Example

Recorded Future can predict cyber attacks before they happen by constantly scanning a wide range of sources—like news sites, blogs, dark web forums, social media, and hacker communities.

5. Reduced False Positives

One of the challenges of traditional cybersecurity tools is the high number of false positives—alerts that flag benign activity as a potential threat. This can overwhelm security teams and lead to alert fatigue.

AI tools help solve this problem by learning from past data and continuously improving their ability to distinguish between normal behavior and actual threats.

Example

Exabeam cuts down on false alarms using User and Entity Behavior Analytics (UEBA). It can tell the difference between normal unusual activity and true signs of a cyberattack.

Final Thoughts

As more businesses and individuals rely on cloud storage and online transactions, the risk of cyber attacks continues to rise. While there are countless AI-powered business tools to help grow your enterprise, remember that hackers are always on the lookout for vulnerabilities.

The larger your company, the more attention it attracts from cybercriminals. With AI tools capable of breaching systems in minutes, the threat becomes even more imminent.

Given these risks, investing in advanced AI-driven cybersecurity solutions has become a necessity. These tools can detect threats in real-time, predict potential risks, and respond to attacks before they escalate—helping to safeguard your business.

About the Author

Sujan Sarkar is cofounder of aitools.xyz, onelittleweb.com and writerbuddy.ai. A veteran SEO strategist and AI industry expert with over 12 years of experience in driving organic growth.

As co-founder of OneLittleWeb and AItools.xyz and writerbuddy.ai, Sujan's deep understanding of search algorithms and data analytics has established him as a trusted authority in both SEO and AI landscapes.

His data-driven research on AI tools has been widely cited in prestigious academic journals.

Suajn can be reached online at sujan@aitools.xyz , Twitter, LinkedIn , and at our company website onelittleweb.com

How Rugged Equipment Improves Cybersecurity

By Zac Amos, Features Editor, ReHack

Rugged devices are tough, purpose-built hardware that operate in harsh environments — such as jobsites with heavy dust or constant vibration — where standard laptops or tablets wouldn't stand a chance. Their use expands across industries like construction and emergency services, where teams need tech that won't break under pressure.

As more business operations go mobile and rely on real-time data, these devices are critical in keeping that data secure. That's why companies invest in rugged tech — to protect against damage and ensure sensitive information stays safe, even in the toughest conditions.

Industries Relying on Rugged Devices

Rugged devices have become essential in industries where conditions are unpredictable, and real-time access to information can make or break productivity. They allow workers to share updates and data with their teams without stepping away from the jobsite. This instant communication streamlines decision-making and helps businesses across various industries stay agile, including:

- **Construction and engineering:** Crews use tablets and laptops to access blueprints, log updates and communicate with project managers. Gadgets need to withstand dust and weather while keeping sensitive project data secure.
- **Manufacturing and industrial operations:** Rugged devices help teams on the factory floor monitor machinery, run diagnostics and report issues instantly. Their durability and security features prevent data loss and system interruptions.
- **Logistics and transportation:** Rugged handhelds keep things moving, from tracking deliveries to managing warehouse inventory. Real-time data sharing ensures accurate delivery schedules and smooth supply chain coordination.
- **Emergency and mobile health care:** First responders and paramedics use tablets to access patient records, coordinate care and share updates on the go. Devices must remain functional in chaotic, high-pressure environments.

4 Cybersecurity Benefits of Rugged Devices

Rugged devices also come equipped with features that strengthen cybersecurity in high-risk environments. These built-in protections offer peace of mind for industries handling sensitive data.

1. Secure Access Controls

Rugged gadgets offer durability and security features that protect sensitive data in the field. From biometric logins to smart card readers and multi-factor authentication, these tools help ensure that only authorized users can access critical systems and information.

Biometric security adds a strong layer of defense by using unique physical traits like fingerprints or facial recognition. This makes it harder for malicious third parties to break in, even if the device is in the wrong hands. This built-in protection is a big security win for industries relying on remote connectivity and real-time data sharing.

2. Fewer Entry Points for Threats

Rugged devices often feature minimal ports and tightly controlled software environments that reduce the attack surface. This locked-down approach makes it harder for unauthorized access or malicious code to slip through unnoticed. It’s an important advantage, especially as hackers increasingly target IoT and edge hardware, using them as gateways to infiltrate larger networks.

If a single vulnerable device is compromised, it can quickly escalate into a larger security breach affecting every connected system. Rugged gadgets help close that door before it opens, which makes them a practical choice for any business prioritizing secure operations in the field.

3. Enhanced Physical Security

The physical durability of rugged devices keeps confidential data safe, especially in industries where damage or disruption is a constant risk. Unlike standard hardware, these gadgets can survive drops, spills and rough handling without compromising performance or data integrity. This is especially true for rugged servers, which can handle environmental hazards like excessive vibration and temperature shock.

These physical risks can easily damage traditional systems, but rugged servers continue running smoothly in tough conditions. By reducing the chance of hardware failure, these gadgets also lower the risk of data loss or unauthorized tampering by minimizing downtime.

4. Compliance With Industry Standards

Many rugged devices are built to meet strict cybersecurity standards like HIPAA, which makes them reliable for industries that handle confidential information. These certifications reflect a machine's ability to securely support data storage, transmission and disposal. For example, HIPAA regulations require health care organizations to implement strong security measures that protect patient information at every stage.

Rugged handhelds that comply with these standards help businesses stay ahead of regulatory demands while reducing the risk of data breaches and costly penalties. This built-in compliance adds an extra layer of trust for teams working in health care, defense or other regulated sectors.

Why Rugged Devices Belong in Every Cybersecurity Strategy

For businesses operating in high-risk environments, rugged devices offer a smart, long-term investment that safeguards people and sensitive data. Integrating this tech into a broader security strategy can help industries stay resilient and better prepared as cybersecurity threats evolve.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on X (Twitter) or LinkedIn.

How Vibe Coding Is Changing the Economics of Software Development

Exploring how AI is shaping code editors, generators, and developer workflows

By Nahim Nasser, Head of Engineering, Georgian

Introduction

Software development has changed dramatically in recent years. Developers have moved from copying code from Stack Overflow to using ChatGPT for code suggestions, using Integrated Development Environments (IDEs) with AI-powered autocompletion, to now prompting large language models (LLMs) to generate entire applications. This shift is transforming how engineering teams work and is reshaping the economics of software creation and cybersecurity.

In this article, I'll explore how AI is shaping code editors, generators, and developer workflows. I'll examine the landscape of AI coding tools, the forces driving their evolution, and the implications of these changes—from democratizing development to addressing cybersecurity risks. By understanding these trends, organizations can better prepare for the opportunities and challenges of this new era.

The New Era of AI-Driven Development

According to a November 2024 AI adoption benchmarking report by Georgian and NewtonX, more than 50% of R&D (product/engineering/IT) leaders report seeing increased costs due to training and skills development for their teams. Furthermore, about 40% of R&D leaders reported that the absence of technical talent was a barrier to scaling AI.

It's not surprising that as we enter 2025, two trends are shaping developer workflows around code generation: "vibe coding" and autonomous agents.

Vibe coding enables developers to offload significant cognitive effort by allowing LLMs to take the lead in writing, debugging, and testing code. With vibe coding, users provide natural language prompts to describe their desired outcomes, and LLMs respond by generating code snippets, assisting with debugging, and validating functionality. This approach is making coding more intuitive, accessible, and efficient—even for individuals without traditional programming expertise.

AI coding tools are now leveraging advanced multi-step agentic architectures to manage entire development cycles. These tools can autonomously generate code, execute it in shells, verify its correctness, and request human validation only when necessary. Tasks that previously required weeks of manual effort are now completed in hours, constrained only by LLM token limits and GPU processing speeds.

For software engineers, this shift means that much of the traditional development workflow— reading API documentation, writing tests, code implementation, and verification—can be, and is being, automated. Rather than writing every line of code themselves, developers can now collaborate with AI tools to refine and optimize outputs.

Landscape of AI Coding Tools

Despite the explosive growth of AI-powered coding solutions, many tools converge around a core set of features, such as code completion and code understanding. While some tools aim for autonomous full-application generation, others remain IDE-first in their approach. At time of writing, product differentiation is partly being driven by tools designed for different developer audiences (front-end, back-end, etc.), and different interfaces and form factors (stand-alone IDE, extension, CLI-tool, etc.).

Open-source attempts at full automation have yet to reach high reliability (e.g., no major AI model has surpassed 50% auto-resolution on SWEbench's Full Test). Nevertheless, ongoing advancements in foundation models and agentic architectures are driving optimism around greater adoption and improved reliability.

Two Forces Driving Innovation

1. **Foundation Model Improvements:**

Progress in foundational models directly impacts the efficacy of AI coding tools. As models improve correctness, latency and cost, iteration speed for users materially improves. Competitors are racing to dominate public benchmarks like SWEbench, where correctness outweighs inference speed due to the high value of engineering tasks.

2. **Agentic Architectures:**

Beyond coding, LLMs are being integrated into agentic systems. These architectures break down problems into manageable tasks, allowing LLMs to execute complex workflows through "tool calling," memory management, and retrieval-augmented generation (RAG). By packaging multiple agents into cohesive systems, developers now have access to higher levels of abstraction, enabling tools that are more powerful and flexible than ever before. Many IDEs have even embraced model-context-protocol servers (you can think of them as mini-agent servers), which enable agents to call other agents – to achieve even more sophisticated workflows and tasks.

Implications for Software Businesses and Cybersecurity

While the rapid adoption of AI coding tools brings opportunities for software business, there are some barriers to adoption. 60% of R&D leaders are concerned about data privacy and security. Some opportunities and corresponding challenges for software businesses include:

- **Increased Code Production**: The ability to generate correct code in hours rather than weeks has dramatically reduced the cost of production. However, this also means that the amount of code being generated is growing exponentially, increasing the attack surface for cyber threats. Traditional security programs and approaches still apply, but may require increased automation, discovery of applications, and a federated secure software supply-chain in order to be effective. The ideal ‘shifted-left’ state involves code-generation tools becoming security-aware and environment-aware so it does not produce offending insecure code and applications – and we’re still in the early stages of this.
- **Accessibility for Non-Engineers**: Technology-adjacent professionals, such as project managers and product developers, can now produce code without formal engineering training. This democratization of code creation empowers a broader range of individuals to contribute to software development, fostering innovation and speeding up project timelines. However, it also introduces significant security risks, such as the potential generation of insecure code and vulnerabilities without the oversight of a skilled reviewer. Many organizations take the approach of hard isolation of applications from core systems and deploy ‘prototype’ or ‘marketing’ systems. But to enable both speed and security, this approach may be labour and cost intensive as it requires establishing the plumbing to spin up secure and ephemeral environments in a fully automated way.
- **Cybersecurity Economics**: It would not be far-fetched to extrapolate that the cost to produce software is materially decreasing from a labor perspective, particularly if an engineer can produce

something in days that used to take weeks or months. Unfortunately, the same math applies to bad actors using modern code generating tools to generate offensive code to exploit vulnerabilities. The decrease in cost and effort to generate code may result in an increase in the cost to defend systems. Startups, which often prioritize speed over security, may face increased risks as they scale. Large enterprises, which dominate cybersecurity spending today, may need to invest in solutions that account for the sheer volume of new code being produced.

The Path Forward

In my opinion, with the proliferation of AI-generated code, companies must prioritize scaling cybersecurity defenses to match the velocity of development. Open-source tools remain a vital equalizer for startups, but a broader shift is needed to improve the accessibility and affordability of security solutions for small and medium businesses. Without this, breaches—whether detected or not—are likely to escalate in frequency and impact.

Other key approaches that organizations can take to strengthen their cybersecurity practices in the age of vibe coding and agentic AI include:

- Maintaining tight access controls by ensuring that only authorized human and non-human entities are able to interact with AI models,
- Ensuring strong data governance practices by implementing strict rules around what data can be used and accessed by tools and AI agents, and
- Using monitoring and evaluation tools to monitor AI systems for anomalies like malicious prompts or unexpected model outputs.

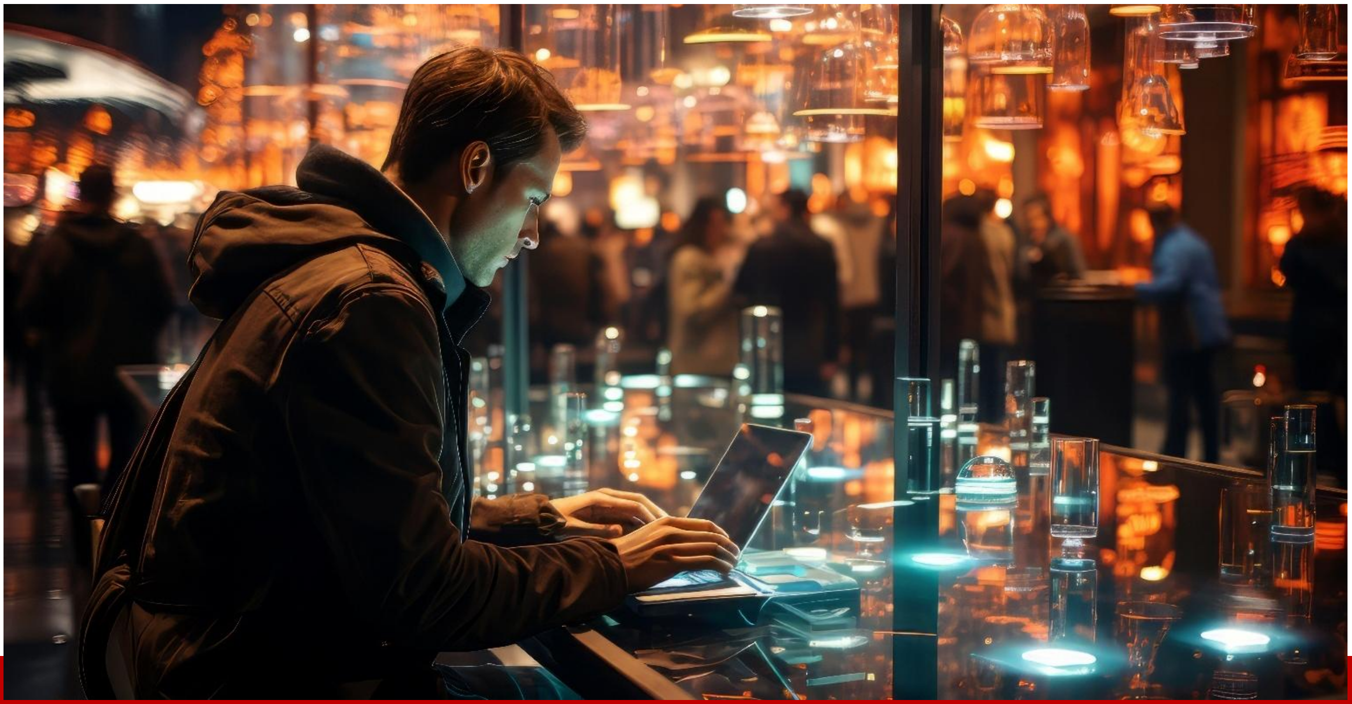
Furthermore, organizations can leverage LLMs to effectively enforce their visions, policies, and standards. Utilizing LLMs to scan for adherence to architectural patterns, standards, and security policies is a logical evolution from the automated code scanning processes employed in relation to the code review of legacy vendor tools. Moreover, LLMs could potentially be expanded to enforce broader policy compliance across various organizational functions, thereby enhancing overall governance and risk management.

As we move into this new era of AI-driven development, a key challenge will be balancing the productivity gains of tools like autonomous agents with the growing need for robust, scalable defenses. While vibe coding may redefine how we build software, it also calls for a fundamental rethinking of how we protect it.

(*Note: All statistics cited in this article have been pulled from* Georgian & NewtonX, AI Applied, November 2024*).*

About the Author

Nahim Nasser is the Head of Engineering in VC firm Georgian's AI Lab, where he leads the engineering team and collaborates closely with portfolio companies to accelerate growth. Previously, he served as VP of Engineering at Credit Sesame, CTO at STACK, and VP of Engineering at CoreLogic. Nahim studied software engineering at Carleton University in Ottawa. In his spare time, he enjoys working with bare metal servers and spending time with his toddler and chihuahua. Nahim can be reached at linkedin.com/in/nahimnasser and at Georgian's website: https://georgian.io/.



Why Managed Security Information and Event Management (SIEM) Is the Cornerstone of Modern Cyber Defense

By Anton Ovrutsky, Principal Threat Hunting and Response Analyst, Huntress and Dray Agha, Senior Manager, Security Operations Centre, Huntress

Visibility is the foundation of effective cybersecurity. Without it, detecting and responding to malicious activity becomes a guessing game, leaving attackers free to exploit weaknesses unnoticed. Security tools such as firewalls and endpoint agents play a critical role, offering essential insights into network and host-level activity. However, these tools are often focused on specific areas and are limited in the broader context they can provide.

Security Information and Event Management (SIEM) solutions address these limitations by consolidating and analysing data from across an organisation's entire infrastructure. This provides a more complete view of potential threats and attack patterns, connecting dots that would otherwise remain scattered. That being said, many traditional SIEMs struggle to deliver on this promise, often overwhelming security teams with unfiltered logs and irrelevant alerts. Instead of simplifying detection, they can bury critical insights in noise.

For smaller teams or organisations with limited resources, these challenges are amplified. Traditional SIEMs demand constant fine-tuning and highly skilled management to function effectively, making them a luxury only big enterprises can afford. This results in a tool that remains underutilised or shelved. Compounding the issue, the high costs tied to unpredictable data ingestion fees force organisations to choose between affordability and complete visibility.

This is where a Managed SIEM becomes indispensable. A properly managed SIEM solution compresses, filters, aggregates, and correlates telemetry data to cut through the noise, reduce costs, and provide security teams with clear, actionable insights. This enables faster detection, facilitates more precise responses, and empowers teams to proactively hunt threats before they escalate.

A Data Lake for Threat Hunting: Centralisation and Normalisation at Scale

One of the most powerful features of a SIEM solution is its ability to centralise and normalise vast quantities of log data.

Most devices—from servers and endpoints to firewalls and cloud services—produce logs that capture vital security-related activity. However, without centralisation, this data remains fragmented, inconsistent, and difficult to interpret in any meaningful way.

A SIEM brings all this information into one place and normalises the data into a consistent format. This makes it possible to apply detection rules, build correlations, and identify patterns that span multiple systems. This centralisation effectively creates a threat-hunting data lake: a unified environment where investigators can query, analyse, and cross-reference indicators. Unlike endpoint detection and response (EDR) tools, which primarily focus on host-level behaviour, a SIEM offers a much broader perspective across the entire infrastructure. This enables investigators to detect activity in areas that other tools simply don’t monitor, such as cloud logs, network appliances, or non-agent devices.

However, the full potential of a SIEM is unlocked when it is expertly managed. With carefully curated detections and the context provided by skilled management, a Managed SIEM can highlight anomalies, enrich events with threat intelligence, and surface high-risk behaviours. This reduces the operational burden on internal teams while enabling the proactive identification of early indicators of compromise, empowering organisations to respond before threats escalate.

Enhancing Visibility for Non-Agent Devices: The Value of Log Forwarding

Another often underappreciated advantage of SIEM is its ability to ingest data from systems where deploying an agent is either difficult or impossible. These include network appliances such as VPNs, firewalls, routers, switches, and legacy servers that cannot support agent installation.

These devices are often early targets for attackers. VPN gateways, for example, are commonly scanned for weak credentials or outdated firmware, while Remote Desktop Protocol (RDP) servers frequently face brute-force attacks. Since these systems are typically exposed to the internet and are relatively easy to exploit, they tend to be among hackers' first targets when attacking an organisation.

While these devices may not support rich telemetry, nearly all of them support the forwarding of syslog, a protocol that computer systems use to send event data logs to a central location for storage. By forwarding these logs into a SIEM, organisations can monitor authentication attempts, configuration changes, and network anomalies in real time.

With the right parsing and alerting, a Managed SIEM transforms basic syslog data into high-value security insights. For instance, repeated failed login attempts from a single IP address targeting multiple accounts could indicate brute-force activity. Similarly, a sudden spike in VPN sessions from a region with no known users might suggest compromised credentials. Without a SIEM, these signals could easily be missed. With a SIEM, they become clear warnings. In many cases, forwarding logs from such devices can drastically improve an organisation's visibility. It enables defenders to monitor areas that would otherwise remain blind spots and provides critical context for incident investigations.

Detecting and Disrupting Threats Early in the Attack Lifecycle

The earlier a threat is detected, the lower the cost and effort required to contain it. This principle lies at the core of the cyber kill chain, which outlines the stages of a typical intrusion. Catching an attacker in the early stages can prevent an incident from escalating into a breach.

A well-managed SIEM is uniquely positioned to achieve this. By collecting and analysing telemetry in near real time, it can detect malicious activity before attackers accomplish their objectives. Take brute-force attacks, for example. These are often used to compromise RDP or VPN services by automatically trying thousands of passwords. Such attacks are noisy, but they are only visible if someone is actively monitoring the relevant logs.

A Managed SIEM enables that monitoring. It can generate alerts for unusual login behaviour, excessive failed authentication attempts, or access attempts from suspicious locations. When integrated with other security tools, it can even automate response actions, such as blocking an IP address, disabling a user account, or terminating a VPN session.

Why Expert Management is Needed

Despite these many benefits, traditional SIEM solutions often fall short in practice. While they excel at consolidating and normalising vast amounts of telemetry, they demand constant fine-tuning and specialised expertise to remain effective. Without dedicated resources to manage configurations, tune alerts, and interpret insights, traditional SIEMs quickly become overwhelming.

This is where the value of a Managed SIEM becomes clear. Rather than placing the burden of deployment, configuration, tuning, and threat detection solely on internal teams, a Managed SIEM pairs the technology with experienced investigators who ensure it delivers real security outcomes.

For organisations without an in-house security operations centre (SOC), this model provides access to expert monitoring, tailored detections, and proactive guidance. This means organisations get not just more data but the right data, properly interpreted, enriched, and prioritised without having to build or maintain expensive in-house expertise.

A Powerful Tool in The Hunt for Hackers

In a world where cyber threats are increasing in both frequency and sophistication, the need for comprehensive visibility and rapid detection is more urgent than ever. A Managed SIEM offers both. It centralises data, extends monitoring to otherwise unmonitored devices, and helps defenders act before hackers can cause real harm.

Rather than seeing SIEM as a legacy tool or a compliance checkbox, we should recognise it as a critical pillar of modern cyber defence. With the right management and context, it becomes far more than a log aggregator. It becomes a proactive, intelligent engine for detecting and shutting down attacks, often before they even begin.

About the Authors

Anton Ovrutsky is the principal threat hunting and response analyst at Huntress. Ovrutsky transitioned into cybersecurity from a Service Desk role, initially gaining experience through governance, risk, and compliance work. He specializes in looking at the incidents that the SOC escalates that require more in-depth review. To put it another way, his expertise ensures that complex security incidents are thoroughly investigated and addressed. Anton holds several prestigious certifications, including CISSP, OSCP, OSCE, CCSP, and KCNA. Prior to joining Huntress, he gained valuable experience in the SIEM vendor SaaS space. Anton can be reached online at https://www.linkedin.com/in/antonovrutsky/?originalSubdomain=ca and at our company website https://www.huntress.com/.

Dray Agha is the senior manager, security operations centre at Huntress. Dray holds (among other certifications) an OSCP certification (Offensive Security Certified Professional). The training for OSCP covers several aspects of penetration testing, including network enumeration, vulnerability analysis, buffer overflows, web application attacks, privilege escalation and more. Dray specializes in Digital forensics and incident response and is interested in defensive and offensive information security. Dray can be reached online at https://www.linkedin.com/in/drayagha/?originalSubdomain=uk and at our company website https://www.huntress.com/.

Cybersecurity's Blind Spot: Why Human Behavior is Every CISO's Business

To truly protect people and systems, CISOs must close the gap between security tools and human behavior.

By Paige Schaffer, CEO of Iris Powered by Generali

When a major breach makes headlines, the impact ripples far beyond the individuals whose data has been compromised. It shakes consumer trust, triggers urgent internal questions from staff, and lands squarely on the shoulders of the CISO. And although cybersecurity leaders have long been focused on preventing and responding to attacks, the missing piece in many programs isn't technological. It's behavioral.

We have reached a pivotal moment in the data security conversation. Despite record-breaking investments in cybersecurity tools, the most vulnerable part of the equation remains underprioritized – the human element.

So, what does that mean for the modern CISO?

It requires shifting some of the focus from firewalls and frameworks to something less quantifiable but equally critical: a deep understanding of how people think, feel, and respond to risk.

Perception vs. Reality: The Consumer Confidence Gap

In April, we released the results of the *Identity & Cybersecurity Concerns (ICC) Survey*, a recent nationwide survey of U.S. adults, that revealed a telling contradiction. While 87 percent of people say they feel secure using internet-connected devices, nearly the same percentage – 85 percent – are also worried about being hacked, and 88 percent are concerned about password compromises.

This disconnect is more than just cognitive dissonance. It's a signal to cybersecurity leaders that traditional security awareness efforts are not resonating. Despite widespread messaging around strong passwords and cyber hygiene, only three in ten respondents said they follow all recommended data protection practices. In other words, consumers may feel confident, but most are not taking important personal steps that could significantly strengthen their protection.

This gap presents both a challenge and an opportunity for CISOs. The challenge is that many security programs are built on the assumption that users will act rationally and consistently follow best practices. In reality, evidence shows that this is rarely the case. This misalignment weakens even the most sophisticated of defenses – and highlights a need for a more human-centric approach to cybersecurity.

And herein lies the opportunity. CISOs can reassess how they evaluate their security programs and deliver cybersecurity. Are those programs designed primarily to protect systems, or to support the people who rely on them? This means going beyond technical controls and compliance checklists to consider the lived experience of users, how they perceive risk, what drives their decisions, and where they encounter friction or confusion.

The Human Behavior Challenge

The issue is not a lack of concern on behalf of the consumer (or your users). The survey found that 91 percent are worried about the use of artificial intelligence in cyberattacks. More than half say they feel only somewhat secure while using their devices, suggesting that anxiety lingers beneath the surface. Despite this apprehension and the mounting threats to their identity, inaction abounds.

The reasons vary, from unclear guidance to alert fatigue, to the perception that cyber protection is too complex. These barriers to behavior change are often underestimated by cybersecurity teams who assume that logic and policy alone are enough to drive compliance. But security is not just a technical challenge; it's a psychological one.

People do not always make rational decisions, especially when it comes to abstract or invisible threats like identity theft or account takeovers. They may acknowledge the risk but still reuse passwords. They may hear understand the gravity of a breach but do not take steps to monitor their accounts.

When organizational security programs fail to acknowledge how real people behave, even the strongest technological defenses can be weakened from within.

Indeed, as a CISO, it's important to recognize that employees are people first, and their personal habits carry over into the workplace. That’s why the broader consumer data we’re discussing is more than just market insight; it’s a mirror of employee behavior and, by extension, organizational risk. Promoting secure habits in their personal life – like offering identity protection as an employee benefit – reinforces a culture of security that protects both the individual and the enterprise. What strengthens people, strengthens the organization.

The Emotional Toll of Breaches

Despite common narratives of increasing consumer apathy in the wake of repeated breaches, our survey results tell a different story. A staggering 94% of respondents said they would be concerned if they received a notification that their sensitive information was involved in a data breach, with 75% saying they’d be extremely or very concerned.

This matters – a lot. Consumers aren’t tuning out, and they care greatly about their personal security. Breaches still trigger strong emotional reactions.

As a CISO, it’s important not to view breaches as an unfortunate setback; they are experienced as deeply personal violations, and they can either rebuild or permanently fracture trust. CISOs must recognize the emotional toll behind the breach and design their strategies accordingly. Technical remediation must be paired with empathetic communication, clear next steps, and real support to help people feel safe again. In short, organizations that treat breach response as a human experience (and not just a technical exercise) will be the ones who preserve loyalty in the long term.

What CISOs Can Do Differently

There is no one-size-fits-all solution, but there are ways to begin building a more human-centered cybersecurity strategy. Here are a few ideas:

- **Reframe security education around emotion, not just logic.** People are more likely to remember and act on stories than statistics. Tie guidance to real-life scenarios and outcomes.
- **Treat post-incident response like customer service**. Go beyond technical containment. Make it easy to understand and be emotionally supportive.
- **Focus on moments of vulnerability.** Identify when customers are most exposed and proactively offer protection and guidance.
- **Measure the human experience.** Track not just technical recovery, but how users feel, how long their recovery takes, and whether they are likely to trust the organization again.

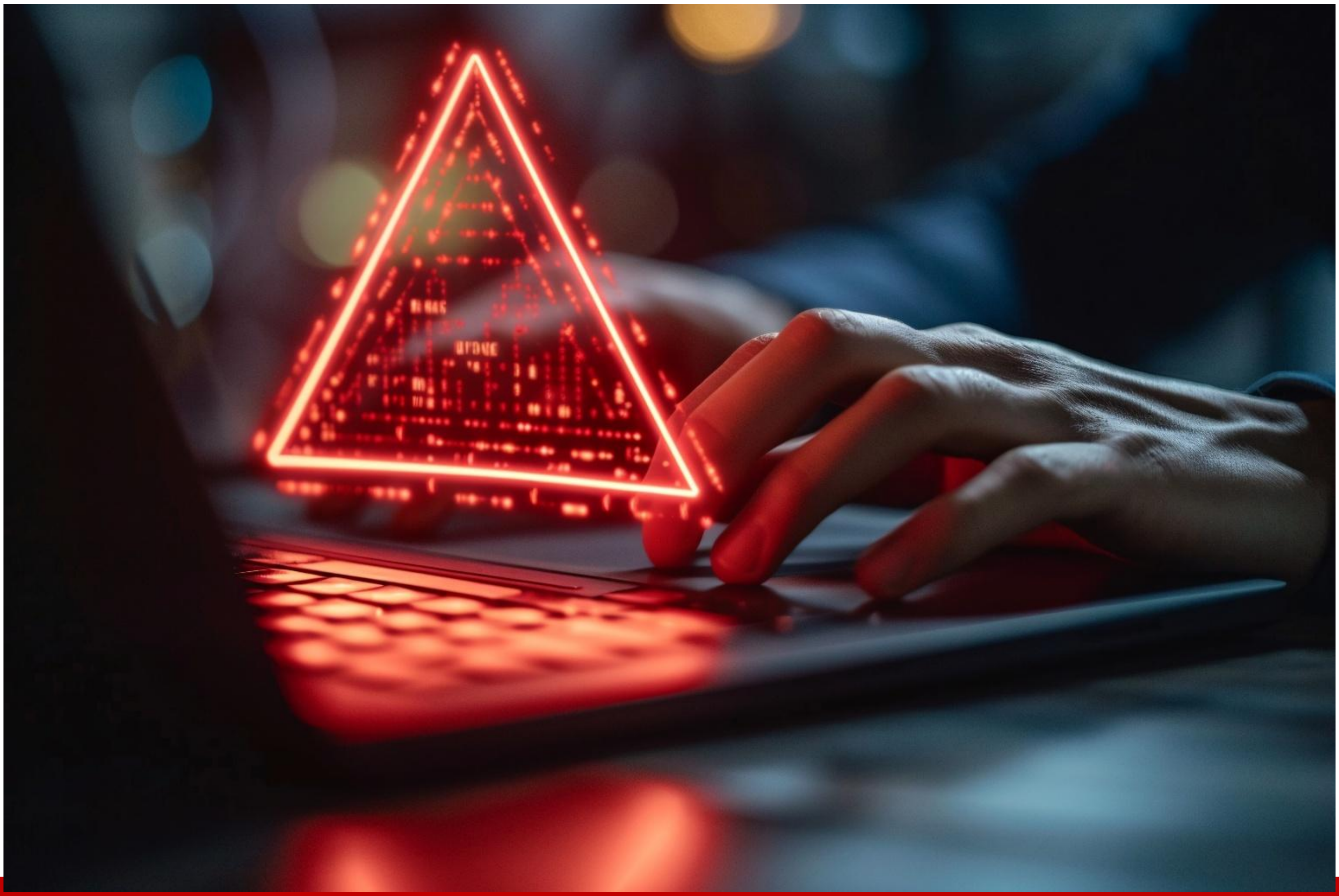
A Human-Centered Future for Security

CISOs are not only responsible for defending infrastructure. They are also responsible for safeguarding the human experience that lives within it. The future of cybersecurity depends not just on smarter tools, but on more empathetic strategies.

Protecting people means understanding how they behave, how they feel, and how they respond when things go wrong. Closing the experience gap is not just good practice; it is essential leadership.

About the Author

As CEO of Global Identity and Cyber Protection Services at Iris® Powered by Generali (the Company), Paige Schaffer leads sales & marketing strategy and revenue growth initiatives, managing operations as well global expansion. Leveraging her subject matter expertise of 15+ years in identity & cyber protection and restoration services, particularly as they apply to B2B2C software-as-a service, she was the visionary behind the behind the creation and evolution of Iris' innovative identity & cyber protection services. Under her guidance, Iris has secured multiple multimillion-dollar contracts with Fortune 500 companies, and Ms. Schaffer has directly sold new business and negotiated extended contract lengths, thereby maximizing revenue streams for the Company. Iris Powered by Generali's website https://www.irisidentityprotection.com/



Legacy Solutions Have Become a Cyber Defense Problem

By Kris Bondi, Co-Founder and CEO, Mimoto

The cyber defense community is at a crossroads that is magnified by cyber criminals' adoption of AI and ransomware-as-a-service. With year-after-year of the IBM Cost of Data Breach report showing the time to discover and contain a breach hovering around 200 days, it's obvious that AI and ransomware-as-a-service is not fully responsible for current situation. They've made a bad situation worse but aren't solely responsible.

With millions of dollars being invested in cyber security platforms, it's reasonable to ask why is so much still getting through and not being found. The best way to find the answer is to examine the problem: what is the common thread among both breaches and internal threats? People. While this is the undisputed answer, legacy security solutions focus instead on increasingly problematic substitutes, particularly credential.

When organizations manage access via credentials alone, they must accept that they're taking a calculated risk. If you doubt it, only look at the brute force attack that hit 2.8 million IP addresses daily from January and February of this year. It overwhelmed systems with millions of attempts to login with automated user and password combinations. This attack hit major security vendors, including Palo Alto Networks and SonicWall. Attempting to use security providers as the attack vector isn't new, but it is increasing.

While pairing credentials with MFA is a security posture improvement, MFA introduces its own set of security issues. We've seen it be leveraged by cyber criminals, who have resent credentials to grant themselves broader access and authorization. Just as it is sometimes forgotten that a credential is not a person, it should also be remembered that MFA is verifying a device at a specific point in time. There is no guarantee that the person holding the device is who you expect it to be. The credential and MFA combination model has been put to the test and failed when applied to hybrid, remote, and offshore teams.

Modern security practices diverge from legacy solutions in several critical areas. While legacy solutions focus on managing a process or understanding how an exploitation was possible. They attempt to work within existing or expected workflows. This approach of making a newer version of an approach that isn't working is doomed to fail. When legacy solutions introduce changes, they are often at the expense of the end user, in the form of additional friction in their processes. We've repeatedly seen that as friction is introduced, adherence to security protocols decreases. Making access cumbersome doesn't equal a more secure organization.

Modern security shifts from the credential-MFA model to a comprehensive understanding of who is doing what. Through the use of ML and AI, real-time person-based modeling at scale is possible in a way that wasn't even a few years ago. AI-enhanced behavioral-based analysis enables securities to identify when behavior, at a person-level, doesn't match what is expected. Obvious initial questions include: Is this person access from a different region? OR Are they using a machine they haven't used before? By adding AI-enabled behavioral analysis, signals may be added to address human-centric characteristics. With this important addition, false positive rates fall dramatically while real-time detection and response are added.

When considering modern security, it is not enough to send alerts if a potential anomaly is detected. SOC analysts, security engineers, and CISOs report alert fatigue. Increasing alerts without providing context increases noise and anxiety, does little to truly help the situation. Context is king! Instead of sending an alert indicating there is something odd with an account and should be checked, security solutions need to provide a deeper understanding of who is the person acting and what are they attempting to accomplish.

What modern security enables that legacy solutions struggle with is delivering real-time understanding of which person is actively engaged in malicious behavior.

About the Author

In prior executive leadership roles, Mimoto CEO & Co-founder Kris Bondi made a name for herself as a category creator and GTM strategist that significantly increased adoption and positioned companies. She contributed to seven acquisitions and two IPO filings. She's best known for making the "serverless" a movement and a category.

Kris is a pioneer in applying AI to real-world problems. As CMO of Neura, an Israel-based AI company, Kris championed the concept of products proactively interacting with people. This prior experience with a neural network of digital doubles has enabled her to determine where Mimoto's groundbreaking technology can immediately address an organization's most critical internal security gaps, as well as envision the company's future use cases.

Among her career highlights is as a stringer for the Harrisburg Patriot covering Nelson Mandela's first speech in the United States.

Kris can be reached online at https://www.linkedin.com/in/krisbondi/ and at Mimoto's company website https://www.mimoto.ai/

Mind the Middle

Cybersecurity Starts with Frontline Managers

By Thomas E. Armstrong, Director of Strategy and Enterprise Architecture for the State of Connecticut

In an era where digital threats can cripple a business overnight, where threat actors can use AI to customize and automate attacks at scale, and where enterprises face constant budget pressure, CISOs are asked to do more than ever before. They are accountable not only for protecting systems and data but for cultivating a culture of vigilance across the organization. Yet, amid the firewalls and frameworks, one vital element is often overlooked: the frontline IT Manager.

Many IT managers, especially those newly promoted, are thrust into leadership roles without the training they need. Yet, they are the operational backbone of any cybersecurity strategy. They manage the teams responsible for system administration, patching, endpoint protection, logging, and access control. They turn policy into practice and strategic intent into day-to-day action. When they falter, the consequences can extend far beyond system downtime.

Most IT managers aren’t trained for the combination of technical, operational and leadership pressures they’re expected to navigate. They’ve earned their roles through technical excellence but often without the management or leadership experience needed to succeed. They know how to configure group policy but not how to resolve team conflict. They can script an automation routine but struggle to delegate effectively. In a world where cybersecurity readiness increasingly demands cross-functional coordination, rapid decision-making, and trust with and across teams, we can't afford to leave these managers behind.

That's why, now more than ever, we must invest in the next generation of IT and security leaders.

Turning Policy into Practice

Most cybersecurity programs live or die on execution. A well-written policy is meaningless if the patching cadence isn't enforced. A defense-in-depth program breaks down when help desk tickets for MFA resets languish for days. CISOs understand this, yet too often, they lack the visibility into the middle layers of IT - the managers who control daily workflow and priorities.

New Managers often struggle to reconcile their past as hands-on technologists with the demands of their new leadership roles. This change is more than a shift in responsibilities; it's a redefinition of identity. For years, managers were measured by their ability to solve problems directly. Now, success depends on building teams and coaching others to resolve issues efficiently, securely, and at scale.

Every IT decision has security implications. Whether it's provisioning access for a contractor, delaying a patch to avoid downtime, or choosing not to enforce password complexity and MFA because "it's annoying," these daily micro-decisions shape the organization's risk posture. If IT managers don't have the training to think systematically, prioritize risk, and lead effectively, they can't help their teams do it either.

Members, Methods, and Measures

In my work with IT managers across the public and private sectors, I've found that effective managers succeed because they know how to guide people, shape processes, and track results. That's the essence of the *Members, Methods, and Measures* framework.

Let's start with **Members**. Security is social. It thrives on collaboration and trust, and it depends on well-functioning teams: system engineers who talk to developers, help desk agents who escalate what matters, and analysts who trust their instincts. But many IT teams operate in silos, hampered by poor communication, weak accountability, and eroded trust. New managers often inherit these dysfunctions, and without the proper support, they unknowingly reinforce them.

CISOs who want better operational outcomes need to look beyond technical training and invest in people leadership. Help your IT managers learn to conduct effective one-on-ones. Teach them to coach, not just correct. Encourage cross-training and build space for shared learning. You won't turn every manager into a security expert, but you can give them all the tools to lead teams that make good decisions, collaborate effectively, and execute consistently.

Then there are **Methods**. These are the practices and workflows that structure how work gets done. Is work flowing as intended or is every process a patchwork of tribal knowledge and kludgey workarounds?

Many operational routines evolve by accident. They're often shaped more by habit, legacy tools, or personnel turnover than by intention. But security depends on discipline and clarity. New managers need support to design processes that are secure from the start, and they need guidance to improve those processes continuously, not just in the aftermath of a security incident.

For CISOs, this means looking closely at how work is operationalized. Are security expectations embedded in daily routines? Are there bottlenecks or ambiguities that increase the likelihood of human error? When you empower your managers to shape secure methods and give them the autonomy to fix broken processes, you reinforce security at the foundation.

Finally, we come to **Measures**. In cybersecurity, we rely heavily on metrics: mean time to detect, patch velocity, incident counts, and phishing click rates. These are important indicators, but they don't tell the whole story. What's often missing are the measures that reflect how well our teams function: onboarding speed, workload balance, and the frequency with which team members raise security concerns without prompting. These human-centered indicators may not show up on a dashboard, but they profoundly impact long-term security outcomes.

Burnout, turnover, and misalignment lead to mistakes. And mistakes are the leading cause of data breaches. According to research from Stanford University, 88% of data breaches are caused by human error. If CISOs want to understand their true risk exposure, they need to measure not only how their tools are working but also how their teams are doing. Train and empower managers to track team health, work distribution, and process adherence. To build better resilience, help them make measures more meaningful with fewer vanity metrics and more actionable insights.

The Leadership Gap You Can't Ignore

In many IT shops, a quiet crisis is unfolding. There's a leadership gap that threatens execution and security alike. Brilliant technologists are being promoted into management roles with no roadmap. They're expected to mentor others, align execution to strategy, manage vendors, respond to incidents, and keep up with the relentless pace of change. And to do it all without formal training. In fact, according to Gartner, 85% of new managers receive no formal leadership training, often stepping into management based solely on their technical performance rather than their leadership readiness.

For a lot of CISOs, their focus naturally drifts up - briefing the board, preparing strategy decks, performing architecture reviews. But some of the most important decisions are happening lower in the org chart. We need to start with the frontline. That means finding the managers doing the work, talking with them, and understanding what they need. Give them the support, structure, and coaching that helps them lead.

Because, at the end of the day, technology doesn't run itself. The people behind the technology—patching systems, resolving incidents, making tough judgement calls—will determine whether your environment is truly secure. And the quality of those outcomes starts with the quality of their leadership.

Frontline managers turn your security strategy into reality. If we want stronger security, it starts with building stronger managers.

About the Author

Thomas E. Armstrong is an IT executive specializing in business transformation, digital innovation, and enterprise architecture. With leadership roles spanning global firms like Deloitte, IBM, and PwC, he has helped top organizations streamline operations, enhance customer experiences, and drive strategic growth. Currently the Director of Strategy and Enterprise Architecture for the State of Connecticut, Tom also teaches IT at the graduate level. He holds degrees from Georgetown, Quinnipiac, and Fairfield University, along with certifications in cloud computing, IT service management, and enterprise architecture. His book, Members, Methods, and Measures: Unlocking the Secrets of IT Leadership, is due out this fall from CRC Press. When he's not tackling complex IT challenges, Tom enjoys life in Connecticut with his golden retriever, Doug. Tom can be reached on LinkedIn at https://www.linkedin.com/in/thomasearmstrong/

Multifaceted Cyber-Attacks Require a Unified Defense Approach

By Rich Campagna, SVP, Product Management, NextGen Firewall, Palo Alto Networks

Gone are the days of attacks hitting a single product or vulnerability. Today, we're seeing the increasing use of multi-vector attacks and multi-stage approaches. For example, a DDoS attack in Indonesia used 20 different vectors in a single attack.

We can expect to continue to see an increase in sophistication and evasion from web-based attacks, file-based attacks, DNS-based attacks and ransomware attacks, which will make it more difficult for traditional, siloed security tools to effectively defend against modern threats. Preventing these attacks will require multiple security solutions to work together as part of an integrated platform to stop every attack along the kill chain.

The rise of multi-faceted attacks

Cybercriminals leverage a combination of tactics, techniques and procedures (TTPs), across multiple areas at once to breach defenses. These can include web-based attacks, file-based attacks, DNS-based attacks and ransomware attacks.

Palo Alto Networks researchers have found that new and unique attacks have increased by a factor of four each day – from around 2.3 million in January 2024 to about 8.9 million in January 2025. One example is Relayed Data Exfiltration via HTTP Headers. An attack of this kind leverages siphoning techniques to exfiltrate proprietary business and/or customer data without being detected. Such attacks slowly and quietly steal data, unlike smash-and-grab style attacks meant to exfiltrate as much data as possible before security teams are able to close vulnerabilities.

Here's what happens: the bad actors use your HTTP headers like an underground tunnel to take data from your network, camouflaging their actions so it looks like typical web traffic. Rather than shipping stolen data straight to the bad actor, small bits of data get inserted into crafty domains and sent to trustworthy internet services. As these services process the domains, they unwittingly forward the stolen data to the bad actor via DNS. Because many security solutions don't inspect HTTP headers for concealed data exfiltration, it's easy for bad actors to exfiltrate your data via this technique.

At the same time, AI is enabling malicious actors to carry out faster and more frequent attacks. Attackers will persist in using AI tools to enhance the scale, speed, and complexity of their attacks, aiming to infiltrate systems through any means possible.

A complex defense landscape

In the face of sophisticated threats, enterprises typically have a fragmented defense, with different products responsible for each aspect of the kill chain. This fragmented approach and tool sprawl is complicating cybersecurity efforts. The vast range of new attacks and attack vectors has made it especially difficult for traditional, siloed security tools to defend against modern threats effectively. In fact, the average organization has 83 security solutions purchased from 29 vendors; 52% of executives say that complexity of this kind is the single largest barrier to more effective security. Defense has become too complicated, too expensive, and too mistake-prone – every mistake is now costlier than ever.

An integrated approach

Security can't exist in silos; as more attack vectors are created, organizations need an approach that protects their dynamic attack surface from ever evolving threats, in an operationally efficient way. Enter platformization. Platformization converges multiple products and services into a single, united architecture. There is one datastore and one management plane for simplified operations, and every module is natively and seamlessly integrated with the others.

An increasingly important value of platformization is how it makes it easy to add new components that keep up with the latest challenges. For example, with a single platform, it is easy to add technologies such as Quantum Security, security for AI, AI copilots, secure browsers and AI-driven threat detection and response. These tools will protect corporate networks from current threats and be prepared to address future threats as well.

However, for platformization to perform well, several critical requirements must be met. First, each product or service added to the platform needs to be as good as or better than its equivalent point product available on the market. Second, it needs to be modular, which allows your company to grow into the use of the platform over time. And third, it needs to empower native platform integrations so that every solution is stronger than it would be by itself.

Done right, platformization offers huge benefits for organizations. According to the IBM Institute for Business Value, organizations using a platform approach require, on average, 72 fewer days to detect a security incident. They also require 84 fewer days to contain an incident. These companies also see an average rate of return of 101%, as opposed to 28% ROI for companies without platformization.

Platformization: Your key to cybersecurity success

Today's cyberattacks are multifaceted and complex, requiring modern organizations to respond with a multifaceted defense approach. But that approach shouldn't compound the complexity they're already experiencing. Platformization helps companies converge and optimize their many security solutions into one powerhouse protection strategy. This is not only more secure, but it also triples ROI and significantly reduces the time needed to detect and contain incidents. Platformization is a key method for effectively addressing today's and tomorrow's security threats.

About the Author

Rich Campagna is the senior vice president for network security, Palo Alto Networks largest business, with more than 65,000 customers. His team of expert technologists have delivered Hardware and Software Firewalls, Cloud-native services, and the highly regarded PAN-OS operating system. These platforms consistently rank #1 in market share and have been recognized as Leaders in the Gartner Magic Quadrant for Firewalls for 12 consecutive years. He is a dynamic leader that is passionate about building high performing teams that innovate and execute to establish strong differentiation and leadership in the market. Rich is a holder of several U.S patents, has co-authored 2 books on network security, and has won numerous nationally recognized awards for leadership and innovation.

Neural Hijacking: Is Your Brain Making Security Decisions Without You?

By Matthias Muhlert

Introduction: The Battlefield Inside Your Head

In cybersecurity, we master firewalls and encryption. But are we neglecting the most critical vulnerability? *The human brain.*

Every day, you make thousands of split-second security decisions. Most operate on autopilot, guided by neural wiring evolved long before phishing emails existed. These mental shortcuts, brilliant for survival, become gaping vulnerabilities when weaponized by attackers.

Welcome to **neurosecurity**—where neuroscience meets cybersecurity. Below, we dissect five moments your brain's instincts betray you, and how to fight back.

1. The Monday Morning Ambush: Overload Hijacking

Picture This: Monday, 8:59 AM. Your inbox explodes with "URGENT" flags. Drowning in chaos, you click a disguised "software patch" alert. Hours later: ransomware.

Why Your Brain Cracks Under Pressure

- **Cognitive Overload**: Your working memory—the brain's scratchpad—overflows, drowning subtle phishing clues.
- **Alert Fatigue**: Constant pings numb defenses. Attackers time strikes for peak chaos.
- **Monday Cortisol Surge**: Stress hormones blur focus, letting cleverly disguised threats slip through.

Attacker Playbook

- **Inbox Camouflage**: Phishing emails mimic routine maintenance alerts.
- **Urgency as a Weapon**: "ACTION REQUIRED" triggers your instinct to clear the queue — *fast*.

Build Your Defenses

- **Automate the Noise**: AI filters prioritize genuine threats.
- **Monday Morning Ritual**: 15-minute "security sweep" before tackling chaos.
- **Bite-Sized Training**: Reinforce habits with 5-minute microlearning, not annual marathons.

2. The 3 PM Slump: Fatigue Hijacking

Picture This: 3:07 PM. Brain fog sets in. A prompt flashes: "Security Update Required". Verification feels like climbing Everest. You type credentials… into a hacker's spoofed trap.

Why Tired Brains Take Shortcuts

- **Decision Fatigue**: Each choice erodes judgment. Your brain craves the easy path.
- **The Afternoon Energy Crash**: Attackers exploit lowered skepticism.

Attacker Playbook

- **"Quick Fix" Pop-Ups**: Mimic familiar tools to bypass scrutiny.
- **End-of-Day Urgency**: "Immediate Action" emails pressure hasty clicks.

Build Your Defenses

- **Micro-Breaks**: Mandate 5-minute walk-and-breathe sessions to reset focus.
- **Adaptive Authentication**: Demand extra proof (e.g., biometrics) during high-risk hours.
- **Flag Late-Day Traps**: Auto-highlight suspicious emails post-2 PM.

3. The Gut Reaction: Affective Hijacking

Picture This: An email punches your gut: “Major Layoffs Announced”. Heart racing, you click the link. Too late —i t’s a credential-stealing imposter.

Why Emotions Override Logic

- **Amygdala Hijack**: Fear/curiosity trigger lightning-fast neural pathways, sidelining logic.
- **Personalized Manipulation**: Attackers reference real events (layoffs, birthdays) to hook you.

Attacker Playbook

- **Fear as Fuel**: “URGENT: Security Breach!” compels panicked clicks.
- **Empathy Exploitation**: Charity scams tug heartstrings.

Build Your Defenses

- **Emotional IQ Training**: Teach staff to recognize manipulation.
- **AI Sentiment Scans**: Quarantine emails with hyper-emotional language.
- **The 5-Second Rule**: For charged emails: *Pause. Breathe. Verify.*

4. The Danger Zone of Routine: Habit Hijacking

Picture This: Morning autopilot. Log in, click prompts—muscle memory prevails. One prompt today? A spoofed “Enable Permissions” pop-up. You click. Malware installed.

Why Autopilot is Risky

40% Habit-Driven: Brains automate routines to save energy. Attackers slip malicious steps into workflows.

Attacker Playbook

- **Login Lookalikes**: “.co” vs “.com” domains.
- **Fake System Alerts**: Mimic updates you habitually dismiss.

Build Your Defenses

- **Disrupt Routines**: Rotate login steps or portal designs to force conscious attention.
- **Behavioral Biometrics**: Flag deviations in typing rhythms or mouse movements.
- **Gamify Vigilance**: Reward staff for spotting fake phishing prompts in drills.

5. The Authority Trap: Trust Hijacking

Picture This: An email from the “CEO”: “Wire $500K NOW for a confidential deal”. A flicker of doubt dies under authoritative tone. You comply. Funds vanish.

Why We Obey Blindly

- **Trust Circuits**: Requests from leaders activate brain reward centers, overriding skepticism.
- **Deepfake Danger**: Synthetic voices add chilling authenticity.

Attacker Playbook

- **Executive Spoofing**: Perfectly mimic email tone, signatures, and insider jargon.
- **Business Email Compromise (BEC)**: Send malicious requests from hacked executive accounts.

Build Your Defenses

- **Multi-Level Approval**: Require two signatures for financial actions.
- **Out-of-Band Verification**: Call the CEO’s direct line to confirm urgent requests.
- **Challenge Culture**: Empower staff to question *any* unusual directive.
- **Conclusion: Arming Your Mind**

Neurosecurity isn’t about blaming human error—it’s about **designing defenses that work with our brains**. By addressing overload, fatigue, emotion, habit, and trust, we transform vulnerabilities into resilience.

For CISOs: The future of cybersecurity isn’t just smarter tech—it’s **understanding how minds make decisions under pressure**. Train teams, tweak processes, and foster cultures where vigilance aligns with human nature.

When we master neurosecurity, the human mind stops being the weakest link—and becomes our most adaptable defense.

About the Author

Matthias Muhlert exemplifies Information Security leadership with over 25 years of transformative contributions. His career is marked by a commitment to empowering teams, optimizing processes, and leveraging cutting-edge technology to ensure operational excellence and strategic alignment with business goals. Currently, as the "Cyber Chef for Pies, Pints, Pastries, Parties, and Pizza" at Dr. August Oetker KG and serving as ECSO CISO Ambassador for Germany as well as DACH Chapter lead, Matthias is dedicated to fortifying digital landscapes against evolving threats.

His journey includes leading global security initiatives, fostering resilient and agile security frameworks, and building robust relationships across organizational levels. Matthias's expertise is validated by certifications such as ISO 27001 ISMS Manager, CISM, CISSP, and Certified Ethical Hacker. His roles have ranged from automotive CISO to spearheading IT security in banking, showcasing his ability to navigate the complexities of cybersecurity in diverse settings.

At Oetker-Group, Matthias is responsible for developing and setting security standards across all companies, orchestrating a group-wide security community, and devising comprehensive strategies for information and OT security. His tenure at HARIBO GmbH & Co. KG involved heading the information security management system, establishing a dynamic ISMS, and pioneering an AI decision model in collaboration with other companies. As CISO at Schaeffler Technologies AG & Co. KG, he led local and global teams, introduced an information risk management methodology, and contributed significantly to international security standards.

Matthias is also the author of Navigating the Cyber Maze: Insights and Humor on the Digital Frontier, further showcasing his ability to articulate complex topics and share his expertise with a broader audience.

There Are Plenty of Phish in The Sea: Here’s How to Avoid Them

By Andy Syrewicze, Security Evangelist at Hornetsecurity

When was the last time you revisited your organization's email security practices? Is your current software up to the task of defending your data against newer and more sophisticated cyber attacks? And is your team armed with the information and education needed to respond if it isn't? These are questions that are taking on greater significance as advancing technology increases our susceptibility to phishing attacks. Phishing is one of the most prevalent forms of email attack, accounting for 33.3 % of cases. So organizations need to do more to combat it.

Most of us depend on email for business, personal correspondence, and general life upkeep, and many tend to use our work email system to do so. In a bid to speed up tasks and operations, one might be tempted to sacrifice security for the sake of ease, forgoing inconveniences like two-factor authentication and other similar safeguards. While that may seem like a small omission to some, it’s important to remember that it only takes *one* successful phishing attempt for all that sensitive information in your email (and potentially your entire account or business!) to become public information. Organizations need to be hyper-aware of this and plan accordingly.

Where are the risks?

Let’s start with clearing up what we mean when talking about email security. Malicious emails can take many different forms. To name a few, there is Business Email Compromise (BEC), where a threat actor impersonates a business leader in the hope of conning the recipient into a money transfer. There are also malicious file attachments that may seem innocuous, but which carry embedded malware that infiltrates your computer and your company's network. Lastly, there’s phishing, which aims to deceive the recipient into clicking a link that leads to a dangerous website. The site may contain malicious code. However, the most common reason for most phishing emails is to compromise a user’s account or device. While all of these methods can lead to the leaking of sensitive information, phishing is the most prevalent – and with the advent of generative AI, attackers have found it much easier to create sophisticated and targeted attacks.

Think of the many things you might use your email for. Booking travel? That often means disclosing your credit card details, and passport ID. A government service? That might involve providing your social security number. Following up on a doctor’s appointment? Sensitive medical history could be accessible to hackers.

Who is vulnerable?

All email users face threats from cyberattacks. While different industries experience different impacts, no business that operates in the digital world is safe from these attempts. Industries like manufacturing and shipping are particularly vulnerable, as they offer attackers access to both IP theft and product disruption as a tool for negotiation and potential ransom. But they are by no means the only target. Brand impersonation is another area that continues to be a major issue for all businesses, with companies like FedEx, DHL, Facebook, DocuSign, Mastercard, and Netflix experiencing notable upticks in the last year.

What can you do?

The good news is that businesses no longer have to employ a roster of complicated applications and services to protect their information. The development of consolidated platforms has helped simplify cybersecurity by providing a single pane of glass view that detects and blocks threats in real time, while also preventing data loss and enabling compliance with industry regulations. Modern solutions incorporate AI such as artificial neural networks, useful for recognizing patterns, [and] deep learning, which improve computer vision, speech recognition, natural language processing and image classification. This means that incoming cyber-attacks are dealt with before they can land in an inbox.

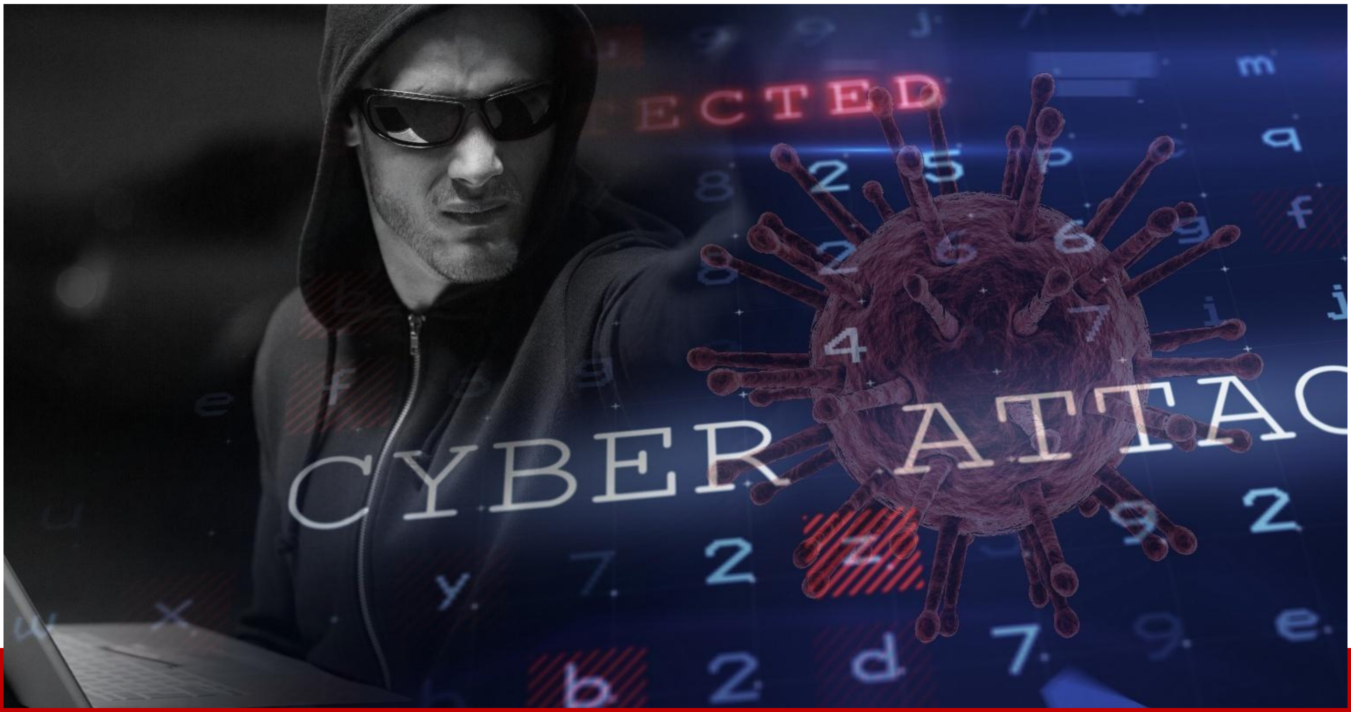
These days, there is no shortage of helpful suggestions for improving digital hygiene and knowing the signs of a phishing attempt. But with more advanced hackers and cyberattackers, organizations need more than good instincts to protect their information – they need good, ongoing, company-wide training.

As it stands, 26% of organizations are failing to provide any IT security training to end-users, and many of the programs that do exist are insufficient to meet the specific challenges of the moment. Undergoing comprehensive, current, and expert-developed cybersecurity training is absolutely critical to securing your data. Effective training should educate the user and cultivate awareness, but should also include practical, immersive simulations in preparation for real-world situations. It should inform users on how to prevent attacks, while also providing them with the resources to act quickly and effectively should one occur. This means getting familiar with backup and recovery processes so that nobody is caught without a plan of action in a worst case scenario. In the event of a breach, navigating the situation with a cool head and clear procedure can significantly minimize damage done and time lost. Ultimately, finding the right software is important, but the tools are only as good as the user behind them.

As phishing technology has progressed, so have threat detection capabilities, breeding a new tier of cybersecurity tools to safeguard your data and give you peace of mind. As the saying goes, information is power. Don't wait to safeguard yours.

About the Author

Andy Syrewicze, Security Evangelist at Hornetsecurity, is a 20+ year IT Pro specializing in M365, cloud technologies, security, and infrastructure. By day, he's a Security Evangelist for Hornetsecurity, leading technical content. By night, he shares his IT knowledge online or over a cold beer. He holds the Microsoft MVP award in Security. https://www.hornetsecurity.com/en/



Post Quantum Threats - The Encryption Apocalypse That Isn't

Why your data breaches will have nothing to do with tomorrow's quantum computers

By Sid Dutta, Founder & CEO, Privaclave Inc.

Preface

RSA Conference just wrapped up, and while phrases like "We are an Agentic AI solution for XYZ," "AI in Cybersecurity," and "Risks of AI Adoption" echoed across the expo halls, panels, and keynotes, you probably caught a few sessions on quantum threats and Post-Quantum Cryptography (PQC) too.

Beyond RSA, the noise about quantum is everywhere!! Articles, LinkedIn rants, webinars, fireside chats, even happy hour small talk - all swirling around a common narrative: quantum computers will soon break all encryption, and attackers will "harvest now, decrypt later."

On one end, pundits (many without any background in cryptography) are proclaiming that "the sky is falling," insisting some nations have already built quantum machines capable of breaking encryption. On the other hand, vendors are pushing "quantum-safe" solutions or offering tools to make you "crypto-agile."

So, the natural reaction? "Why bother encrypting anything if it's all going to be broken anyway?" Some even ask, "Is protecting customer data with current encryption still relevant?" Or "Should I just buy whatever that shiny PQC product was at the RSA booth with the fancy swag and wine webinar?"

Here’s my take: **It’s all BOOP** (*Blown Out Of Proportion*)!!

Not because it’s baseless, but because it’s rarely explained accurately, fully, and in context. So before we enter “hair-on-fire” mode, take a breath. Let’s unpack this in smaller, digestible pieces, clearly and pragmatically.

But first, a quick detour: Quantum computers aren’t your most immediate threat. It’s not some teenager with a quantum laptop breaking your encryption next year.

The real threat? Your current security postures.

The next data breach your company suffers likely won’t come from quantum. It’ll come from a misconfigured bucket, a compromised credential, a 3rd party security gap, an unsecure code, a vulnerability you didn’t patch, an exposed API, or lack of visibility of where your data is or moving.

As the saying goes: "There are two types of companies - those who’ve been breached, and those who don’t know it yet."

What Can Quantum Computers Actually Break?

Let’s be clear: quantum computers, once scaled to a large, fault-tolerant state (~4,000+ logical qubits), will completely break many of today’s most widely used asymmetric encryption algorithms. These include:

ALGORITHM	VULNERABILITY	WHY IT BREAKS	IMPACT
RSA	Broken	Integer factorization	TLS, email, digital signatures
Diffie-Hellman (DH)	Broken	Discrete log problem	VPNs, SSH, key exchange
ECC / ECDSA	Broken	Elliptic curve discrete log	Blockchain, TLS, certificates
DSA	Broken	Discrete log variant	Code signing, auth, crypto wallets

Once those machines arrive, these algorithms will fall, much like how short passwords do today.

Now, when that will happen is still debated. Some experts estimate we're 5–15 years out from a truly "cryptographically relevant" quantum computer. Others argue it's closer than we think. Regardless, one thing is clear: data encrypted today using RSA or ECC can be recorded now and decrypted later, the infamous "**Harvest Now, Decrypt Later**" threat.

A Real-World Example: TLS Under Quantum Attack

TLS (Transport Layer Security) secures most internet traffic, from HTTPS websites to API calls. But it heavily relies on asymmetric cryptography during the handshake phase.

TLS Workflow (Simplified):

A. Handshake Phase

- Uses RSA or ECDHE to exchange keys
- Verifies identity with a digital certificate (RSA or ECDSA)

B. Data Phase

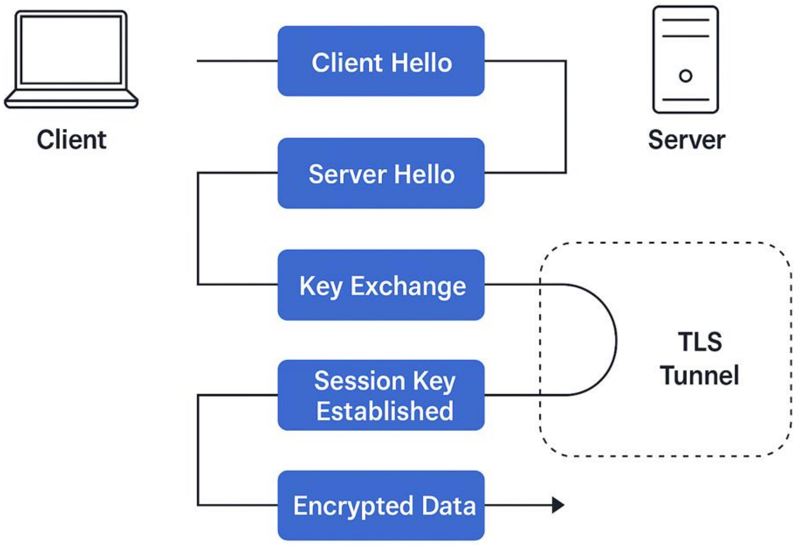
- Uses symmetric encryption (AES) with the shared session key

Quantum Breaks TLS Here:

TLS Function	Crypto Used	Quantum Threat	Impact
Key Exchange	RSA / ECDHE	Shor's algorithm	Session keys exposed
Certificate Signature	RSA / ECDSA	Shor's algorithm	Server impersonation possible

So, When Will Data Be Exposed in a Post-Quantum World?

Let's walk through a familiar example: a TLS connection using RSA or ECDHE for key exchange.



Here's how an attacker with a quantum computer compromises it:

1. Record the TLS handshake and encrypted session now
2. Wait until quantum computers mature
3. Break RSA/ECDHE using Shor's algorithm
4. Recover the AES session key
5. Decrypt the payload (your data)

Even AES-256 encryption (used in the data phase) remains secure, but if the session key is exposed, the encryption is worthless.

Even TLS 1.3 with ephemeral key exchange and AES-256 can be retrospectively broken, if the handshake uses quantum-vulnerable algorithms.

The Bottom Line

Quantum computers will compromise:

- Session keys via broken key exchange
- Identities via forged signatures
- Data, if it's been captured and encrypted using today's public-key algorithms

And it's not just about data in transit. Even data at rest (like archives and backups) may be exposed if:

- AES keys are wrapped with RSA/ECC
- Or the payload itself was encrypted using public-key crypto

So, the threat isn't always direct. It can be indirect, cascading through broken authentication, confidentiality, or integrity guarantees.

What’s Being Done About It

To get ahead of this, NIST has standardized four core Post-Quantum Cryptography (PQC) algorithms, forming the foundation for future-proofing security systems.

Algorithm	Type	Purpose	Typical Use Cases
Kyber	Lattice-based (KEM)	Key exchange (fast, efficient)	TLS, VPNs, messaging, encrypted storage
Dilithium	Lattice-based (Signature)	General-purpose signatures	TLS certs, code signing, digital documents, auth
Falcon	Lattice-based (Signature)	Compact signatures for constrained devices	Smart cards, mobile apps, hardware modules
SPHINCS+	Hash-based (Signature)	Stateless, conservative option	Archival signing, compliance systems, backup PKI

Are Symmetric Algorithms at Risk?

Not broken but weakened.

Quantum computers don’t break AES or ChaCha20 with Shor’s algorithm (they’re not based on factorization or discrete logs). But Grover’s algorithm can reduce the effort needed to brute-force them.

Algorithm	Classical Attack Complexity	Quantum Attack Complexity (Grover’s)
AES-128	2^{128} guesses	2^{64} guesses (quantum weakened)
AES-256	2^{256} guesses	2^{128} guesses (still strong)

Grover's algorithm gives a quadratic speed-up, not exponential, so doubling key sizes is an effective defense. Symmetric Encryption Is Still Safe (If You Use Strong Keys).

These are the algorithms, and their quantum impacts and mitigations:

Algorithm	Status	Quantum Impact	Mitigation
AES-128	Weakened	Becomes equivalent to AES-64	Use AES-256 instead
AES-256	Still Strong	Becomes equivalent to AES-128	Still secure
ChaCha20	Still strong	Weakens brute force to 2^128	Safe alternative to AES
SHA-2 / HMAC	Weakened	Hash collision search speeds up	Use longer digests (e.g., SH 384+)
FPE-FFX	Still Strong	With AES-256 becomes equivalent to AES-128	Still secure as long as AES-2 is used

AES-256 remains secure even under quantum attack, as 2^{128} operations is still practically infeasible.

Not All Data Is Worth “Harvest Now, Decrypt Later”

Let’s be clear, the “Harvest Now, Decrypt Later” risk primarily applies to data that will still matter years or decades from now, such as personal health records, national identifiers, legal contracts, or intellectual property.

But a lot of data doesn’t fall into that category. Much of it is:

- Ephemeral (chat messages, alerts)
- Time-limited (access tokens, session IDs)
- Low value (performance logs, anonymized metrics)
- Rotated or short-lived (credit card numbers, transactional data, temp keys)

In these cases, quantum attacks later won’t matter because the data will no longer be useful or sensitive.

Are Hackers Really Banking on “Harvesting Now, Decrypting Later?”

While quantum fear fuels urgency, let's be real: **Data Depreciates, Fast**. The idea that attackers will store encrypted data for a decade hoping it becomes useful later is economically unrealistic. Most hackers are after instant payoff, not for a future payday. They target what's monetizable now, such as credentials, financials, sensitive PII; not data that could be worthless in five years. Quantum may be real but immediate profit still drives the motivation and breach.

You Don't Necessarily Need PQC to Prevent a Data Breach

What if I told you that you can still protect your data effectively using today's tools, and you don't necessarily need to adopt PQC right now?

Don't believe me? Fair. Keep reading.

Let's revisit that TLS scenario we walked through earlier. Now imagine that, instead of relying solely on the TLS session key to protect sensitive data, the payload itself had already been desensitized - meaning the sensitive fields were:

- Encrypted using AES-256, or
- Tokenized with Format-Preserving Encryption (FPE-FFX using AES-256)
- All done using a separate symmetric key

Now consider what happens when an attacker:

1. Records the full TLS handshake and encrypted session
2. Obtains (or waits to obtain) a quantum computer
3. Breaks RSA/ECDHE/ECDSA using Shor's algorithm
4. Derives the session key
5. Decrypts the TLS payload
6. Discovers sensitive fields that are still encrypted or tokenized with AES-256/FPE-FFX
7. Can't decrypt the sensitive data because Grover's algorithm isn't enough to break AES-256

Same Applies to Data at Rest, Backups, and Archives

If sensitive fields in stored or archived data were pre-desensitized with AES-256 or FPE-FFX, then even if the outer AES key (wrapped with RSA/ECC) is compromised via quantum methods, the core sensitive fields remain protected.

In both cases, quantum attacks are neutralized by a single smart move: desensitizing sensitive data before it travels, gets stored, or is shared.

Why "Harvest Now, Decrypt Later" Doesn't Always Apply

The HNDL threat can be rendered irrelevant if enterprises:

- Desensitize sensitive data upfront
- Use strong symmetric encryption (AES-256) or format-preserving tokenization (FPE-FFX)
- Avoid relying solely on TLS

This approach keeps data persistently protected - at rest, in transit, and even in use. So even if an attacker (or insider) compromises access credentials and exfiltrates data, what they get is garbage. The data exfiltration incident doesn't escalate into a data breach.

Quantum Isn't What Will Breach You Today

The real risk isn't quantum. It's poor security hygiene!! Most enterprises still rely on outdated, compliance-driven playbooks: encrypt at rest, use TLS, and apply access and perimeter controls. But common missteps like hardcoded secrets, keys stored with data, and quantum-vulnerable key wrapping (like RSA/ECC) still leave you wide open, even with AES-256.

Migration to PQC Is Important — But Not Your Only Defense

Yes, post-quantum cryptography will be vital for long-lived systems, especially those tied to trust (e.g., TLS, PKI, digital signatures). But let's not mistake it as a silver bullet. You don't need PQC to protect all data, or PQC won't protect your data, if your current practices are already flawed.Your Current Path Towards Being Quantum Safe

The most practical path to becoming quantum-safe isn't waiting for standards or overhauling your infrastructure, but by protecting data at the field level using quantum-resilient techniques like AES-256 or FPE-FFX. This keeps sensitive data persistently protected not just at rest or in transit, but even during use. By decoupling security from platforms and perimeters, this approach future-proofs enterprises for a world of AI agents, APIs, and decentralized workflows, ensuring that even if systems are breached, the data itself stays secure.

The Better Way: Frictionless, Persistent Data Protection

While legacy data security tools exist, they're invasive, developer-heavy, and costly to integrate — often requiring:

- Deep cryptographic knowledge
- App rewrites or instrumentation
- Lengthy development and deployment cycles

You need solutions that enable automated, non-invasive/non-disruptive encryption & tokenization of sensitive data at the individual data element level, without breaking your applications, workflows, or budgets. What you get are:

- Persistent protection of sensitive data
- Defense against today's threats and tomorrow's quantum risks
- Accelerated Risk Remediation
- All with a fraction of the effort, cost, and time required by incumbent tools

The Future is Runtime Data Security

As enterprises embrace AI-driven workflows and autonomous agents, we're entering the age of Runtime Data Security, where data is constantly in motion, accessed, transformed, and acted upon in real time, and in a lot of cases, autonomously without any human supervision. In this new paradigm, traditional security models that rely on static controls, perimeter walls, and post-facto scanning simply don't apply, with or without PQC.

It's the age of Runtime Data Insights & Protection (RDIP), enabling enterprises to see, secure, and control sensitive data as it moves, in real time, across AI agents, APIs, legacy systems, and modern stacks. With automated and real-time visibility, and persistent desensitization, RDIP solutions make the journey from risk detection to protection frictionless, and future ready.

Because in the era of quantum uncertainty and AI autonomy, only runtime security is effective security.

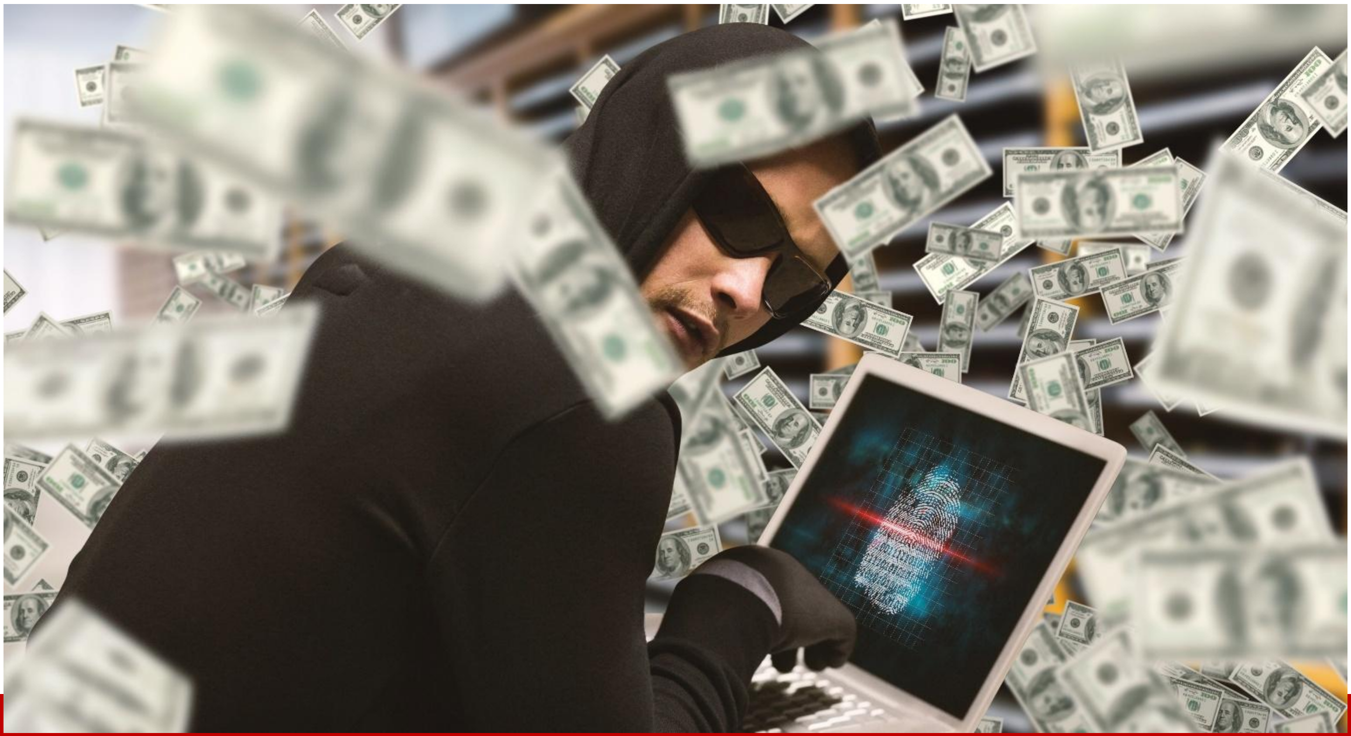
About the Author

Sid Dutta is a Data Protection and Cybersecurity Executive, a Security Advisor, an entrepreneur, with multiple patents and industry certifications. With 23 years of industry experience, Sid has been driving Data Protection and Privacy programs for the last 10 years across multiple large enterprises and has worked on/with various data security solutions including Data Discovery & Classification/DSPM, Data Subjects Rights Management, PKI/Certificate Management, Encryption, Tokenization, Key Management, P2PE, Payments and General Purpose HSMs, CASB, and various Cloud Security services.

He has also served on several vendor and Cybersecurity advisory boards and provides security advisory services to startups. Sid has multiple issued patents to his name and majority of them are within the domain of cryptography, blockchain, and tokenization.

He holds a master's degree in business administration, and a bachelor's degree in Electronics & Telecommunications Engineering. He is currently the Founder & CEO of Privaclave™, but prior to that he has held several Cybersecurity Leadership Roles, such as, Vice President – Data Protection & Privacy Engineering, at Activision Blizzard (Microsoft Gaming); Product Head – Voltage SecureData, OpenText (formerly Micro Focus); Vice President – Global Head of Data Protection & Applied Cryptography, Worldpay; and Director – Cryptographic Utilities & Services, American Express.

Sid can be reached online at sid.dutta@privaclave.com , https://www.linkedin.com/in/sid-dutta/ and at the company website https://www.privaclave.com/.



Preventing Costly Data Breaches Requires a Robust Physical and Digital Security Posture

By Santiago Del Portillo, Senior Manager of Tech Support and Systems Engineering, Kensington

Independent market research firm Vanson Bourne recently conducted a study querying 1,000 senior IT decision-makers across the US and EMEA regarding their organizations' security policies for reducing and preventing data breaches. The study revealed that 46 percent of respondents had experienced a data breach as a direct consequence of an unsecured device. As workers become increasingly mobile due to hybrid or remote working practices, the security risks of losing devices or data increase dramatically, exposing companies to potentially damaging financial and legal consequences.

Physical and Digital Security Deliver Robust Protection Against Data Theft

Protecting against the theft of valuable company data requires both positive control over work devices (i.e., laptops, desktops, tablets, and smartphones) and the ability to deny access to the data by unauthorized individuals or entities. A stolen laptop does not just result in the loss of hardware; it opens up the possibility of a potential data breach. Cable locks protect corporate assets and sensitive data from being compromised by providing an effective visual and physical deterrent against the theft of devices in offices and public spaces such as coffee shops and airports.

However, a robust physical security protocol is not a foolproof solution for preventing data theft. The Vanson Bourne study found that 38 percent of participants who reported using security locks experienced a data breach or loss of sensitive data due to an unsecured device.

Organizations are increasingly combining physical security and digital authentication methods to ensure the security of corporate devices and the data accessible through them. Digital security is no longer as simple as creating strong passwords and changing them regularly. Technologies such as biometrics, hardware- or token-based authentication, and zero-trust principles are key to providing robust protection against data breaches and theft.

Digital authentication methods include TouchID, MFA tokens or security keys, and push-based apps that provide OTP (One-Time Passwords) or codes to log in. For instance, Windows Hello and Hello for Business integrate with hardware keys, such as Kensington's VeriMark™, to bridge the gap between physical and digital security. These solutions require both a unique key to be connected to the device and a fingerprint swipe to log into the device.

Even with strong physical security and digital authentication protocols in place, visual hacking remains a significant threat, especially in public places. Privacy screens significantly narrow the viewing angles of laptops, monitors, and mobile devices to reduce the risk of unauthorized viewing and protect sensitive information. The use of privacy screens as a physical security measure can prevent data leaks when working in open spaces, ensure compliance with data privacy laws, and reduce visual distractions while working.

Biometrics are the Future of Data Security

Biometrics is gaining popularity due to its high accuracy and convenience, eliminating the need for complex passwords and allowing devices to be accessed using the individual users' unique physical or behavioral characteristics. Facial recognition and fingerprint scanning are becoming standard authentication methods, making it easier and more secure for users to access their devices and data.

Device manufacturers have incorporated biometric authentication technology as a native security component of their operating systems. For instance, the goal of Microsoft Windows Hello is to reduce reliance on passwords, which are the weakest link in cybersecurity. macOS devices use Touch ID to provide secure fingerprint authentication on MacBooks, iPhones, and iPads, and Face ID, which is an advanced facial recognition technology powered by Apple's TrueDepth camera system. ChromeOS devices utilize security key integration for multi-factor authentication (MFA) online services and apps.

At the enterprise level, many companies are deploying Windows Hello for Business to provide a passwordless, phishing-resistant authentication experience for their employees. Using this authentication protocol enables users to log in quickly with a touch or glance and enhances data security by eliminating the phishing risks tied to passwords. In addition to eliminating passwords through the use of biometrics or FIDO security keys, Windows Hello for Business integrates seamlessly with corporate security policies and provides an audit trail of logins.

The Rise of Security Keys (FIDO2, U2F, and Beyond)

Unlike traditional passwords and SMS-based two-factor authentication (2FA), hardware-based authentication provides virtually unphishable security by relying on factors that make it difficult to compromise remotely. Universal 2nd Factor (U2F) uses physical USB or NFC devices in addition to a password to provide strong but simple user authentication. Security keys, like Kensington's VeriMark™, integrate biometric authentication and hardware security to provide enhanced protection.

Companies like Microsoft, Google, and Apple are pushing to replace legacy authentication with security keys that support passwordless standards and applications like FIDO2 and WebAuthn, which use more secure methods like passkeys and hardware security keys. New upcoming technologies like FIDO2.1 will further enhance security, providing enterprise-level authentication and integration with more online service applications. The adoption of security keys as a vital component of MFA will continue to grow as businesses face the ever-increasing threat of data theft and breaches caused by remote work, and the need to provide privileged access to systems and protect high-risk accounts.

Industry Trends Shaping the Future

- **Passwordless Authentication**: Given the inherent vulnerabilities and IT-related challenges of traditional password systems for authentication, passwordless authentication will continue to grow in adoption across government, enterprise, and consumer devices.
- **Zero-Trust Security**: Organizations are moving toward a "never trust, always verify" approach that prioritizes strong authentication methods. In a Zero-Trust environment, trust by default is replaced by continuous verification and authorization for every access.
- **AI and Security**: Advances in machine learning and AI-driven biometric authentication will further enhance security to detect spoofing attempts and deepfake threats.
- **Regulatory Compliance**: Global regulations will continue pushing companies toward passwordless authentication.

About the Author

Santiago Del Portillo is the Senior Manager of Tech Support and Systems Engineering at Kensington. With over 10 years of experience in technical sales and engineering, Santiago has been a key player in the security industry. He joined Kensington seven years ago and has since performed various roles, including Security Category Marketing Manager, Sales Engineer, and Tech Support Manager. Santiago's extensive expertise and dedication to advancing security solutions have made him a trusted authority in the field. Santiago can be reached online at Santiago.DelPortillo@kensington.com and at our company website https://www.kensington.com

Effortless Cloud Security: A Beginner's Checklist for a Safer Cloud Environment

By Ranjan Kathuria, Cloud Security Architect at Rubrik Inc.

In the past few years, the world has embraced a new era of AI, introducing an array of security tools that leverage advanced technologies to automate deployments, conduct real-time scanning, agentless scanning and monitor user behavior for unusual activity. Despite these innovations, security incidents and attacks from malicious threat actors remain prevalent. Why is this the case? The answer lies in "misconfiguration." When misconfigurations occur in the cloud, the consequences can be dire.

What Is Cloud Misconfiguration and How Does It Happen?

Cloud misconfiguration refers to any insecure settings or configurations within a cloud environment. For instance, creating an IAM user without enforcing Multi-Factor Authentication (MFA), allowing root or admin accounts to bypass MFA, or failing to configure a load balancer to mitigate high-traffic spam attacks or denial-of-service attacks are all examples of misconfigurations.

Misconfiguration often occurs for several reasons:

1. **Overconfidence in Expertise**: Many individuals assume they are cloud experts simply because they find it easy to use. While cloud platforms can be user-friendly, they still require a comprehensive understanding of security practices.
2. **Misplaced Reliance on Application Security**: It's crucial to remember that merely identifying vulnerabilities in code will not resolve misconfigured cloud settings. Application security is just one piece of the puzzle.
3. **Pressure for Speed and Manual Processes**: The need to innovate quickly can lead to shortcuts in security protocols. Relying on manual processes can create deviations from automated security systems, resulting in potential gaps in protection.

What Does a Misconfiguration Look Like?

Many cloud breaches occur when the basics of cloud security are neglected, often due to what can be described as "**overconfidence in expertise**." Organizations sometimes over-engineer solutions and overlook the fact that many problems can be resolved with straightforward fixes.

Consider the scenario where a new cloud environment is created without implementing essential and basic security measures:

- **Single Sign-On (SSO) Users**: Users are still relying on usernames and passwords to log in to their cloud accounts.
- **No Multi-Factor Authentication (MFA):** MFA is not enforced for user logins.
- **Lack of Cloud Security Policy Restrictions**: Most cloud providers offer options to enforce security policies, such as disabling external IP addresses on cloud resources, preventing the use of insecure protocols like IMDSv1, and restricting internet access to critical ports like SSH, RDP, and various database ports.
- **Insecure Identity and Access Management (IAM):** Users have overly permissive roles that grant excess access beyond what is necessary for their tasks.

In the above example, we highlight two critical pillars of cloud security: **identity and access management**, as well as **cloud security policies**. Strengthening these pillars can significantly reduce vulnerability to attacks in your cloud environment.

Imagine a scenario lacking all the above-mentioned measures. The consequences of such misconfigurations could include:

A non-SSO user accessing the system with just a username and password, coupled with no MFA, could create additional users, access keys, and resources. Without enforced cloud security policies, this user may be able to create a new network completely exposed to the internet, allowing public access through SSH or RDP. Let's analyze the potential risks involved:

1. **Non-SSO User with Username and Password and No MFA**: This situation invites brute-force attacks on your cloud environment. A successful brute-force attack can grant attackers access to your cloud infrastructure, jeopardizing sensitive data and resources.
2. **Over-Permissive Access**: If a user has permissions to create other users and generate access keys, it opens the door to significant security risks. Programmatic keys should be managed carefully; they should have resource-specific access rather than wildcard permissions and always be stored securely in a secret manager or vault.
3. **Absence of Cloud Security Policies**: By allowing users to create networks that are entirely open to the internet, you make your environment vulnerable to various attacks and exploits associated with SSH and RDP. This lack of restriction exposes your cloud resources to all existing vulnerabilities.

Mitigation: Cloud Security Fundamentals

Effective mitigation starts with the basics. While embracing new technologies to secure cloud environments is essential, the mitigation techniques discussed below focus on foundational principles that can help establish a secure cloud environment.

As we've seen, breach prevention begins at the most fundamental level. Let's explore the two critical pillars and how they can fortify your cloud environment:

1. **Root or Admin Users:** In many cloud environments, the root or administrator user holds unparalleled access and should be treated as the most critical account. The credentials for this user must be securely stored in a vault or secrets manager, and Multi-Factor Authentication (MFA) should be implemented to enhance security for this account.
2. **Secure Identity and Access Management**: Although advanced access management strategies like Just-In-Time (JIT) access are now available, it's vital to focus on foundational practices. A new cloud environment should never permit human IAM users to operate solely with usernames and passwords. Instead, all human users should utilize Single Sign-On (SSO) to enhance security.
3. **Restrict Over-Permissive Permissions and Ensure Secure Access Key Management**: Users should receive access strictly based on resource-specific needs, and wildcard permissions should be avoided for all human IAM and programmatic IAM users. DevOps or cloud administrators should oversee the generation of access keys for programmatic users, ensuring access is tightly controlled, and that keys are stored securely in a secrets manager, thus eliminating hardcoding practices. It's also important to establish a process for regularly rotating keys and credentials, though that could be a topic for another discussion.
4. **Enforcing Cloud Security Policies from Day One**:

- Prohibit External Addresses: No external IP addresses should be allowed on cloud resources. Instead, create a secure, routable network accessible through a VPN.
- Control Firewall Management: Firewall rules should only be managed by designated cloud administrators. Policies must be enforced to prevent overly permissive internet access to security groups and firewall configurations.

- Disable Insecure Protocols: Protocols such as IMDSv1 should be disabled to reduce vulnerabilities.
- Prevent Accidental Exposure: Implement policies that block accidental exposure of storage objects and buckets.

In conclusion, establishing a secure cloud environment begins with a focus on fundamental principles like secure identity and access management, appropriate permissions, and strict policy enforcement. While these measures cannot guarantee complete security, they address basic issues and can prevent many attacks. By prioritizing these strategies, organizations can significantly reduce vulnerabilities and enhance their overall cloud security posture, laying the groundwork for a resilient, secure cloud infrastructure.

About the Author

Ranjan Kathuria has over nine years of experience in the security industry, where he has played a key role in developing and mentoring security engineers for recent employers. Currently, he serves as a Cloud Security Architect at a data security company, where his focus is on safeguarding the cloud environment. Additionally, he is recognized as a top-tier security researcher for HubSpot and Quora's Bug Bounty Programs on Bugcrowd, contributing to the enhancement of security measures on these platforms.

Retail Budgets at Risk: Price-Scraping and Fraudulent Bot Attacks Are on The Rise

Bots have become more sophisticated and difficult to detect. However, if retailers take a proactive role in monitoring their traffic, they can shine a light on fraudulent bots and block them from harming budgets before the damage is done.

By Chad Kinlay, CMO at TrafficGuard

Competition in the eCommerce industry is becoming increasingly rivalled. As consumers turn to online stores, more and more retailers are making the jump themselves and pivoting towards digital. Joining such a lucrative market is a no brainer for retailers. However, competition between retailers has led to the development of shady market manipulation tactics like price-scraping.

Price-scraping is a rapidly growing problem in eCommerce. Bots powered by artificial intelligence (AI) are programmed with the express purpose of harvesting data from eCommerce sites.

Businesses and Fraudsters can then use this data to undercut their legitimate competitors' prices and steal their audience. The effects of this goes beyond price undercutting, as price-scraping can impact retailers in multiple ways, from slowing website performance to skewing campaign metrics. To keep the playing field fair and prevent price-scraping bots from further damaging revenue, retailers need to act now.

Underhanded Tactics

Price-scraping is the process of using bots to extract pricing data for illegal competitive price monitoring. Bots will disguise themselves as legitimate traffic to carry out data scraping anonymously and without permission.

With online retail, price information on goods and services is common public knowledge. This has made the eCommerce industry particularly vulnerable to price-scraping, as bots have no barrier to entry.

Retailers can automatically adjust their prices based on those of their competitors by rapidly scraping data at high volumes. These bots have grown in popularity recently, with it even being possible to hire their services easily online.

Despite claims that price-scraping is harmless, it is in reality incredibly damaging to businesses. Some of the negative consequences are:

- Reduced Revenue: By undercutting prices, competitors can successfully steal target audiences. Customers will run to the competitor's online store, and revenue will rapidly decrease.
- Drained Ad Budgets: Bots significantly drain advertising campaign budgets by driving up customer acquisition costs (CACs). In the process of gathering data, these bots relentlessly click on paid campaign ads. Allocated budgets are quickly exhausted from frequent clicks, and as bots have no intent to purchase, retailers lose out on profit. Juniper Research found up to 22% of global ad spend was lost to ad fraud like this.
- Skewed Metrics: Most retailers can't distinguish between legitimate traffic and fraudulent bots. A flood of bots makes it appear a campaign is performing well, tricking retailers into optimising towards underperforming campaigns. Retailers lose out on genuine customer engagement while competitors use clean data and lower prices to gain the upper hand.

Price Scraping and Beyond: How Bots Exploit eCommerce

Bots in eCommerce have evolved far beyond simple automation, engaging in a range of deceptive and harmful practices that exploit both consumers and retailers. These malicious bots, designed for fraudulent and competitive gain, include several types that wreak havoc across online platforms:

- Reseller Bots: These bots are programmed to rapidly purchase high-demand products, such as concert tickets, limited-edition sneakers, or new electronics, before legitimate consumers can. By monopolizing stock, fraudsters resell these items at inflated prices, exploiting consumer demand

and leaving genuine buyers at a disadvantage. This practice not only scams consumers but also creates significant challenges for retailers, who may face financial losses and reputational damage.

- Data Scraping Bots: These bots infiltrate websites to extract sensitive information, such as pricing, stock levels, and SEO/keyword data. Competitors use this data to undercut prices or optimize their own strategies, undermining fair competition and eroding retailers' market positioning.
- Account Takeover Bots: Using stolen login credentials from data breaches or phishing attacks, these bots gain unauthorized access to online banking or eCommerce accounts. Once inside, fraudsters can make illicit purchases, steal personal information, or lock out legitimate users, causing significant harm to both consumers and retailers.
- Credit Card Fraud Bots: These bots exploit stolen credit card details to make fraudulent purchases on websites and payment gateways. Fraudsters use them to obtain free goods or services and to test which stolen cards remain active, leaving retailers to bear the cost of chargebacks and potential fines.
- Ad Fraud Bots: Designed to drain competitors' advertising budgets, these bots repeatedly click on rivals' online ads, artificially inflating cost-per-click (CPC) rates and lowering return on investment (ROI). This depletes marketing resources and distorts campaign performance metrics.

The impact of these bots is profound. Retailers face financial strain from chargebacks, as fraudsters often use stolen payment methods, leaving businesses to refund unauthorized transactions.

Beyond monetary losses, retailers risk fines, damaged brand reputation, and eroded consumer trust. Meanwhile, consumers are scammed into paying exorbitant prices for resold goods, suffer account breaches, or have their personal data misused. The pervasive threat of these sophisticated bots underscores the urgent need for robust cybersecurity measures in eCommerce.

Exposing Fraud

Fraudsters are deploying a range of malicious bots, including price-scrapers, reseller bots, and account takeover bots, to manipulate markets, steal data, and hinder legitimate retailers' revenue. The challenge is detecting these bots before they can scrape sensitive information, commit fraud, or harm businesses.

Fraudsters have taken advantage of bots' ability to mimic human behaviour and blend in with normal traffic to carry out large-scale attacks. However, it is possible to identify when bots are targeting your site by looking out for the tell-tale signs.

For example, abnormally high page views paired with an increased bounce rate is an indicator that bots are trying to overwhelm your site. Bots may also leave incomplete conversions and items in carts. Bots are also likely hiding behind suspicious accounts from locations your target audience wouldn't typically be based in.

By taking an active role and regularly monitoring your traffic can help to identify these potential signs of fraud. Bots can then be blocked from the site before they have the chance to steal any data. Fraud detection tools can also combat rising CACs by identifying and filtering out bot-driven clicks. These tools can detect clicks from non-human sources like bots and block them from interacting with ad campaigns to safeguard budgets.

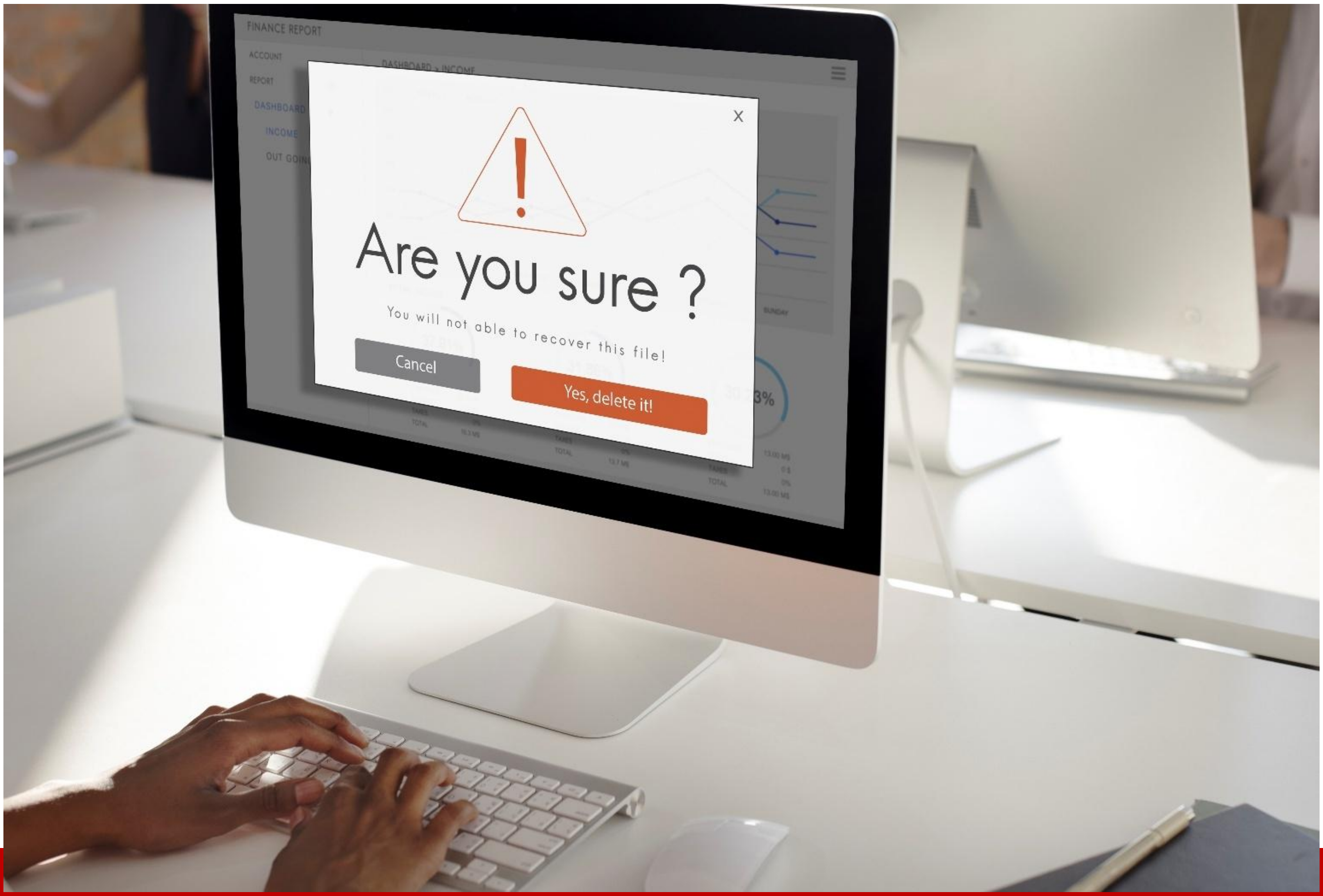
Preventing Market Manipulation

Price-scraping is a challenge that will only grow if left unchecked. In a competitive landscape like eCommerce, retailers can't afford to lose out on revenue due to devious bot activity.

Bots have become more sophisticated and difficult to detect. However, if retailers take a proactive role in monitoring their traffic, they can shine a light on fraudulent bots and block them from harming budgets before the damage is done. Legitimate retailers can then ensure they're keeping both their data and their budgets safe.

About the Author

Chad Kinlay, CMO of TrafficGuard, is a driven, open-minded, creative senior marketer with a strong sense of dedication and commitment. With over 15 years of progressive international experience in marketing and communications management, Kinlay has a credible history of commercial success. Chad can be reached at the company website https://www.trafficguard.ai



Risk Has Moved Beyond Your Inbox

From Email to Everywhere: The New Threat Landscape

By Jeremy Ventura, Field CISO, Myriad360

For years, email was the main security battleground. Phishing, scams, and account takeovers were problems companies knew how to fight—at least in theory. Secure email gateways, AI-driven detection, relentless user training. We built entire industries around stopping bad emails from reaching inboxes.

But now? Attackers don't even need your inbox. They've moved to the communication and networking platforms businesses rely on every day. Places where users trust too much and security teams think too little.

Here's the truth: The way people work has changed. Collaboration is real-time, fluid, and decentralized. But security hasn't kept up. Most organizations still defend like it's 2015, focused on email-first security strategies. Meanwhile, attackers have already adapted—phishing inside Slack, hijacking Teams credentials, running scams on LinkedIn.

The result? A massive gap in defenses. One that's being exploited right now.

The Attack Surface Has Shifted—But Defenses Haven't

We used to say email is the number one attack vector—and for a long time, that was true. But in 2024, cybercriminals don't need to start with email anymore. They go straight to where people work.

The numbers prove it:

- Proofpoint reported a 2,524% increase in URL-based threats delivered through SMS, many of which target Slack, Teams, and LinkedIn (Proofpoint).
- SlashNext saw a 703% spike in credential phishing attacks in the second half of 2024 (SlashNext).

The problem isn't just that attacks are shifting—it's that companies aren't shifting defenses to match them.

Cybersecurity has spent the last two decades hardening email. Secure email gateways (SEGs), phishing-resistant authentication, AI-powered anomaly detection—email security is battle-tested.

Slack security? Not even close.

Why Slack Is a Hacker's Playground

Slack wasn't built for security teams. It was built for speed. The entire platform is designed around fast, frictionless communication—real-time messaging, open channels, instant file-sharing.

In August 2024, researchers uncovered a vulnerability in Slack's AI feature that allowed attackers to steal data from private channels via prompt injection (PromptArmor Blog).

Slack's design philosophy makes it great for productivity—but also a dream for attackers.

1. Users Assume Slack Is a "Safe Space"

Employees treat Slack like an internal chatroom, not a security risk. They don't scrutinize messages the way they do with email.

That's a problem, because Slack isn't actually internal.

- Guest Accounts: External contractors, vendors, and even customers can be invited into channels.
- OAuth Integrations: Third-party bots and apps often have access to message history and files.
- Cross-Workspace Messaging: Slack Connect lets employees chat with users in different organizations—creating a huge blind spot for security teams.

Security teams aren't monitoring who gets invited into what channels. They're not running behavioral analysis on how files move between workspaces. And attackers know it.

2. The Disney Breach: A Case Study in Slack Exploitation

Disney didn't get hacked because of a sophisticated zero-day exploit. They got hacked because an employee unknowingly downloaded malware disguised as an AI tool, which compromised credentials and gave attackers access to Slack. The result? More than 44 million internal messages were exfiltrated and leaked publicly (Wall Street Journal).

The stolen data wasn't just random Slack conversations—it included unreleased project details, source code, login credentials, and internal APIs. Slack's structure gave attackers access without requiring further escalation.

Disney's response? They shut down Slack entirely (Business Insider).

Most companies won't go that far. But the lesson is clear: Treat Slack with the urgency of email—because attackers already do.

3. Lateral Movement Inside Slack

If an attacker gets into your email, they can phish other employees—but most phishing filters will catch it.

If an attacker gets into Slack? They can impersonate an employee in real-time, join sensitive channels, and spread malware without triggering traditional security alerts.

Slack wasn't designed with intrusion detection in mind. That's why lateral movement is so easy for attackers—once they're in, they're invisible.

Why Employees Trust These Platforms (And Why They Shouldn't)

Security training has drilled skepticism into employees when it comes to email. Hover over links. Verify senders. Assume danger.

But inside collaboration tools? That same scrutiny disappears.

Think about it—if a coworker messaged you in Slack and said, "Hey, I need your help processing this payment real quick," you'd probably do it without second-guessing. In email, you might double-check. In Slack, it feels like an internal request. That's why these attacks work.

Attackers are weaponizing trust—and it's paying off.

How Security Teams Are Catching Up

The old playbook—blocking malicious emails, filtering spam, deploying secure email gateways—isn't enough. Organizations need a security model that extends beyond email to where real work happens.

That's why the future of security is cross-platform protection.

Companies are shifting toward:

- AI-driven behavioral monitoring that detects anomalies inside Slack, Teams, and LinkedIn.
- Continuous access monitoring to flag unusual login patterns and unauthorized data movements.
- Proactive threat hunting across collaboration platforms—not just email.

The security industry is quickly evolving, with many organizations making adaptive resilience a top priority in 2025. Because companies that get ahead of this shift? They'll stop attacks before they start. The ones that don't? They'll be cleaning up breaches.

About the Author

Currently, as the Field CISO at global systems integrator Myriad360, Jeremy Ventura is a seasoned cybersecurity professional and advisor, specializing in information security best practices, driving defense strategies, and safeguarding organizations against evolving threats. With extensive experience in vulnerability management, API security, email security, incident response, and security center operations, he has honed his expertise through roles at premier security vendors and internal security teams. Follow Jeremy on LinkedIn.

Saas Security Best Practices

By Priyanka Nawalramka, Staff Software Engineer, HouseCanary

Software as a Service (SaaS) is the prevalent software distribution model in the tech industry. Whether you are a young startup founder or a mature business owner, ensuring a robust security posture within the system is crucial. Moreover, privacy regulations and compliance requirements necessitate the need for a strict approach towards security in a SaaS organization. SaaS systems typically consist of multiple components and overall system security involves many aspects. Top considerations include effective identity and access control policies, data security, monitoring, compliance and privacy policies.

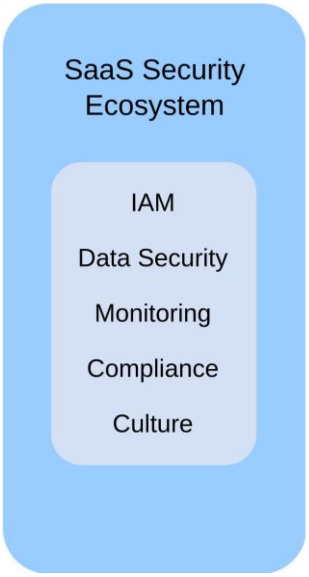
Authentication and Authorization

Authentication and authorization form the backbone of security in SaaS applications. Simply verifying a username and password via basic authentication is not enough for production systems. Enforcing a strong password policy is the minimal requirement for secure authentication. Production systems for human users should be protected via multi-factor authentication (MFA), 2-factor authentication being common practice. MFA methods have evolved and various options are available including Personal

Identification Number (PIN), possession factor methods such as SMS and email, hardware tokens and more advanced biometrics (fingerprint, face/voice recognition etc.).

Organizations often delegate authentication and authorization to a dedicated identity provider (IdP) for separation of concerns. This helps them gain a comprehensive security stance while being able to focus on business logic. Widely used protocols such as OAuth2.0 and XML based SAML facilitate secure communication between the IdP and service provider.

Authorization involves granting the authenticated user privileges within the system once they have proved their identity. Common authorization models vary from the simplest form using Access Control Lists (ACLs) to more robust forms like Role Based Access Control (RBAC) or even more granular Attribute Based Access Control (ABAC). The Zero Trust model discourages implicit trust. It operates on the “never trust, always verify” principle, requiring explicit verification of each request before granting access to resources. Access must be granted using the least privilege approach.



Data Security

Data security in SaaS applications entails guarding against data breaches (unauthorized access) and data loss prevention due to system failures. Data loss can be mitigated via frequent backups and replicating the data to multiple regions (availability zones). Regular disaster recovery tests help assess availability and data recoverability. Preventing unauthorized data access is much more nuanced. The stakes are higher when customer data is involved due to compliance. The importance of encryption in data security cannot be overstated. Encrypt your data, both in transit and at rest using industry standard encryption protocols. Furthermore, data segmentation as per sensitivity levels and client specific encryption keys can enhance the security of persisted data.

Effective authentication and authorization mechanisms prevent bad actors from accessing the data. Modern cloud-based data storage solutions often support a multitude of authentication mechanisms like password based and key-pair authentication. For automated systems, key-pair authentication, which relies on asymmetric encryption, provides enhanced security by nature of cryptography and eliminating the need to manage passwords. Some data solutions incorporate other authentication mechanisms discussed above such as OAuth, SAML and Single Sign On (SSO) making it easier to integrate data storage with Identity and Access management (IAM) solutions.

Observability and Monitoring

Maintaining awareness of what is going on in each part of a SaaS system can be challenging, however it is essential for an enhanced security posture. This goes beyond observing and reacting to system failures. Constant vulnerabilities monitoring and mitigation, threat detection and prevention, a secure deployment strategy, user session, request and network activity tracking are a part of a robust monitoring approach. Systems must be hardened against penetration and Denial of Service (DoS) attacks. Assessing third party vendors for their security posture is also necessary to maintain a healthy environment. Have an efficient alerting mechanism in place so that when anomalies are detected, remediation measures can kick off in a timely manner. Adapt a proactive versus reactive approach.

Privacy and Compliance

Regular security and compliance audits evaluate the system's overall security posture and must be at the top of the security checklist. Handling customer data requires adherence to privacy laws concerning Personally Identifiable Information (PII) and General Data Protection Regulation (GDPR) as applicable. Compliance audits measure the system against criteria such confidentiality, availability, integrity, security and privacy. Conduct the necessary audits and patch the system against issues reported in a timely manner. Undergoing compliance audits also helps the organization build trust with clients and partners as it validates the implementation of industry standard security measures and controls.

Culture

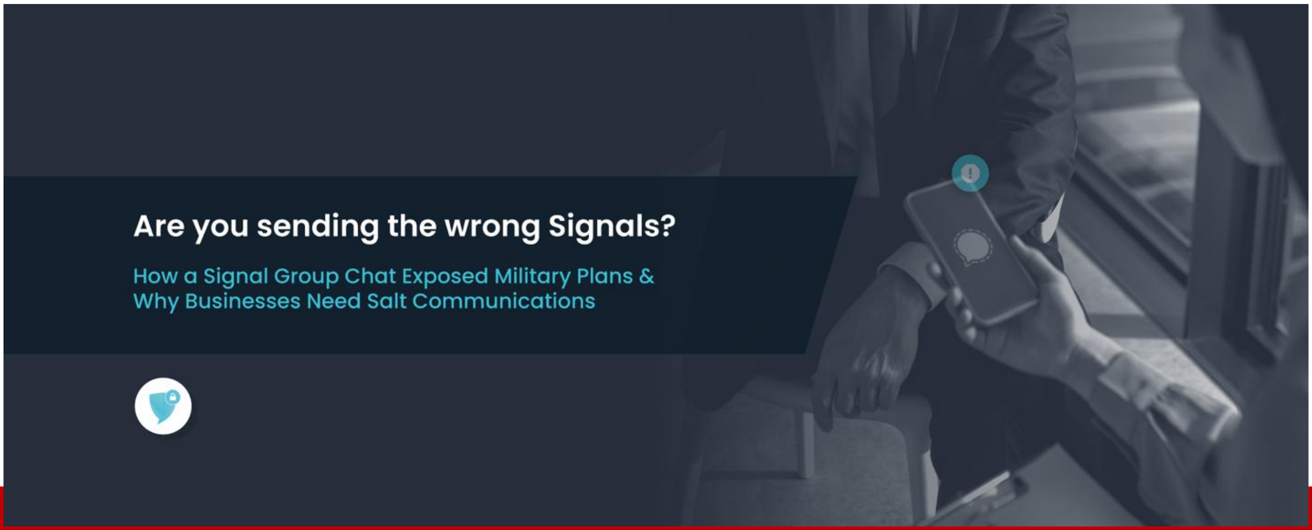
Engage employees and ensure there is awareness around compliance requirements and security best practices within the organization. Security must be cultivated as part of the organization's culture. Employees must be aware of appropriate handling of sensitive data and actions to take in times of compromise. Provide training and educational tools necessary to build that muscle.

Final Thoughts

Security in a SaaS environment is non-negotiable. Maintain a security checklist for a secure and robust SaaS ecosystem. In addition to the measures discussed above, having a solid security incident response and recovery plan is an essential step in preparation. It is not uncommon for firms to have to deal with a security breach or incident in this digital age. In addition to monetary implications, loss of reputation is a major consequence of a breach. With the help of better security posture management, stakeholders can be prepared to handle such incidents appropriately if and when the need arises.

About the Author

Priyanka Nawalramka is Staff Software Engineer of HouseCanary. She was formerly Software Engineer at JumpCloud, an identity and access management company. Priyanka specializes in identity and currently focuses on building secure data solutions at HouseCanary. She is a Senior Member of the IEEE. Priyanka can be reached online at priyanka@nawalramka.io


Are you sending the wrong Signals?
How a Signal Group Chat Exposed Military Plans & Why Businesses Need Salt Communications

Are You Sending the Wrong Signals?

How a Signal Group Chat Exposed Military Plans & Why Businesses Need Salt Communications

By Nicole Heron, Marketing Manager at Salt Communications

The Salt team has spent the last 5-10 years producing blogs, comparison documents and webinars which highlight our credentials versus consumer apps. To get the message across we frequently reference real-life issues our customers have faced - without naming the customer in order to protect their reputation. However, several recent events have done such a great job at highlighting the dangers of using consumer messaging apps for sensitive discussions that I feel like taking the rest of the week off in order to enjoy some Spring sunshine. But before I go…

On Monday 24th March 2025, the Atlantic ran a story, "The Trump administration accidentally texted me its war plans", which highlighted how The Atlantic's editor in chief, Jeffrey Goldberg, was inadvertently added to a Signal group chat by National Security Advisor, Michael Waltz. However, the inclusion of the journalist is only part of the story. The fact that they are using Signal which, just the previous week ,was being called out by Ukrainian officials as being unsupportive in helping to undermine the Russian efforts to use the Signal app to target Ukrainians involved in the ongoing war.

If you deal in sensitive information, then you or your colleagues are potentially under threat by state actors. Or, just as bad, your organisation or government could be massively undermined by group chat mishaps.

For businesses and government agencies handling sensitive information, consumer apps like Signal pose significant risks and they have chosen to carry those risks up to this point. Is this a turning point? If you're asking the question, "well what is the alternative?", then we believe we have the answer. Salt Communications provides a closed, enterprise-controlled system designed specifically to protect your data and conversations. It feels like a consumer app but it's not. It also has additional features which make you and your company more efficient in day-to-day business exchanges, or when escalating sensitive information in a hurry when managing a critical moment.

Why Consumer Messaging Apps Are Not Enough

Apps like Signal are popular for personal use, but they lack the enterprise-level security, control, and compliance features businesses need. Here's a direct comparison of the two platforms:

Salt Communications vs. Signal: A Security & Compliance Comparison

Feature	**Salt Communications**	**Signal**
System Structure	Closed system with organisational controls	Open system, anyone can be added
Security	Enterprise-grade encryption with administrative oversight	End-to-end encryption with limited controls
Data Protection	On-premise deployment & secure hosting options	Cloud-based with limited organisational control over data
User Verification	Requires organisational authentication	No verification required for users
Business-Specific Features	Secure broadcasting, live event reporting, and project tracking	Limited to personal messaging only
Accountability	Enforced identity verification within organisations	Anyone can sign up anonymously
Risk of Unauthorised Access	No external contacts unless approved	Open to any contact in user's phonebook

The Risks of Using Signal for Business

The recent security lapse highlights a major flaw of consumer apps—the lack of administrative oversight. When employees or officials use Signal, there is no way to prevent unauthorised contacts from being added, increasing the risk of accidental exposure or targeted attacks.

Consumer apps like Signal are not designed for classified environments and can be misused in ways that pose serious security risks. Without proper controls, organisations have no visibility or governance over communications, making these platforms unsuitable for handling sensitive or classified information.

For organisations that value security, compliance, and control, **Salt Communications** is the clear choice. Unlike Signal, Salt offers:

☑ **Strict access control** – Only approved contacts can communicate within your network.
☑ **Enterprise security** – Protects against zero-day vulnerabilities and cyber threats.
☑ **Data sovereignty** – Allows organisations to host data securely in-region or on-premise.
☑ **Compliance features** – Supports regulatory needs with optional message archiving.

Protect Your Communications Before It's Too Late

Don’t wait for a data breach to take action. Whether you’re in government, finance, policing, military, or any industry handling confidential data, your organisation cannot afford to rely on consumer messaging apps such as Signal.

About the Author

Nicole Heron, Marketing Manager at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company.

Nicole can be reached online at LinkedIn, X (Twitter) or by emailing nicole.heron@saltcommunications.com and at our company website https://saltcommunications.com/

SMBs Know the Risks, So Why Are Cybercriminals Still Winning?

Inside SMB Security Flaws and What Comes Next

By Kevin Pierce, Chief Product Officer at VikingCloud

Cybercriminals are no longer primarily focused on large enterprises. They now see small- and medium-sized businesses (SMBs) as prime targets because they lack the resources, expertise, and robust security measures that larger businesses can afford.

As a result, cybersecurity is now a matter of survival for SMBs. In fact, new research found that 1 in 5 SMBs could shut down for good after a cyberattack.

SMBs are beginning to grasp the severity of the threat – with 60% acknowledging they're at a heightened risk compared to their enterprise counterparts. But with 80% recognizing vulnerabilities in their current defenses, they're positioned to fall dangerously short when it comes to action. Luckily, Artificial Intelligence (AI) is emerging as a key solution for SMB protection and resilience.

Cybersecurity: A Risk Too Big to Ignore

Ask any SMB owner what keeps them up at night, and cybersecurity is near the top of the list. In fact, it ranks as the second biggest business concern among SMBs – second only to inflation and rising costs.

And for good reasons. One successful cyberattack could mean financial ruin. Over half of SMB owners report that losing $50,000 to a cyberattack would be enough to force them to close their doors for good. Many SMBs operate on razor-thin margins. Losing just $10,000, an amount that could equate to a single day of disruption, would mean “game over” for 30% of SMBs.

Despite this, a dangerous paradox exists: SMBs recognize their risk but remain unprepared.

The Gaps Leaving SMBs Exposed

Cybersecurity should be treated with the same urgency as other critical business functions like sales and marketing; however, it often receives significantly less investment and attention from many SMBs. The gaps are clear. 1 in 3 are working with outdated cybersecurity technology. 23% admit they don’t fully understand their cybersecurity risks. 26% acknowledge the person managing their cyber program lacks proper training.

And here’s the kicker – the untrained “cyber expert” managing their security posture is often the business owner themself. An alarming 74% of SMBs either self-manage their cybersecurity or rely on friends and family members, creating a dangerous expertise gap.

Beyond expertise, many SMBs are making avoidable security mistakes. Weak passwords remain a common pitfall, with nearly a quarter of businesses using easily guessed credentials like "123456," pet names, or "store staff." Others admit to never backing up their data, failing to train employees on cybersecurity best practices, missing regular software updates, or ignoring security for internet-connected devices like mobile phones.

Neglecting these fundamental protections has real consequences. Many SMBs experienced website downtime (45%), point-of-sale failures (33%), or fraudulent credit card activity (31%) over the past year. The financial impacts extend beyond the initial attack, leading to lost customers, lower sales, and lawsuits from affected clients and partners.

Cybercriminals Are Getting Smarter

On top of obvious cybersecurity gaps, cybercrime is evolving at an alarming rate – experts say cyber criminals are getting 10 to 14 minutes faster every year. SMBs are struggling to keep pace. Small businesses are twice as likely to miss a sophisticated cyberattack – such as a deepfake – compared to the more obvious disruptions like network downtime. As cybercriminals increasingly leverage AI, SMBs must be prepared to recognize and respond to new age threats.

While many have basic cyber tools like antivirus (50%), real-time threat monitoring (47%), network scanning (47%), and firewalls (44%), these alone won't keep them safe. More advanced protections – like penetration testing, endpoint monitoring, and endpoint security – are still missing from most SMB cybersecurity strategies, but they don't have to be.

The Business Case for AI: The New Era of SMB Cybersecurity

As expertise and resource gaps persist, SMBs are searching for solutions – like AI. In fact, 65% see cybersecurity as the #1 business function that could be managed more effectively with AI – ranking ahead of sales, marketing, and customer service. The same technology that gives cybercriminals an edge can also level the playing field for SMBs.

AI helps bridge the expertise gap, offering real-time threat detection and automated responses – no in-house security team required. More than half of business leaders (55%) believe AI can identify cyber threats before they disrupt operations, and nearly half (49%) say it can provide real-time response recommendations. It can also tackle the everyday security missteps that leave SMBs vulnerable, from generating strong passwords to automating software updates.

AI brings scalability that SMBs desperately need. As the volume and complexity of threats increase, AI can continuously learn, adapt, and scale protection in a way that manual processes simply can't. It empowers SMBs to move from reactive to proactive cybersecurity strategies, detecting patterns across systems and flagging anomalies before damage is done. And as AI tools become more accessible and affordable, even the smallest businesses can implement enterprise-grade protection – without breaking the bank.

The Time to Act is Now

For SMBs, cybersecurity is no longer optional. A single attack can determine a company's fate. While AI won't eliminate all risks, it can be a force multiplier, lightening the load on small teams while strengthening defenses against an increasingly sophisticated threat landscape.

The choice is clear: invest in cybersecurity now or risk everything later. The first step is understanding your current security posture. Start with a cybersecurity assessment to identify where your gaps exist. This can be done by leveraging cyber risk scores, which can quickly pinpoint your priorities. Then, take a data-driven approach to your investments, and remember: cybersecurity isn't a one-and-done exercise. Continuously monitor your environment to measure the impact of your efforts and stay ahead of emerging threats. The earlier you act, the stronger your position will be in this relentless threat landscape.

About the Author

Kevin Pierce is the Chief Product Officer of VikingCloud. He has been with VikingCloud since 2016. Kevin leads the company's global product development, service delivery, consulting, and managed security testing teams as they leverage machine learning and artificial intelligence to deliver next-generation cybersecurity. During his nearly 30 years in the technology space, Kevin designed and built highly scalable cloud systems for secure data exchange, supply chain optimization, and cybersecurity in multiple industries. He also co-founded two technology companies that each grew to hundred-million-dollar valuations prior to exit. Kevin can be reached online at https://www.linkedin.com/in/kevin-pierce-0b740a1/ and at our company website https://www.vikingcloud.com/.

The Future of API Security Reviews

Establishing Industry Expectations

By Puskhar Jaltare, Security Architect, Fastly

As organizations increasingly rely on application programming interfaces (APIs) to facilitate communication and data exchange between software systems, these “gates” become primary targets for attackers. Businesses that fail to put API security at or near the top of their priority list risk suffering costly data breaches, service interruptions, reputational damage, and more. Yet, despite the importance of API security, many organizations neglect to allocate sufficient resources for performing regular, thorough API reviews.

As a result, these organizations put their very futures in jeopardy. For example, Traceable’s State of API Security report, released earlier this year, found that 99 percent of organizations reported API security issues in the past year, and 57 percent experienced API-related data breaches. Numbers like that make it imperative for security teams to recognize the most common vulnerabilities found in today’s APIs, the obstacles to conducting thorough API security reviews, and what they can do to implement best practices to keep their internal systems and customer data safe from malicious exploitation.

Why APIs are prime attack targets

Imagine a large farm with multiple gates. It is essential for the farmer to always know the status of each gate. An open gate could lead to the loss of valuable livestock that could wander away or result in costly damage from predators that make their way onto the property. It's the same for today's organizations. Failure to maintain the security of their API gates can lead to harmful data breaches that result in financial loss, reputation damage, and operational disruption.

For instance, an API attack in April 2024 resulted in unauthorized access to 1.3 million accounts in the PandaBuy system. Another API-related attack in March 2024 targeted public GitHub repositories and extracted nearly 13 million API keys, tokens, and other secrets. Attacks like these are why The Hacker News recently reported that "organizations are losing between $94 - $186 billion annually to vulnerable or insecure APIs…."

Unfortunately, cybercriminals exploit many vulnerabilities in today's APIs. These include broken authentication and authorization, injection attacks, insecure direct object references (IDOR), insufficient rate limiting and resource consumption, security misconfigurations, insecure data transmission (lack of encryption), improper API versioning, business logic flaws, and third-party API risks.

The Quest Diagnostics API breach is an example of a third-party attack. In that incident, cybercriminals gained access to the medical information of 11.9 million Quest patients by exploiting a vulnerability in a third-party web payment page. A recent example of an injection attack is the Reddit API breach by BlackCat, where attackers exploited weaknesses in Reddit's API to obtain 80GB of data and demand a $4.5 million ransom.

How to shore up API defenses

Due to existing API weaknesses, thorough API security reviews are critical to any organization's security strategy. Without regular security assessments, vulnerabilities can go unnoticed and lead to data breaches, financial losses, and reputational damage. The keys to conducting thorough API security reviews rest largely in overcoming several obstacles that commonly arise in organizations. Those obstacles and their solutions include:

1. *Poor visibility and documentation solution.* Utilize API discovery tools and enforce documentation standards to track all API endpoints, versions, and integrations.
2. *Frequent API changes/updates solution.* Move security testing into the continuous integration and continuous delivery (CI/CD) pipeline and use automated scanning and real-time monitoring to catch issues early.
3. *Inadequate authentication and authorization review solution.* Perform consistent penetration testing and enforce strict authentication mechanisms such as open authorization (OAuth), JSON web token (JWT), and role-based access controls (RBAC).
4. *Insufficient security expertise solution.* Provide API security training, hire dedicated security professionals, and foster collaboration between development and security teams.

5. *Time and resource constraints.* Automate API security testing with tools like Open Web Application Security Project Zed Attack Proxy (OWASP ZAP), Burp Suite, or API security gateways to reduce manual effort and ensure continuous protection.
6. *Insecure third-party integrations.* Conduct security assessments of external APIs, enforce vendor security policies, and use API gateways to monitor and control third-party access.

Points.com, a platform that manages loyalty programs for major brands like Delta SkyMiles, United MileagePlus, Hilton Honors, and Marriott Bonvoy, conducted a comprehensive security review in 2023. The report identified significant API vulnerabilities that could have allowed unauthorized access to customer data and accounts. The company promptly addressed the issues and avoided a costly and reputation-damaging data breach. By committing to thorough API security reviews, organizations can proactively identify threats, enforce security best practices, and maintain a much stronger security posture.

Committing to thorough, standardized AP security reviews

To ensure consistent, high-quality reviews, it is essential for security professionals and engineers to work together to create secure, scalable, and consistent API security practices. Collaborations that are proactive, structured, and integrated into the development lifecycle provide the best results. The most effective reviews incorporate well-established frameworks, such as OWASP API Security Top 10, threat modeling (STRIDE, DREAD, or PASTA), DevSecOps practices, and secure software development lifecycle (SDLC). Up-to-date methodologies and industry standards further support these strategies.

Other best practices include maintaining an accurate API inventory and enforcing strong authentication and authorization, such as implementing OAuth 2.0, JWT, or API keys for secure authentication, and applying role-based access control (RBAC) and least privilege access to restrict sensitive data exposure. Companies can also secure data transmission by enforcing HTTPS/TLS encryption for data in transit, using end-to-end encryption for sensitive API communications, implementing rate limiting and throttling to prevent denial-of-service (DoS) attacks, and controlling excessive requests from a single source. Additional best practices are validating and sanitizing inputs to protect against injection attacks, conducting regular penetration and fuzz testing to uncover vulnerabilities, and enabling real-time monitoring to detect and quickly address abnormal behaviors.

Organizations can significantly lower the threats associated with API vulnerabilities by staying committed to API security best practices, consistently reviewing API security policies, and updating those policies and practices based on evolving threats. This comprehensive approach will reduce legal risks, protect sensitive data, and maintain customer trust by building a more secure, resilient API ecosystem that fosters growth.

Stay vigilant to maintain API security

Technology isn't going to stop advancing, and cyberattackers aren't going to stop evolving. As APIs grow in popularity, it is critical for organizations to resist complacency and continue to improve their security, which means staying on top of new trends and technology. API interfaces are likely to get significantly more complicated as organizations create new products based on advances in artificial intelligence, machine learning, and cryptocurrency technologies. The visionary companies that embrace the latest trends and technological advances and future-proof their API security strategies will best position themselves to stay ahead of evolving threats.

About the Author

Pushkar Jaltare is a security architect at Fastly with expertise in web, mobile, and cloud security assessments, threat modeling, and identity and access management. Pushkar holds a master's degree in information assurance from Northeastern University. Connect with Pushkar on LinkedIn

Telcom Security: The Intersection of Critical Infrastructure

By Trea Zemaitis, a Senior Security Engineer with Core4ce

Telecommunications service providers (TSP) are foundational to the functioning of our modern technical society, serving as the conduit through which many critical infrastructure sectors maintain communication, coordination, and control. While industrial control systems (ICS) typically operate within isolated operational networks/enclaves, some critical infrastructure sectors depend on TSPs for remote monitoring, data transmission, or secure connectivity across dispersed sites. For example, this dependency is seen in sectors such as communications, energy, water and wastewater, transportation, emergency services, and critical manufacturing. The intersection of TSP and critical infrastructure presents an attractive target for malicious actors, as weaknesses in telecommunications infrastructure can provide a conduit for the potential of disrupting, intercepting or manipulating communications as seen in many Advanced Persistent Threat (APT) campaigns.

Telecoms Increasingly Targeted by Adversaries

TSPs have become a central focus for cyber adversaries due to their dual role as both infrastructure and intelligence gateways. Groups like Sandworm in Ukraine, Salt Typhoon in the U.S and globally, and the Volt Typhoon campaign against a Guam TSP illustrate how telecoms are now critical nodes in cyber operations. Threat actors exploit telecom environments to harvest sensitive intelligence driven data and subscriber information and deploy ransomware for financial gain. Critically, they could also use this access for advanced recon and access interdependencies that lead to other sectors (e.g., energy, emergency services, or military communications). Once inside a telecom provider's environment, attackers can tap into the systems that manage how calls, messages, and data are routed (SS7/Diameter), as well as the platforms used to administer customer accounts and network operations (OSS/BSS). They may also target managed infrastructure—core routers, switches, and other network appliances—that handle internal and customer traffic. These aren't just telecom-specific systems—they're strategic assets. From here, adversaries can quietly observe, exfiltrate data, or move laterally into other connected sectors. Even if the breach is detected at the telecom level, it's possible the attacker has already pivoted into customer networks or embedded themselves in managed infrastructure, lying in wait for a future opportunity. As global tensions rise, these networks are no longer neutral infrastructure — they're contested terrain.

Cross-Sector Cyber Risk: Lessons from Modern Campaigns

Recent campaigns underscore a troubling trend that threat actors are breaching TSPs, not as an end goal, but as a gateway into broader critical infrastructure. In 2024, China-linked Salt Typhoon infiltrated major telecoms using both credential abuse and long-standing router vulnerabilities, harvesting sensitive metadata and potentially accessing systems linked to political and national security interests. Similarly, Volt Typhoon (active since at least 2021) used stealthy, "living off the land" techniques to persist inside telecom and infrastructure networks across sectors like energy, water, and transportation, embedding themselves within control systems. These operations suggest not just espionage or profit driven operations but contingency planning for future disruption. In 2023, Sandworm infiltrated Kyivstar, Ukraine's largest TSP, disrupting services for approximately 24 million users. While the headlines focused mainly on the destruction and degradation used in these campaigns end state, the many months that the adversary was embedded was likely utilized to evaluate pathways to other targets and maintain operations outside of the crippled TSP.

Looking Ahead

As the threat landscape continues to evolve, defenders must prepare for adversaries who view TSPs not as final targets, but as strategic entry points into broader ecosystems. Future campaigns will likely continue to blur the lines between sectors, exploiting trusted interconnectivity to attempt to map and move from TSPs to other critical infrastructure. Since incident response generally focuses on the direct compromise (scope, cost, authority, etc.), there is often a blind spot when it comes to assessing where attackers may have already pivoted if outside this scope. This underscores the need for integrated threat hunting and information sharing across both provider and customer environments, improved telemetry on managed infrastructure, and proactive cross-sector collaboration. Defenders must expand their scope beyond containment and eradication to consider the long game, adversary dormant periods, to disrupt the attacker's ability to nest in one sector with the goal of reaching into another.

About the Author

Trea Zemaitis, a Senior Security Engineer with Core4ce and has extensive experience in vulnerability/penetration testing assessments, computer forensics, and SOC operations. His career spans public and private sectors, consulting, and military roles, where he has led global security engagements, to include red and purple teaming. Trea also holds advanced degrees in Cybersecurity and Economics, with a focus on game theory, and has a wide range of advanced industry certifications.

The AI Threat: How Enterprises Can Defend Against the Next Generation of Attacks

By Michael Gray, CTO, Thrive

AI is transforming the way work gets done across industries. But while it improves business efficiencies, it also arms cybercriminals with highly effective tools. These bad actors use AI to power sophisticated social engineering tactics, including malware, ransomware, and convincing phishing campaigns, to trick targets into giving up personal information, compromising themselves and their organizations.

The rise of large language models (LLMs) and generative AI (GenAI) makes it extremely difficult to spot these malicious schemes when they occur. They can create communications that, at times, can be nearly indistinguishable from those written by humans. To make matters worse, these advanced campaigns are more straightforward for cybercriminals to quickly build and deploy, which is why these attacks have exploded in volume, according to McKinsey. Since the proliferation of GenAI platforms in 2022, phishing attacks have risen by 1,265%.

Bad actors have ramped up their ability to find vulnerabilities, leaving enterprises to fend off a new wave of advanced attacks. While organizations look for ways to optimize AI to work for them, they must also elevate cybersecurity practices to defend against it.

Prioritize Risk Assessments

AI systems can quickly analyze large volumes of network data to find patterns, anomalies, and weaknesses. This can either work for or against an organization. Cybersecurity criminals use the ability to identify target areas of an organization for attack campaigns.

Organizations must be one step ahead and identify these weaknesses before bad actors do. To do this, enterprises must use AI and risk assessment tools to locate and address security vulnerabilities, and they should start with a penetration (pen) test. Pen tests are often used to simulate an attack on a system to find weaknesses, which allows enterprises to map out their needs and formulate a comprehensive cybersecurity strategy. They can be conducted at any time and should be done proactively and frequently, so that no stone gets left unturned. Autonomous penetration testing, especially, can enable organizations to identify new weaknesses as they emerge so they can take proactive steps.

Put the Right Technologies in Place

Once assessments have been performed, companies must decide on the tools and processes they need to implement to mitigate risk and patch vulnerabilities. Each organization's approach will be different, but finding the right combination of technology is critical to maintaining proactive security.

Endpoint management is a critical piece of the puzzle for modern organizations. Any given organization has a slew of different endpoints to manage. From laptops to smartphones, there are a host of targets for cybercriminals to go after and for security professionals to defend. In today's world, where the mobile workforce can access sensitive business data from anywhere, endpoint management is a necessity.

The advent of AI-powered security threats puts a greater onus on IT teams to manage and lock down these endpoints to avoid breaches. Next-gen endpoint protection solutions use AI, machine learning, and behavioral analytics to continuously monitor and detect suspicious activity before it becomes a serious issue. By protecting every connected device, organizations can strengthen their broader security framework.

Enterprises should further secure their environments through multifactor authentication software and, of course, the best practice of using strong passwords. When combined, these help to fend off brute force attacks by making it increasingly difficult for cybercriminals to access login credentials. If an employee loses their mobile device, these authentication safeguards will help keep business data protected.

Take a Layered Approach to Security

In medieval times, kingdoms guarded villages with tall castle walls to keep out attackers. In case attackers had ladders to scale the walls, these kingdoms sometimes surrounded their walls with moats. To prevent attackers from crossing the moat and scaling the walls, these kingdoms had archers shoot at oncoming attackers.

Each safeguard is a different layer of security, precisely how IT teams must defend their organizations. Relying on a single line of defense is not viable against AI-powered attacks, and no single security solution can guarantee that attackers won't get through. However, a comprehensive multi-layered approach can significantly reduce the chances of a breach.

Software is one layer of security, while employee education and activity, continuous system updates, and partnerships with security experts are additional safeguard layers. Each one presents different benefits. To minimize the likelihood of an attack being successful, enterprises must invest in security training for all employees. AI makes many cyber threats more tenacious and sophisticated. For example, by educating employees on the latest ploys and tactics of AI-powered phishing attacks, employees are less likely to be fooled, making the attacks ineffective. Furthermore, training employees on what compromised website links may look like and to avoid clicking them minimizes the risk of infecting endpoints with malware.

Almost all software today has built-in security tools to ward off threats. As these attacks grow in tenacity and sophistication, software vendors release patches and updates to help defend against them. This is why organizations and employees must continuously update their software with the latest security patches.

Lastly, partnering with security experts and consultants can help fill any security gaps, whether they're around solutions, knowledge, or training. These partnerships can also be more cost-effective. Rather than buying security infrastructure or hiring a security expert to work in-house, organizations can pay for a subscription to security services and hire consultants to help them with their needs as they arise. Partnerships are a great way to boost security and resiliency and map out a strategy for specific needs and environments.

As AI-powered cyber threats continue to evolve, enterprises must adopt a more secure approach to security. Understanding where vulnerabilities lie and crafting a strategic plan to eliminate them will help protect data, revenue and reputation. By consistently conducting assessments and putting the right tools, technology and processes in place, organizations can not only get ahead of AI threats but also develop a security posture that will endure whatever the next wave of threats may be.

About the Author

Michal Gray is the CTO of Thrive. Michael has been a strong technology leader at Thrive over the past decade, contributing to the consulting, network engineering, managed services and product development groups while continually being promoted up the ladder. Michael's technology career began at Dove Consulting and later Praecis, a biotechnology startup that was acquired by a top five pharmaceutical firm in 2007. Serving in his current role, he is now responsible for Thrive's R&D, technology road-mapping vision, while also heading the security and application development practices. He is a member of several partner advisory councils and participates in many local and national technology events. Michael has a degree in Business Administration from Northeastern University, and he also maintains multiple technical certifications including Fortinet, Sonicwall, Microsoft, ITIL, Kaseya and maintains his Certified Information Systems Security Professional (CISSP).

Michael can be reached online at https://www.linkedin.com/in/michael-gray-4861663/ and at our company website https://thrivenextgen.com/.

The Future of Automotive Cybersecurity Safeguarding the Next Generation of Mobility

From electrification to autonomy, the automotive world is undergoing a technological revolution. But as vehicles become more connected, they also become more vulnerable. Automotive cybersecurity is no longer a niche concern — it's a necessity. As we step into 2025, a wave of innovations promises to redefine how we protect vehicles from digital threats. The race is on to build a future where safety is measured not just in crash tests but in cyber resilience.

By Bhushan Dhumal, Media Relations Professional, At Transparency Market Research

The Current Landscape of Automotive Cybersecurity

Modern vehicles are essentially computers on wheels. With up to 100 million lines of code and a growing number of wireless interfaces — from infotainment to vehicle-to-everything (V2X) communication — each new feature is a potential entry point for hackers. Automotive cybersecurity focuses on securing these systems from unauthorized access, data breaches, and malicious control.

Key Vulnerabilities in Connected Vehicles

The rise of electric vehicles (EVs), autonomous driving systems, and over-the-air (OTA) updates has introduced complex cybersecurity risks. Hackers can exploit weaknesses in ECUs (electronic control units), Wi-Fi and Bluetooth connections, and even tire pressure monitoring systems. Without proper defenses, cyberattacks could lead to vehicle theft, compromised safety features, or even remote hijacking.

Technologies Driving Cybersecurity Innovation in 2025

With cybersecurity fast becoming a pillar of automotive design, 2025 will be defined by the next wave of protection technologies and regulatory milestones.

AI-Driven Threat Detection

In 2025, Artificial Intelligence (AI) will take a front seat in detecting and responding to cyber threats in real time. Machine learning models will be embedded in vehicles to recognize unusual patterns, isolate threats instantly, and update defenses proactively. These systems will learn from each attack attempt — evolving continuously to stay one step ahead of bad actors.

Secure Vehicle Architecture

Automakers are shifting to a "security by design" philosophy. Centralized software-defined vehicle architectures — like zonal control and integrated domain controllers — will replace older, fragmented designs. This transition simplifies cybersecurity implementation and ensures consistent protection across all vehicle functions.

Blockchain for Data Integrity

As cars increasingly share data with each other and with infrastructure, ensuring the authenticity and immutability of that data is crucial. Blockchain technology is emerging as a powerful tool to verify data transactions, manage OTA updates securely, and prevent unauthorized code injection.

Regulatory Momentum

2025 is also expected to see a rise in global cybersecurity regulations. UNECE WP.29 mandates for cybersecurity management systems are already shaping the industry. The U.S., Europe, and Asia are following suit with stricter requirements for securing software, hardware, and vehicle communication layers. Compliance will no longer be optional — it will be the baseline for vehicle approval.

Market Outlook: Accelerating Demand for Automotive Cybersecurity

The global **automotive cybersecurity market** was valued at US$ 4.6 billion in 2023 and is projected to reach US$ 25.5 billion by 2031, growing at a CAGR of 17.2%. This surge is driven by increased connectivity, regulatory pressures, and rising public awareness of digital safety.

Cybersecurity as the Cornerstone of Autonomous and Connected Vehicles

As vehicles become smarter, more connected, and increasingly autonomous, cybersecurity is no longer a luxury — it's a critical necessity. Modern cars are now rolling computers, relying on complex networks of sensors, processors, and communication modules to perform everything from navigation to adaptive cruise control. This increasing dependence on software opens up potential vulnerabilities that malicious actors can exploit. From hijacking GPS signals to disabling brakes remotely, cyber threats in the automotive world pose risks not only to data but to lives.

With the arrival of vehicle-to-everything (V2X) communication — where cars interact with infrastructure, pedestrians, and each other — the need for secure communication channels has never been more pressing. Hackers gaining access to these systems could create large-scale traffic disruptions or worse, endanger public safety. That's why leading automotive manufacturers and cybersecurity firms are working hand-in-hand to create advanced encryption protocols, intrusion detection systems, and over-the-air (OTA) updates that keep vehicles secure and adaptive.

Artificial Intelligence (AI) is also playing a pivotal role. Predictive threat intelligence systems powered by AI can identify unusual patterns in vehicle behavior and take preemptive action to stop attacks before they occur. In the near future, cars will need to be equipped not only with smart features but also with smart defenses — ones that evolve with the threats they face.

Impact Across Key Sectors

- **Autonomous and Electric Vehicles**

Self-driving cars and EVs rely heavily on software and connectivity. In 2025, cybersecurity will be essential for ensuring public trust in these technologies. Enhanced protection mechanisms will guard against system manipulation, unauthorized data access, and energy management sabotage.

- **Fleet Management and Logistics**

Commercial vehicle fleets — especially those relying on real-time route optimization — will benefit from encrypted communication channels and endpoint protection to prevent hacking attempts that could disrupt supply chains or compromise sensitive data.

- **Insurance and Risk Assessment**

Automotive insurers are beginning to factor in cybersecurity readiness when determining policy rates. In 2025, telematics-based systems will not only track driving behavior but also assess vehicle vulnerability, creating a new dimension of digital risk profiling.

Challenges on the Road Ahead

While progress is rapid, hurdles remain.

- Legacy Systems: Older vehicles and infrastructure lack the capability to support modern cybersecurity solutions.
- Cost & Complexity: Implementing robust, multi-layered cybersecurity in mass-market vehicles without inflating costs remains a balancing act.
- Talent Shortage: The need for skilled automotive cybersecurity professionals is growing faster than the talent pool.

Future Outlook

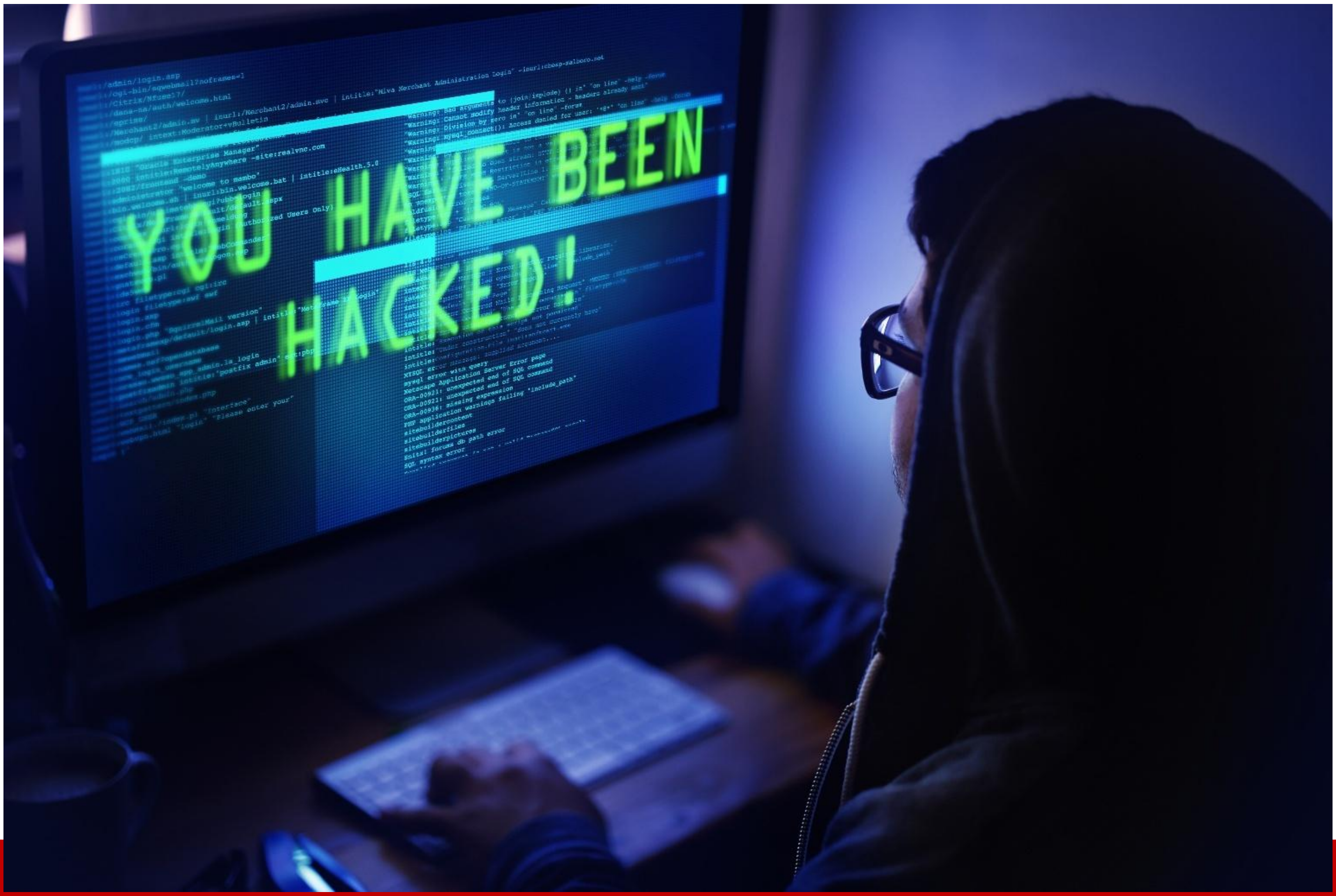
As vehicles evolve into connected digital ecosystems, cybersecurity must evolve with them. By 2025, AI, blockchain, and secure architecture will form the foundation of cyber-resilient mobility. The automotive world is entering a phase where protecting software is as critical as designing strong engines. With innovation and regulation converging, the future of automotive cybersecurity is not just secure — it's smarter, adaptive, and indispensable.

This information is sourced from the Automotive Cybersecurity Market analysis by Transparency Market Research.

About the Author

I'm Bhushan Dhumal, a passionate media relations professional specializing in the automotive security sector. At Transparency Market Research, I focus on turning complex research and technical advancements into impactful stories that resonate with global audiences. With a strong grasp of cybersecurity trends and automotive innovation, I aim to bridge the gap between in-depth market insights and strategic media outreach. My goal is to ensure that developments in automotive cybersecurity are not only understood but also appreciated for their significance in shaping the future of mobility. Let's connect and explore the evolving world of automotive security together.

EMAIL-Bhushan.Dhumal@transparencymarketresearch.com
Web- https://www.transparencymarketresearch.com/



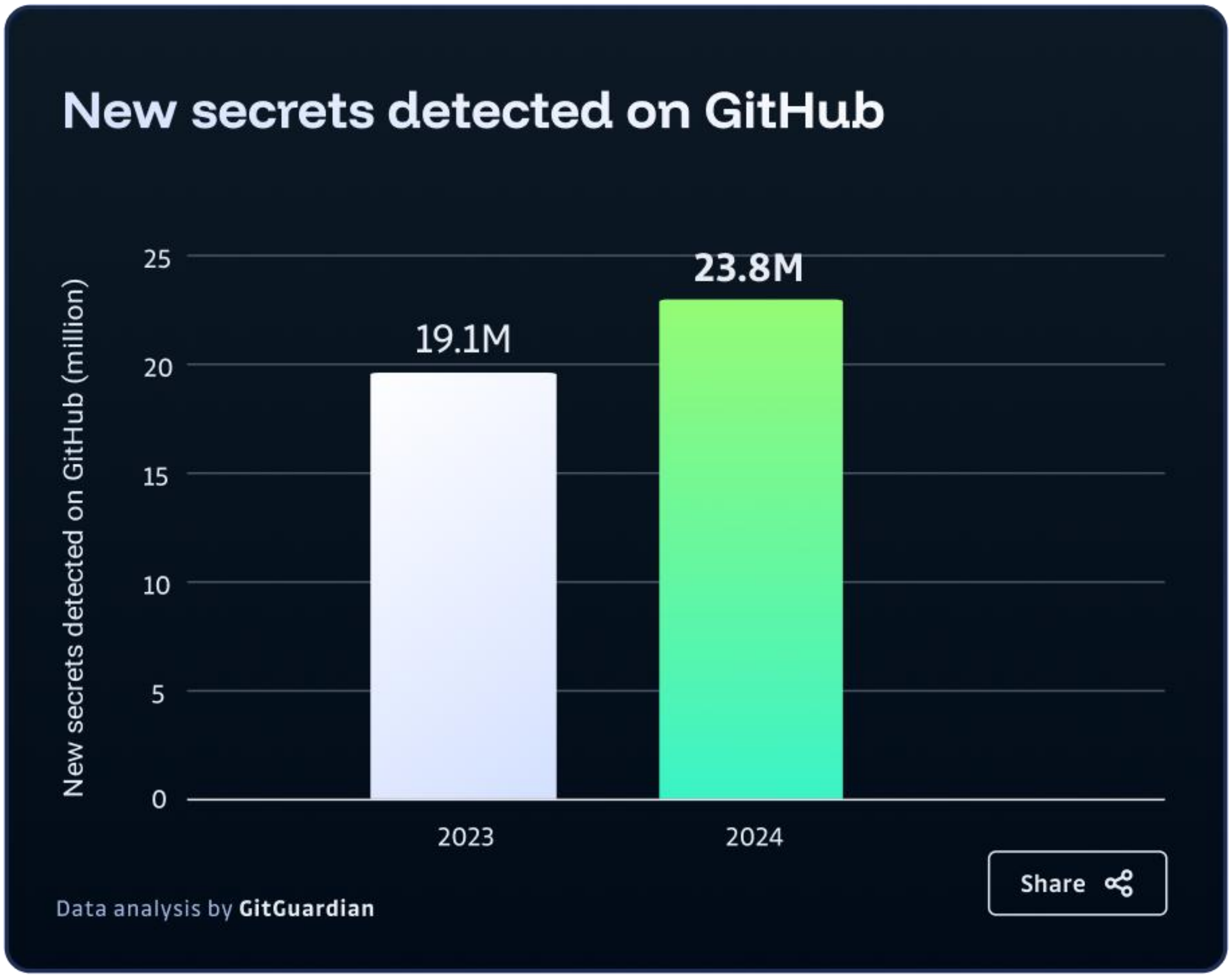
The Hidden Danger: Secrets Sprawl Beyond the Codebase

By Dwayne McDaniel - Sr. Developer Advocate at GitGuardian

GitGuardian's 2025 State of Secrets Sprawl Report reveals an alarming expansion of credential exposure across enterprise environments, with collaboration tools emerging as a critical yet overlooked vulnerability.

Secrets Sprawl Reaches Record Levels

The cybersecurity landscape continues to face mounting challenges as GitGuardian's latest research shows a 25% surge in exposed credentials across developer environments. In 2024 alone, nearly 24 million new hardcoded secrets were detected in public GitHub commits, continuing a disturbing upward trend in secrets sprawl.



Collaboration Tools: The New Frontier of Credential Exposure

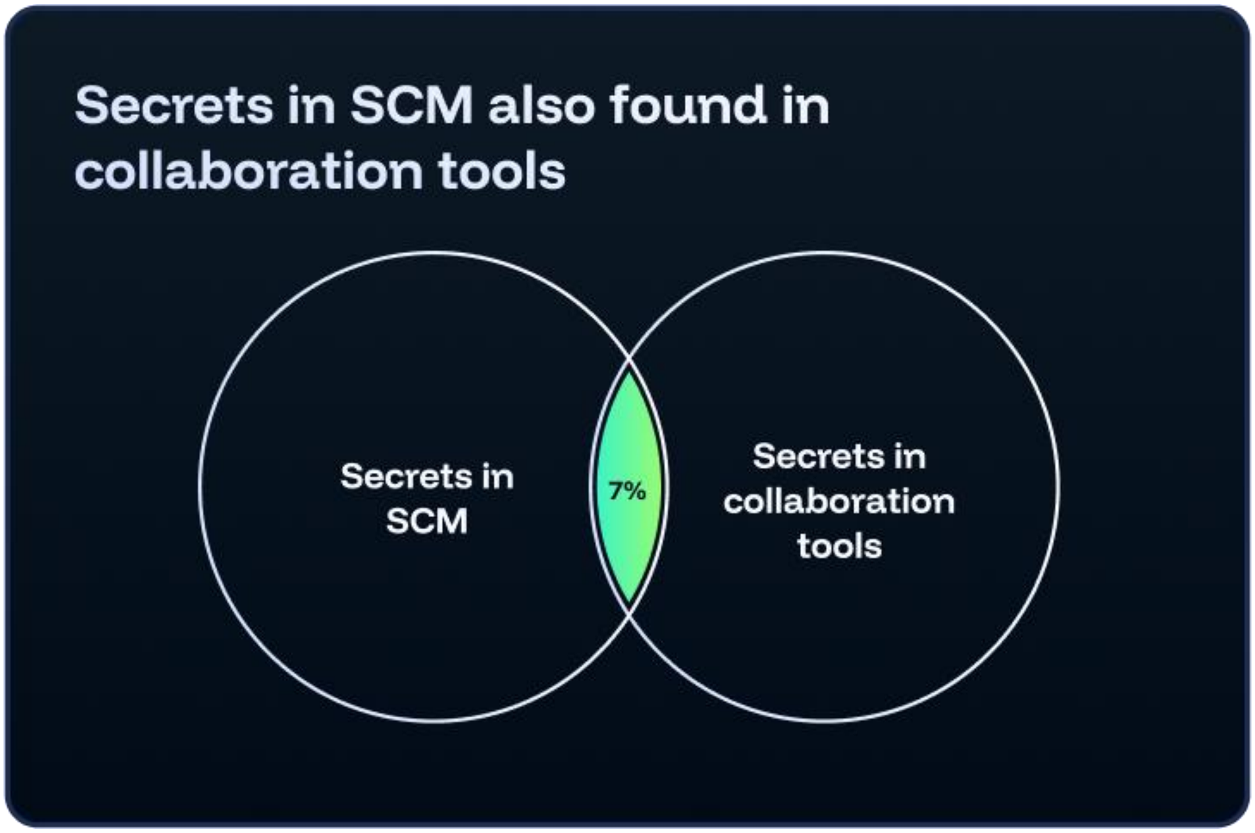
While source code repositories have traditionally been the focus of secrets detection efforts, GitGuardian's research reveals that collaboration and project management tools now represent an equally dangerous—and largely unmonitored—attack surface for organizations.

According to the report, platforms like Slack, Jira, and Confluence have become high-risk zones for leaked credentials. More concerning still, these leaks aren't just more common—they're more severe.

"38% of incidents in collaboration and project management tools were classified as highly critical or urgent, compared to 31% in Source Code Management Systems," the report states. This higher criticality stems from several factors:

- Developers tend to be less cautious with secrets outside of code repositories
- Unlike SCM systems, collaboration tools lack built-in security controls like pre-commit checks
- Less security-aware employees frequently handle sensitive credentials in these tools

Perhaps most alarming is that these credential exposures represent an almost entirely new attack surface. The report found that only 7% of secrets appear in both SCM and collaboration tools—meaning organizations focusing solely on code scanning are missing 93% of the credentials exposed in collaboration platforms.



The Unique Risks of Different Collaboration Platforms

Each collaboration tool presents its own unique risk profile:

Messaging Platforms

Slack channels show a 2.4% leak rate across all channels analyzed, with approximately 1,500 channels per workspace in the average enterprise. The informal, real-time nature of these platforms makes them particularly vulnerable to casual sharing of credentials during troubleshooting or emergencies.

Ticketing Systems

Jira presents the highest leak rate at 6.1% of tickets containing at least one secret. With the average customer managing 150 projects, this creates numerous opportunities for credential exposure. Tickets often contain logs or configuration snippets with embedded authentication details that remain searchable indefinitely.

Documentation Platforms

While Confluence showed a lower leak rate at 0.5% of spaces, the persistent nature of wiki documentation means these exposed credentials often remain in place for years. Architecture diagrams, onboarding guides, and configuration documentation frequently contain hardcoded credentials "for convenience."

Why Collaboration Tools Pose Such a Significant Threat

Several factors make collaboration tools particularly dangerous for secrets sprawl:

1. Design limitations: Unlike code repositories, these platforms prioritize speed and collaboration over security, with no native secrets scanning or prevention capabilities.
2. Widespread access: While code access might be limited to engineers, collaboration tools are used by diverse team members from support staff to executives, many without security training.
3. False sense of security: The report found private repositories are 8 times more likely to contain secrets than public ones—suggesting users behave more carelessly in "private" spaces, incorrectly assuming that access restrictions equal security.
4. No effective lifecycle management: Once posted in a chat, ticket, or document, secrets often remain indefinitely without systematic review or rotation.
5. Difficult monitoring: The high message volume in these platforms makes real-time protection challenging, with Slack alone averaging thousands of messages daily in active workspaces.

The Impact of AI on Secrets Sprawl

The report also highlights another concerning trend: AI coding assistants may be worsening security practices. Repositories using GitHub Copilot showed a 40% higher incidence of secret leakage compared to the average. This suggests that as teams embrace AI for productivity gains, security practices may be suffering.

"This disparity can be attributed to two factors," notes the report. "First, the code generated by Large Language Models may inherently be less secure. Second, and perhaps more significantly, the use of coding assistants may be pushing developers to prioritize productivity over code quality and security."

Addressing the Full Spectrum of Secrets Sprawl

Effective secrets management requires a comprehensive approach that extends beyond code scanning. Organizations need to adopt a multi-faceted approach to combat secrets sprawl by deploying real-time detection mechanisms across all collaboration platforms while implementing robust validation systems that prioritize critical exposures.

Simultaneously, they should automate remediation workflows to drastically reduce the window between detection and resolution, and invest in comprehensive training programs that educate all team members—not just developers—on secure credential handling practices. Finally, organizations must consolidate their incident management processes to ensure that identical leaked credentials appearing across different platforms are treated as a single security event requiring coordinated response, rather than as isolated incidents that might receive inconsistent attention.

As the report concludes, "Secret leaks rarely remain isolated incidents. Instead, they typically serve as entry points for sophisticated attack chains that can compromise entire organizations and their supply chains. This reality demands a shift from simple secret detection to comprehensive secret lifecycle management and rapid incident response capabilities."

Organizations that fail to extend their secrets detection beyond code repositories are addressing only a fraction of their actual risk surface, leaving critical credentials exposed in the very tools their teams use most frequently.

About the Author

Dwayne McDaniel, Senior Developer Advocate at GitGuardian.Dwayne has been working as a Developer Advocate since 2014 and has been involved in tech communities since 2005. His entire mission is to “help people figure stuff out.” He loves sharing his knowledge, and he has done so by giving talks at hundreds of events worldwide. He has been fortunate enough to speak at institutions like MIT and Stanford and internationally in Paris and Iceland. Dwayne currently lives in Chicago.

Dwayne can be reached online at and at our company website http://www.gitguardian.com/

The Impact of Cloud computing in 2025

Cloud Computing Impact in 2025: Trends, Benefits

By Ashish Kumar, Founder and CEO, Teleglobal International

Key Trends Driving Cloud Computing in 2025

1. Smarter Cloud Tools with AI

Artificial Intelligence (AI) and Machine Learning (ML) have become embedded into core cloud offerings. In fact, A Gartner report suggests 87% of organizations will adopt AI by 2025, often via cloud platforms. These capabilities are not limited to automation, they're improving real-time analytics, enhancing customer experiences, and even strengthening cybersecurity.

Cloud-native AI services now help companies detect anomalies, predict user behavior, and make data-driven decisions at scale. Cloud-powered AI is solving real-world problems from fraud detection to predicting what customers will want next.

2. Faster Data Processing with Edge Computing

As more data is generated outside traditional data centers, through IoT devices, smart factories, and autonomous systems, edge computing is rising fast. Research Nester projects that the edge computing industry will grow to $26.6 billion by 2025.

With edge computing, businesses are cutting down lag, processing data on-site, and powering real-time apps more effectively. Cloud providers now offer hybrid edge-cloud solutions that allow businesses to combine central compute power with distributed data processing, enhancing both performance and resilience.

3. Hybrid and Multi-Cloud Becomes the Norm

No single cloud fits every need. That's why over 85% of businesses are expected to adopt a hybrid or multi-cloud strategy in 2025. Companies want the flexibility to run applications across public clouds, private clouds, and on-prem environments, without sacrificing control or performance.

This shift has led to the growth of unified cloud management tools and policy frameworks, enabling organizations to optimize cost, performance, and governance across diverse platforms.

4. Cloud Solutions That Are Better for the Planet

Environmental concerns are influencing IT decision-making. Leading cloud companies like AWS, Google Cloud, and Microsoft Azure are going green by aiming for carbon neutrality and switching to renewable energy sources. Businesses are also becoming more mindful of their own cloud carbon footprints.

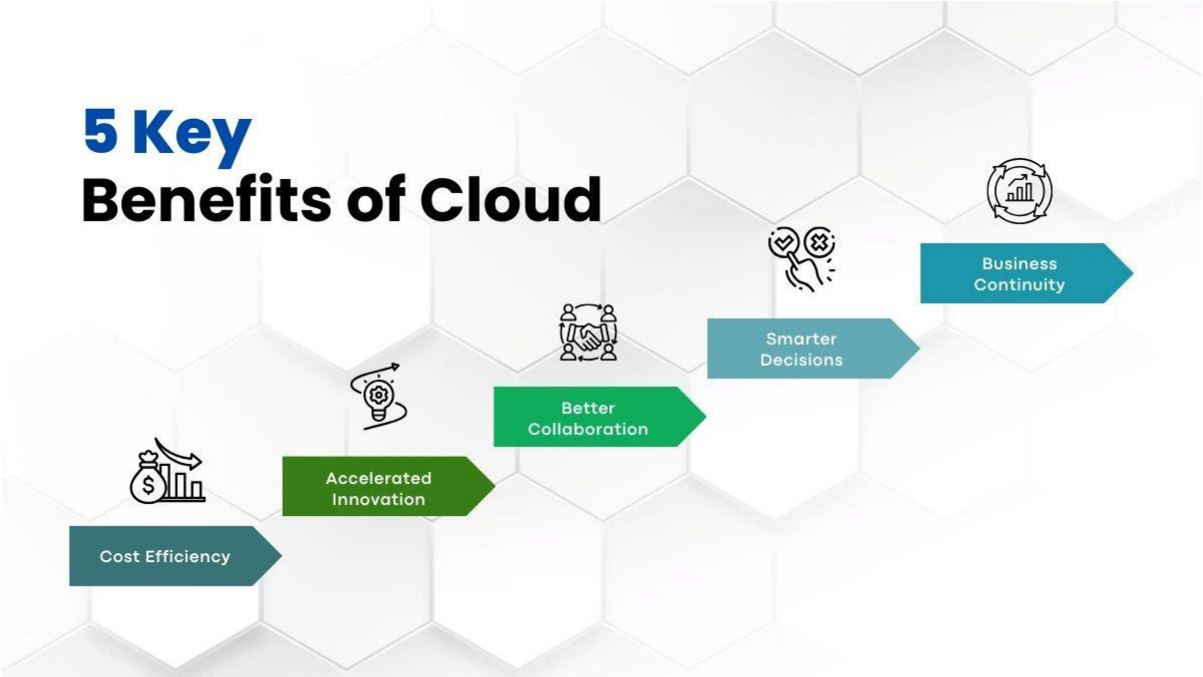
Cloud sustainability now goes beyond marketing, it's about operational efficiency, smarter resource allocation, and environmental responsibility. Choosing greener regions, optimizing workloads, and tracking energy usage are all part of cloud strategy in 2025.

5. Better Security Built Into the Cloud

As cloud usage deepens, security remains a critical, if quieter theme. In 2025, businesses are no longer bolting on security; they're designing with it from the start. With cybersecurity spending on cloud infrastructure projected to surpass $100 billion, companies are leaning into integrated tools for access control, encryption, and continuous monitoring.

Zero Trust frameworks, identity-first security, and compliance automation have become default expectations across industries, not just in regulated sectors.

Unlocking Business Value with Cloud in 2025: 5 Key Benefits



1. Cost Efficiency with Intelligent Scaling

Cloud computing reduces infrastructure costs by up to 30% for some enterprises, according to industry reports. But more importantly, businesses now use cloud elasticity to match resources precisely with demand, eliminating overprovisioning and controlling waste.

Advanced cost optimization tools help organizations monitor usage patterns, right-size deployments, and make smart decisions in real time.

2. Accelerated Innovation and Product Development

Being fast to market has become a crucial factor for staying competitive. With serverless computing, containerization, and microservices, cloud platforms enable faster development cycles and quicker iteration. Businesses can deploy new features or applications in days, not months.

In 2025, innovation doesn't just happen in the R&D department, it's baked into the cloud infrastructure.

3. Better Collaboration and Remote Work Support

Cloud-based collaboration tools are essential in supporting the modern workforce. Over 90% of businesses rely on cloud-based services, including platforms like Microsoft Teams, Google Workspace, and cloud-hosted ERPs, according to industry reports.

Cloud identity services and real-time synchronization keep remote teams connected without sacrificing productivity or data integrity.

4. Smarter Decisions Through Cloud Analytics

From marketing insights to operational forecasting, businesses are making smarter decisions thanks to powerful cloud-based analytics platforms. Real-time dashboards, AI-driven recommendations, and scalable data warehouses allow companies to turn data into actionable intelligence, no matter the volume or velocity.

This capability is especially valuable in sectors like finance, healthcare, and logistics, where timely insights drive mission-critical outcomes.

5. Business Continuity and Compliance Built-In

Cloud computing has revolutionized disaster recovery. Organizations can now replicate critical systems across geographies, ensuring high availability and quick recovery. Downtime, whether caused by technical failure or cyber incidents can be minimized with automated failover and backup systems.

Compliance is also more manageable with cloud-native frameworks offering pre-built controls and audit support. From HIPAA to ISO 27001, regulatory requirements are easier to meet when security and compliance are part of the infrastructure itself.

Future-Ready: Why Cloud Matters More Than Ever

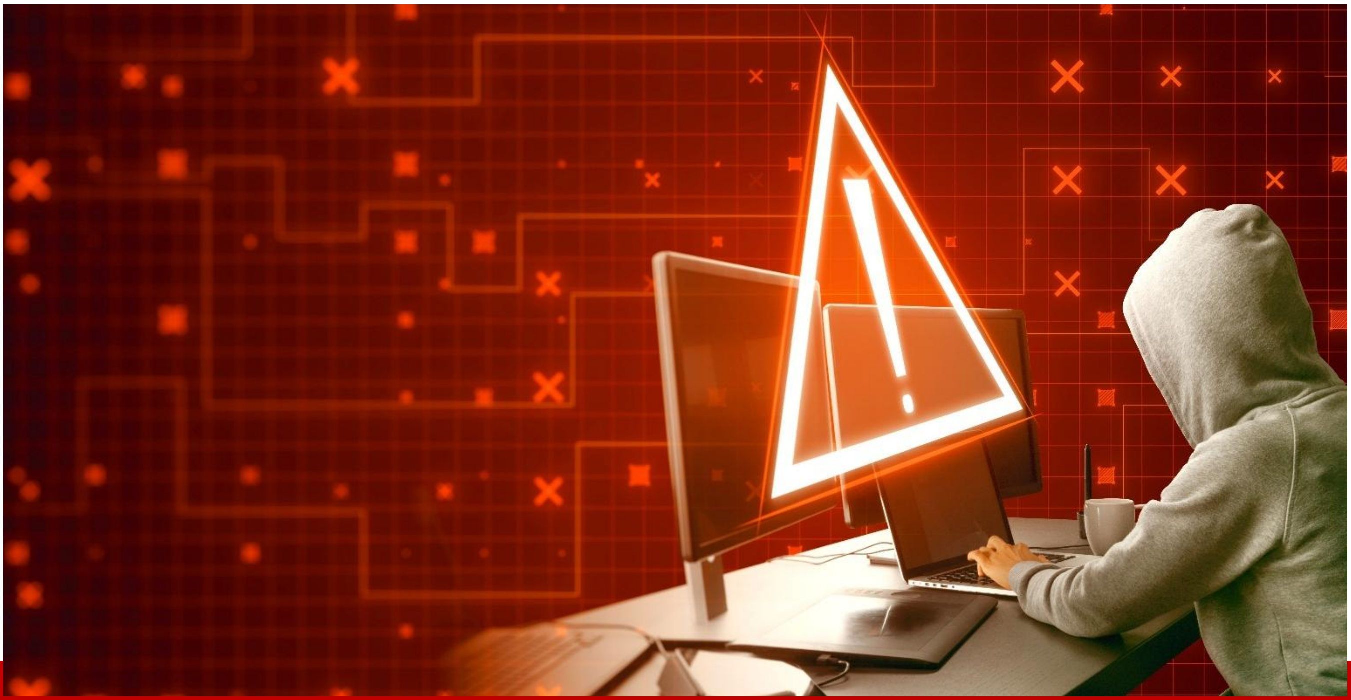
In 2025, business strategy and technology aren't separate tracks—they meet at a digital junction powered by the cloud. Cloud computing is no longer a competitive edge, but a core driver of resilience, innovation, and growth. It supports everything from digital transformation to global expansion, enabling businesses to operate faster, smarter, and more securely.

Enterprises that embrace evolving trends like AI integration, edge computing, hybrid deployments, and responsible cloud usage will not just stay competitive, they'll set the pace for the industries they're in.

Is your organization ready to board the cloud train, or risk being left at the station?

About the Author

Ashish Kumar is the Founder and CEO of TeleGlobal, a forward-thinking IT solutions provider specializing in cloud modernization, Generative AI, and machine learning-driven innovations. With over a decade of experience in enterprise IT and digital transformation, Ashish is passionate about helping businesses leverage technology for scalable growth. Under his leadership, TeleGlobal has emerged as a trusted partner for cloud-native strategies, modernization roadmaps, and AI integration. He regularly shares insights on digital strategy, cloud architecture, and the evolving landscape of intelligent automation. https://teleglobals.com



The Inevitable AI Breach? Predicting Data Theft Through Shared Vulnerabilities

Exploring the Looming Threat of Widespread AI System Exploitation.

By Yashin Manraj, CEO — Pvotal Technologies

Statistics shared by the World Economic Forum in 2024 show healthcare and finance to be the top two industries most targeted by cybercriminals. The data held by companies in those industries is not only very sensitive but also extremely valuable to hackers.

However, recent trends suggest that cybercriminals may be adding some new targets to their hit list. The widespread adoption of artificial intelligence in virtually every industry has caused many companies to begin collecting valuable data on consumers and their behavior.

The evolution of attacks on AI

Data-focused cyber attacks typically seek to steal or encrypt data to demand a ransom for its release. Attacks on AI systems, however, typically have the goal of data poisoning, which seeks to compromise the performance of an AI model by corrupting it with fake or biased data.

Data theft is not as common with AI systems because they typically contain generic data used for training. It's data scraped from the internet or other public datasets that is used to help AI models develop an understanding of general patterns.

As models are deployed, however, they can begin to gather specific user data to fine-tune their response capabilities. AI used by e-commerce marketplaces to identify users' spending trends, for example, incorporates sensitive personal information into AI databases to drive a more personalized experience.

The enhanced databases that AI systems build as they are deployed have the potential to be very desirable to cybercriminals. They also have the potential to be more vulnerable than traditional business databases because companies have had less time to understand their attack vectors and develop effective defenses.

The danger of shared vulnerabilities

When a security vulnerability is discovered in a widely shared system, it can quickly lead to a string of breaches. Cybercriminals put extra effort into identifying such shared vulnerabilities because it increases their efficiency, allowing them to strike effectively at multiple targets once a single weakness is discovered.

There is a high potential for shared vulnerabilities involving AI-powered tools because of the way they are currently developed and deployed. Most companies rely on pre-trained AI models that are widely available. A popular model can be adopted and integrated into the operations of companies of varying sizes across a broad range of industries.

The use of open-source components, which is common in AI development, further increases the risk of shared vulnerabilities. If one of those components is compromised, it can become a vulnerability in countless systems.

Shared vulnerabilities can also exist in the third-party infrastructure used to store data collected by AI systems. Companies using cloud storage, for example, become reliant on cloud providers to keep their customers' personal data secure. A singular weakness in a cloud system could be used to gain access to all of the customer data stored in that system.

The steps needed to address shared vulnerabilities

As the growth of AI continues to enhance business capabilities, it also enhances the cybersecurity threat landscape. To avoid data breaches, companies must understand that embracing AI also requires embracing an elevated security response.

The best strategy for staying secure is focusing on reducing attack vectors. Defending each possible point of entry becomes overwhelming as the potential for shared vulnerabilities increases. Relying on identification or assessment libraries won't provide the protection needed in a landscape that is rapidly evolving, along with the rapid advancement of AI.

Leveraging a zero-trust approach provides a framework for detecting and preventing emerging threats. By assuming that a breach has already occurred, zero-trust significantly reduces the advantage cybercriminals gain from shared vulnerabilities.

Network segmentation can also prevent shared vulnerabilities from creating widespread damage. Isolating the applications that source AI databases through micro-segmentation keeps their vulnerabilities from opening a door to data breaches.

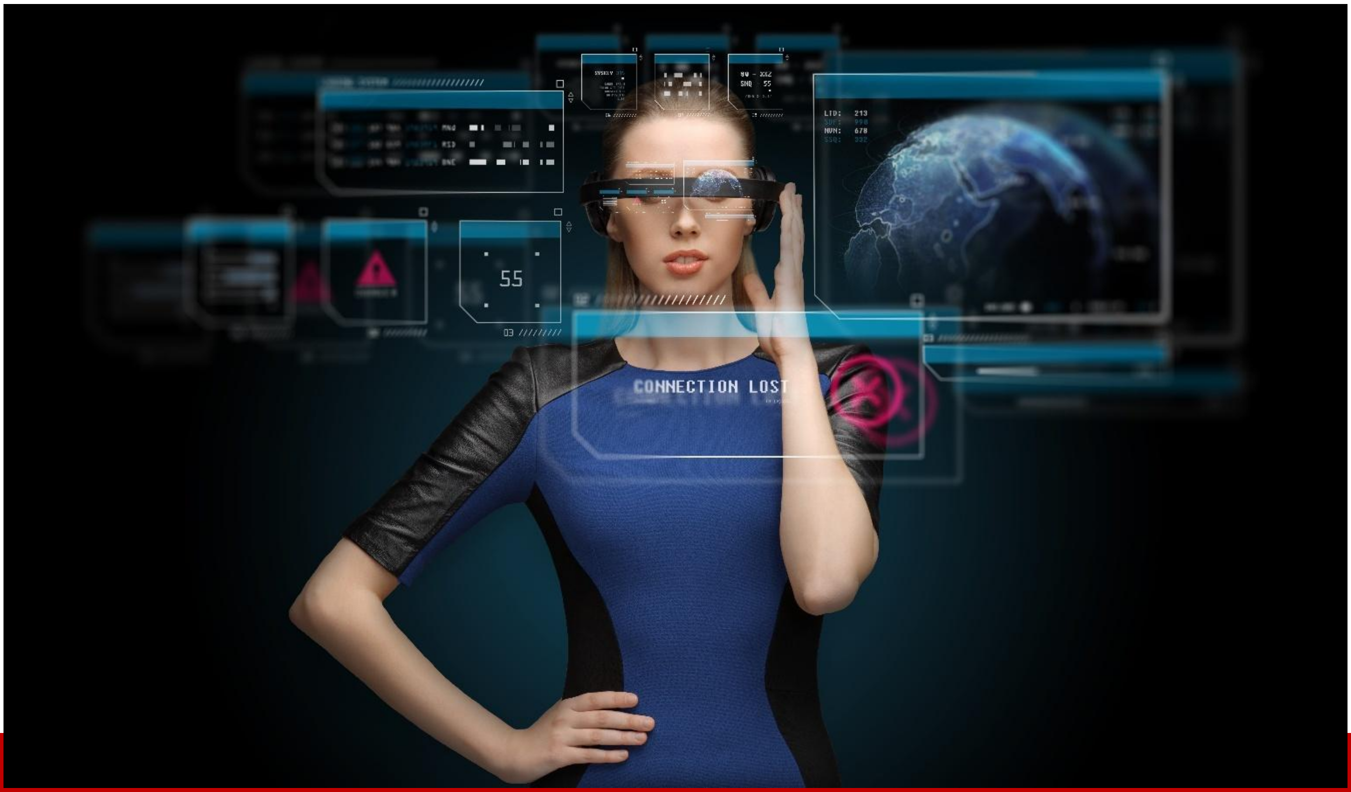
Shared vulnerabilities amplify the damage cybercriminals are able to inflict, creating a domino effect that can topple a wide range of companies. The widespread use of pre-trained models and third-party providers has introduced the threat of those vulnerabilities into the AI space. While a breach may be inevitable, companies that are proactive in adopting targeted security controls can limit their exposure while still benefiting from the advantages of AI.

– Yashin Manraj, CEO of Pvotal Technologies, has served as a computational chemist in academia, an engineer working on novel challenges at the nanoscale, and a thought leader building more secure systems at the world's best engineering firms. His deep technical knowledge from product development, design, business insights, and coding provides a unique nexus to identify and solve gaps in the product pipeline. The Pvotal mission is to build sophisticated enterprises with no limits that are built for rapid change, seamless communication, top-notch security, and scalability to infinity. Pivotal's products and services create Infinite Enterprises that give business leaders total control and peace of mind over their technology systems and their businesses End of article.

About the Author

My Name is Yashin Manraj, CEO of Pvotal Technologies. Manraj has served as a computational chemist in academia, an engineer working on novel challenges at the nanoscale, and a thought leader building more secure systems at the world's best engineering firms. His deep technical knowledge from product development, design, business insights, and coding provides a unique nexus to identify and solve gaps in the product pipeline. The Pvotal mission is to build sophisticated enterprises with no limits that are built for rapid change, seamless communication, top-notch security, and scalability to infinity. Pivotal's products and services create Infinite Enterprises that give business leaders total control and peace of mind over their technology systems and their businesses.

Yashin Manraj can be reached online at yashin.manraj@pvotal.tech and at our company website https://pvotal.tech/



The Limitations of Agentic AI in Cybersecurity: Why Large-Scale Autonomous Cyberattacks Aren’t Yet a Reality

By Dan Schiappa, President of Technology and Services, Arctic Wolf

There are a few universal rules that apply in the ongoing cybersecurity arms race between attackers and security companies.

The first, and most important rule, is that technological evolution that boosts the ability of threat actors to execute their attacks also enhances the effectiveness of cybersecurity tools. Looking at the last three years of AI and machine learning development is proof of this, because as attackers leverage AI to create new methods to infiltrate and exploit their targets, those same models are making threat detection and prevention more efficient than ever.

Agentic AI, or autonomous AI, is widely considered the next frontier in cybersecurity for its ability to enable tools that adapt, learn and execute on their own, absent any human input or intervention. But despite its promise, there are critical challenges that must be overcome before Agentic AI can perform large-scale, fully autonomous cyberattacks, or serve as the basis of a fully autonomous Security Operations Center.

Here’s why. Virtually every business, whether it has 10 or 10,000 employees, requires a certain level of cybersecurity resilience in 2025, because cyber risk is synonymous with business risk. That being said, each organization’s IT infrastructure is vastly different, from the size of their attack surface to the specifical tools, configurations and security controls they use. For an adversary to leverage agentic AI to successfully attack these specific security environments would require that the AI have intimate knowledge of those environments, which is a tall task for threat actors to accomplish with their AI model.

Right now, AI models are not sophisticated enough to carry out precision-targeted attacks at scale without human oversight. It is possible that agentic AI could enable attackers to one day launch ransomware-as-a-service attacks without the need for a service provider, but for now, many AI-driven attacks today are unsophisticated, relying on the “spray and pray” approach—launching broad, untargeted campaigns in hopes of finding vulnerabilities. These kinds of attacks aren’t going anywhere soon, and threat actors will likely only leverage agentic AI to automate social engineering campaigns or scan networks for vulnerabilities in the near future. It’s also not far-fetched to imagine agentic AI enhancing attacks based on image or voice-cloning that are meant to fool the target into believing they’re talking to a real organization or individual.

The good news is that agentic AI is poised to follow the aforementioned rule of technological advancement in cybersecurity; what’s good for attackers is also good for defenses. Agentic AI will be used to enhance threat hunting, augmenting the ability of security analysts by allowing them to focus on triaging only the most pressing threats. We’re likely to see agentic AI used by security vendors in relatively specific scenarios like unearthing bank fraud, government fraud or other limited cases. That’s because the most effective implementation of agentic AI for security professionals is in using it to find Indicators of Compromise (IOCs) quickly and efficiently.

We are far from being able to automate entire Security Operations Centers (SOCs), with agentic AI, however, primarily because of the sheer amount of high-quality data necessary to train an AI model to run an entire SOC by itself. Humans will still be necessary “in the loop” of triaging security incidents and offering creativity in defending against cyber attacks for some time, as poor training data could create an overwhelming number of false positives that mitigates the effectiveness of a fully autonomous SOC.

Ultimately, while the hype surrounding Agentic AI is understandable, the reality is that we are still in the early stages of its deployment. AI-driven cyberattacks are likely to remain unsophisticated for the time being, but as the technology matures, the stakes will continue to rise. Organizations must stay vigilant, invest in both AI-driven defense tools and human expertise, and prepare for a future where the barriers to large-scale cyberattacks continue to decrease.

About the Author

Dan Schiappa is President, Technology & Services at Arctic Wolf. In this role, Dan is responsible for driving innovation across product, engineering, security services, alliances, and business development teams to help meet demand for security operations through Arctic Wolf's growing customer base. Before joining Arctic Wolf, Dan Schiappa was CPO with Sophos. Previously, Dan served as Senior Vice President and General Manager of the Identity and Data Protection Group at RSA, the Security Division of EMC. He has also held several GM positions at Microsoft Corporation, including Windows security, Microsoft Passport/Live ID, and Mobile Services. Prior to Microsoft, Dan was the CEO of Vingage Corporation.

Dan can be reached at https://www.linkedin.com/in/daniel-schiappa-bbb1062/

The Looming Domino Effect of Cyberattacks on Energy and Utilities

By Kory Daniels, CISO, Trustwave

When systems go dark and become unavailable, consumers and operators may feel frustration, panic, and anger. When there is disruption to energy and utilities that affects homes, businesses, and entire geographical regions, that darkness will spur emotional and logistical problems that bring processes to a halt. The CrowdStrike outage caused chaos at airports and other facilities—now, imagine the cascading consequences if every airport, phone network, hospital, and emergency dispatch center went dark.

Energy and utilities are propelling modern civilization into the future and are a unique part of the micro and macro supply chain that includes billions of people, Fortune 500 global enterprises, and everything in between. When the power grid fails, hospitals lose life-saving equipment, supply chains collapse, and transportation screeches to a standstill.

The risks extend to all critical infrastructure. Military bases, intelligence agencies, and national defense systems all require uninterrupted power to maintain operational readiness. Cyberattacks on the energy sector could lead to further geopolitical implications, too, affecting national security and global stability.

As cybercriminals become more sophisticated and aging infrastructure remains a glaring security risk, energy providers must rethink their approach. Findings from Trustwave's recent 2025 Trustwave Risk Radar: Energy & Utilities Sector report underscore the importance of moving beyond compliance checklists to a resilience-based security model, which is essential to mitigating these growing threats.

The Outdated Infrastructure Time Bomb

The average electrical infrastructure in the U.S. is 40 years old, with a quarter of the grid exceeding 50 years. While these systems were designed for stability and reliability, they were not built to withstand modern cyber threats. Unfortunately, this is a two-pronged problem—the aging workforce and its familiarity with primarily outdated systems also opens the grid up to vulnerabilities, particularly within the IT sector responsible for modernizing and maintaining grid operations.

Specifically, many energy providers still rely on outdated industrial control systems and supervisory control and data acquisition networks. In many cases, these operational technology (OT) systems are directly connected to corporate IT networks, significantly expanding the attack surface. Cybercriminals can exploit weaknesses in IT environments to gain entry, then pivot into operational networks to manipulate power distribution systems or disrupt service.

Addressing these risks requires a strategic approach to modernization. Strengthening network segmentation and following a zero-trust security model can be some of the most immediate and effective steps. By separating IT and OT systems as much as possible, organizations can limit an attacker's ability to move laterally if one area is compromised. Zero trust further ensures that even trusted users and devices must prove their legitimacy before interacting with critical infrastructure.

As a longer-term strategy, energy providers should prioritize upgrades to legacy systems, replacing outdated technology in phases to minimize operational disruption while enhancing security. This phased approach should be strategic while not letting security go to the wayside.

For ongoing coverage, continuous monitoring can help provide real-time visibility across IT and OT environments to help detect anomalies early and prevent intrusions before they escalate. While the cost of these improvements may seem daunting, waiting for a catastrophic cyber incident to force change is a far riskier and more expensive alternative.

A High-Stakes Ransomware Game

Unlike other industries, energy operators cannot simply shut down systems to contain a cyber breach. The need to maintain continuous operations makes rapid recovery a top priority—something attackers have weaponized. While established ransomware groups like Conti and LockBit continue to dominate, newer actors such as Hunters International, Akira, and Qilin are aggressively entering the space. Hunters

International alone accounted for nearly 19% of ransomware attacks on the energy sector in the past year.

Ransomware is one of the most significant threats facing the industry today, with Trustwave's report finding an 80% increase in activity year over year. Threat actors exploit the pressure on utility and energy providers to maintain operations, demanding higher ransom payments in exchange for unlocking critical systems. Recent research has found that cyberattacks against the energy and utilities sector are escalating in both frequency and impact. Ransomware incidents have not only become more common but also more costly, with the financial toll of a breach averaging nearly $500,000 more than in other industries.

As attackers refine their tactics, energy providers must adopt a more aggressive defense posture. One of the most effective ways to thwart ransomware threats is by minimizing the reach of an attack. This includes ensuring critical systems have offline backups that cannot be encrypted or accessed by attackers, allowing for faster recovery without succumbing to ransom demands. Implementing automated incident response protocols can also help contain threats before they spread, reducing downtime and limiting financial damage.

Securing the Human Element in Grid Security

Despite widespread cybersecurity awareness initiatives, phishing remains the most common attack vector in the energy sector, accounting for 84% of breaches. Cybercriminals exploit human error through highly sophisticated social engineering tactics, tricking employees into opening malicious attachments, clicking fraudulent links, or unknowingly providing access credentials. Whereas before, an untrained eye could spot a phishing email by its typos, tone, or formatting errors from a mile away, sophisticated AI and deepfake technology have made these phishing attempts hyper-personalized and more realistic than ever.

Given the growing sophistication of phishing and social engineering operators, regular penetration testing and tabletop exercises should be used to simulate attacks and refine response strategies. Additionally, establishing dedicated threat-hunting teams can help identify signs of intrusion before malware is deployed, shifting the response from reactive to proactive.

AI-driven email security solutions that flag suspicious messages before they reach employees can also significantly reduce risk. At a minimum, organizations should mandate multi-factor authentication (MFA) for all personnel with access to OT systems, ensuring that stolen credentials alone are not enough for an attacker to gain entry. While these measures won't eliminate phishing risks entirely, they can reduce the impact if and when an attack occurs.

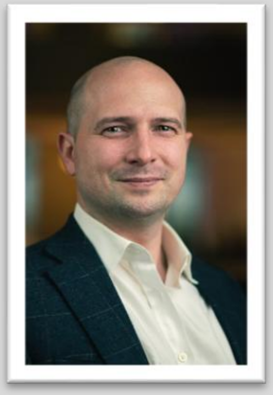
A Blueprint for Resilience

Relying on compliance checklists is no longer enough. Energy providers must take meaningful steps to fortify their security posture against evolving threats. Enforcing strict access controls and network segmentation, continuously verifying the identity of users and devices can limit the impact of a breach.

Collaboration will also be key in the years ahead. Energy providers, government agencies, and cybersecurity researchers must work together to share threat intelligence, conduct joint incident response exercises, and establish industry-wide security standards.

The future of energy security depends on the industry's ability to adapt to an increasingly hostile threat landscape. By prioritizing resilience and embracing modern security frameworks, energy providers can build a more secure foundation for the digital age.

About the Author

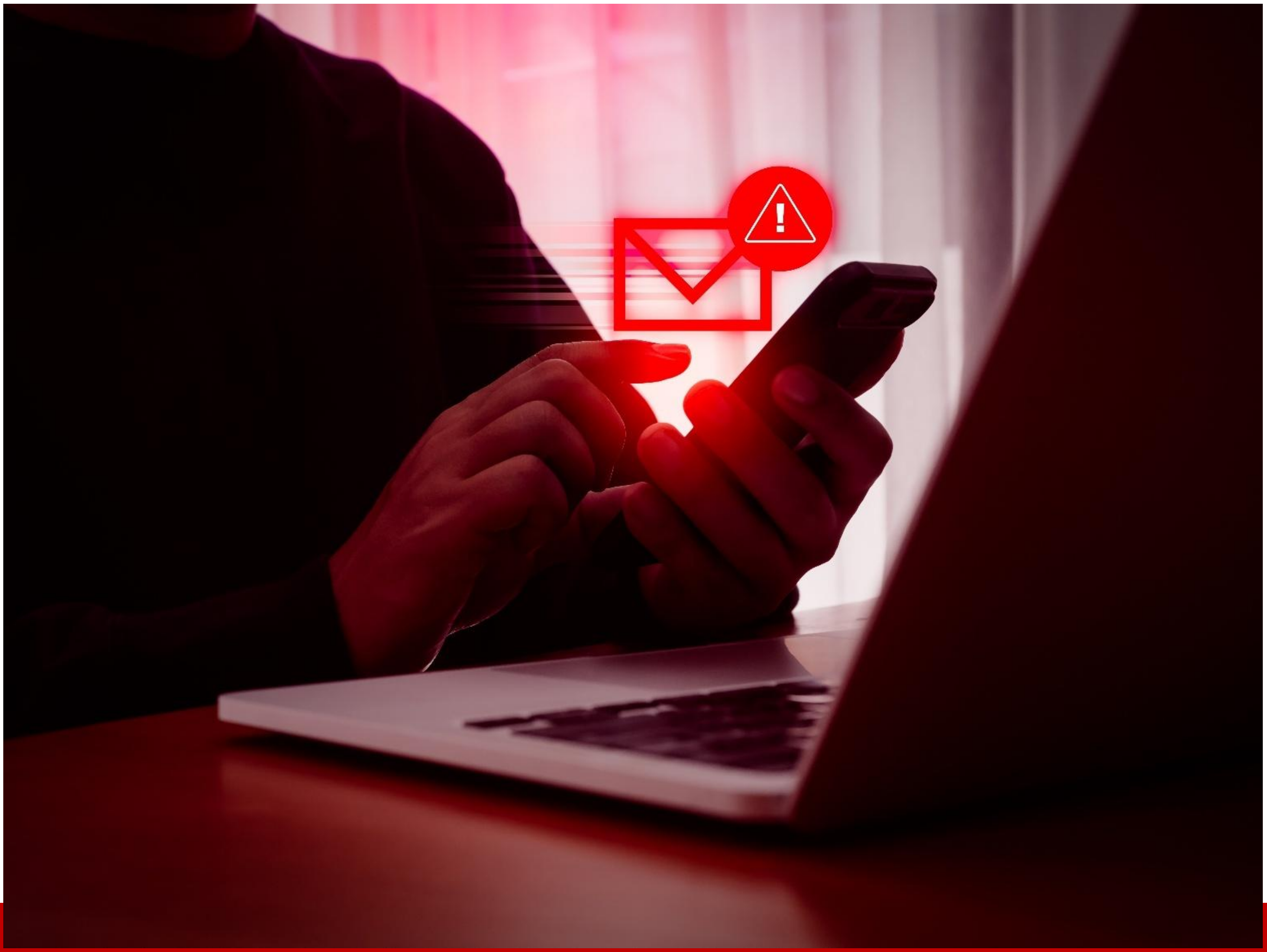


Kory Daniels is the Chief Information Security Officer at Trustwave, overseeing the cybersecurity strategy and defense for the company and its clients. With over 15 years of experience, he has led cyber defense initiatives and modernization efforts, including Trustwave's global cyber advisory and integration services.

Previously, Kory led cyber transformation at IBM, focusing on portfolio innovation, AI and machine learning in cyber defense, and building enterprise cyber defense centers. Before IBM, he held leadership and sales roles at various security startups.

Kory's diverse experience in sales, consulting, and operations has shaped his approach to cyber resilience at Trustwave. He is passionate about building trust within the CISO community and often presents at industry events. Kory holds a CISSP certification and a BA from Drew University.

Kory can be reached at https://www.linkedin.com/in/korydaniels/



Stopping Fraud: What Does Email Got to Do with It?

By Maanas Godugunur, Senior Director, Fraud and Identity, LexisNexis Risk Solutions

With 7.9 billion email accounts worldwide and 4.3 billion active users, emails now play an essential role in fraud detection and identity verification. Businesses leverage email not just for communication but also as a vital tool to assess risk, prevent fraud and gain greater confidence in associated identity attributes. Email addresses anchor digital identities in today's interconnected world.

Email addresses are remarkably stable, with most users keeping the same one for over a decade despite life changes like moving or changing phone numbers. This consistency makes email an invaluable resource in fraud prevention as it allows organizations to gain deeper insights into consumer behavior.

Email as a Constant in the Digital Landscape

Emails persist where other identifiers fluctuate. People often change physical addresses, upgrade devices or adopt new phone numbers, but their email remains a trusted and enduring constant. This permanence allows businesses to assess consumer behavior over time, a process which strengthens fraud detection frameworks.

Beyond its dependability, email dominates consumer-business communication. Research reveals 55% of retail customers prefer email for communication, underscoring its significance. Businesses use email to track not just preferences but also transaction history, creating a robust layer of intelligence for identifying suspicious behavior.

Spotting Fraud Through Consumer Behavior

Understanding the historical behavior of an identity offers the strongest defense against fraud. Email activity patterns help establish baselines. If a fraudster employs an email address outside of an identity's usual patterns, such as initiating spikes in email-driven transactions or shifts in location, it can be a sure sign of fraud.

Imagine an email occasionally used for ordering food or managing accounts suddenly processes 10 transactions in a single day. This deviation raises a red flag. Yet not all unusual behavior points to fraud. Seasonal shopping or travel can cause spikes in transactions and businesses must evaluate additional elements like billing addresses, shipping details and device usage to validate authenticity.

Associated data points, such as social media activity, also offer critical fraud insights. A complete social media profile with a photo, posts and friends suggests legitimacy, while inactive or incomplete accounts may imply risk. By integrating email data with these attributes, businesses build a clearer picture of whether the user is genuine or potentially engaging in fraud.

Addressing the Next Wave of Fraud

Fraud is evolving rapidly with the rise of generative AI, making it essential for businesses to adopt advanced detection tools. Businesses must implement adaptable, machine learning-driven solutions to stay ahead.

Machine learning (ML) enhances fraud detection by analyzing thousands of data points and refining its models based on real-time activity. These intelligent systems identify fraud patterns unique to each industry, region and customer, enabling businesses to counter even the most sophisticated fraud tactics effectively.

Balancing Security and Growth

Advancements in AI and ML will drive the future of email intelligence in fraud prevention, enabling organizations to combat increasingly sophisticated fraud tactics. These technologies will analyze vast amounts of data in real time, identifying nuanced patterns and predicting potential fraud with greater precision.

AI will continuously evolve alongside fraud tactics, learning to detect even the most subtle anomalies while adapting to emerging threats. This evolution will empower businesses to proactively mitigate risks, deliver more accurate fraud detection and balance security with seamless user experiences, cementing email intelligence as a cornerstone in modern fraud prevention strategies.

Businesses must strike a balance between robust fraud prevention and seamless customer experiences. Overly aggressive fraud controls risk alienating legitimate users, while lax measures open the door to fraud.

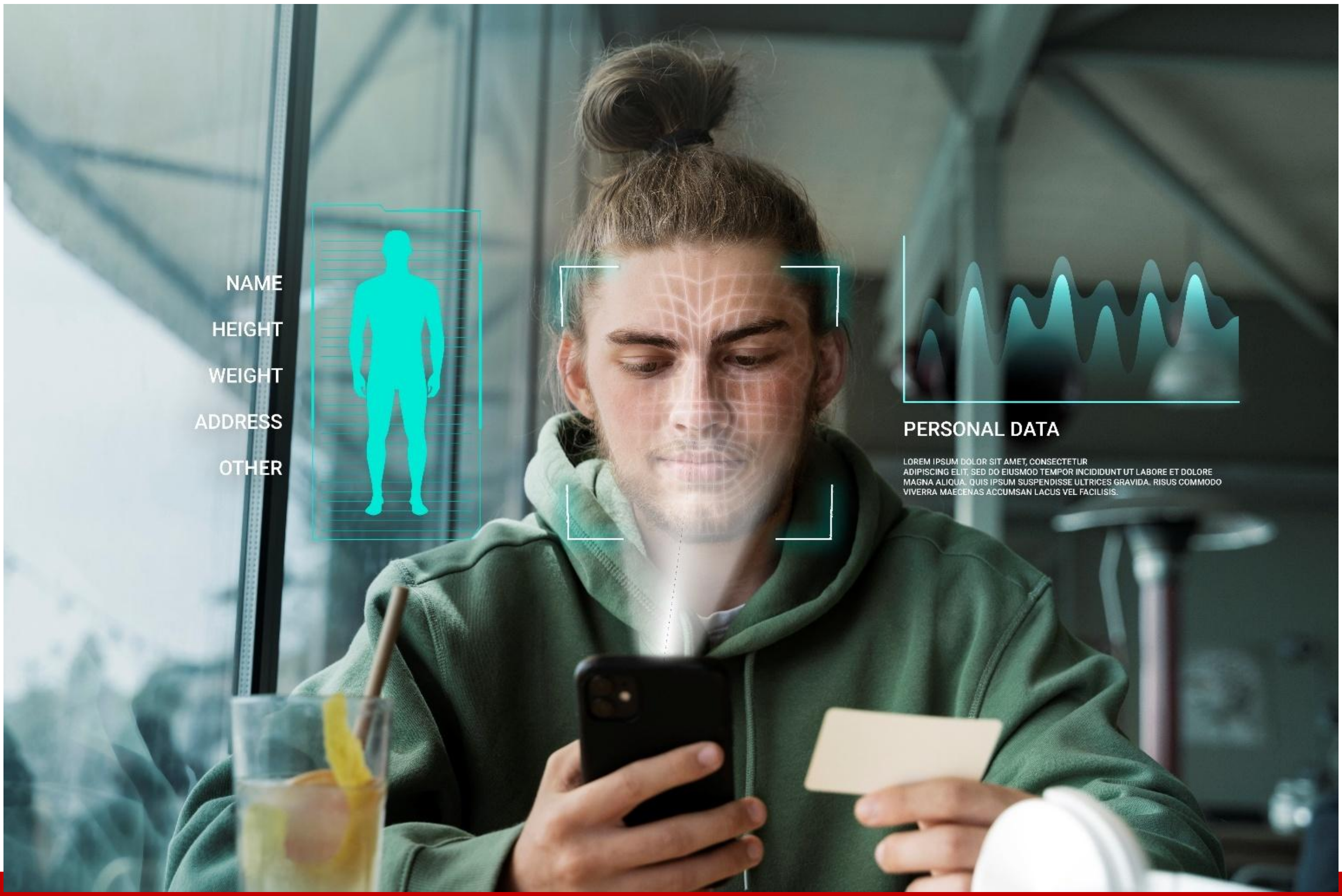
Email intelligence helps businesses maintain this balance. By relying on email's stability and understanding the behavioral context behind it, organizations safeguard their operations while building trust with customers. Fraud prevention, when executed accurately, enhances customer satisfaction and loyalty, driving growth.

With fraud threats growing more complex, the role of email intelligence has become even more critical. By harnessing the stability and behavioral insights provided by email addresses, businesses can combat evolving fraud tactics while ensuring secure, seamless experiences that benefit both customers and organizations alike.

About the Author

Maanas Godugunur is the senior director of fraud and identity at LexisNexis® Risk Solutions, a leader in providing essential information to help customers across industry and government assess, predict and manage risk.

https://risk.lexisnexis.com/


NAME
HEIGHT
WEIGHT
ADDRESS
OTHER
PERSONAL DATA
LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT, SED DO EIUSMOD TEMPOR INCIDIDUNT UT LABORE ET DOLORE MAGNA ALIQUA. QUIS IPSUM SUSPENDISSE ULTRICES GRAVIDA. RISUS COMMODO VIVERRA MAECENAS ACCUMSAN LACUS VEL FACILISIS.

The Power of Identity Analytics to Transform Your ID Management

By Chris Scheels, Vice President of Product Marketing, Gurucul

Digital identities continue proliferating throughout modern organizations and are a significant target for bad actors. Stolen identities and privileged access credentials account for most data breaches. In fact, identities and the systems that manage them are often among the first areas where breach attempts are made.

Managing the growing number of identities is increasingly complex, partly due to the many different Identity Access Management (IAM) solutions most organizations have today. Traditional solutions that comprise identity management include everything from Identity Governance & Administration (IGA) to privileged access management (PAM), Active Directory as a Service (ADaaS) and Single Sign-On (SSO). These tend to be siloed and don't enable organizations to prioritize identity management based on risk.

Applying analytics to the activity of all these solutions to bridge the gap between disparate solutions will reduce risk and improve controls for all solutions. Doing so will enhance identity security posture, but it requires an innovative approach to identity management with a risk mindset and rich overlay analytics to inform it.

Challenges with the legacy approach to identity management

According to the Verizon Data Breach Investigations Report, 68% of breaches involve a non-malicious human element, such as a person falling victim to a social engineering attack or making an error. Methods like account compromise, social engineering, phishing and stolen credentials are typically the first steps in any attack chain.

Identity security is essential; reducing the risk of these events decreases your chances of a breach (with prevention, prediction, detection, and response) and the cost repercussions of a breach, which are rising. The IBM Cost of a Data Breach report found that the global cost of a data breach soared to $4.88 million in 2024, a 10% increase from the year prior.

It's challenging to manage this function without an effective way of integrating the separate aspects and telemetry of identity and access management.

How an identity analytics overlay can help

A risk-based identity management approach aims to protect user identities and systems from cybersecurity threats, combining best practices, tools and processes to find and mitigate identity-based threats. Using identity analytics provides a new cutting-edge ability to bring this all together. It’s a risk-based and value-driven approach that leverages the latest technologies to add or connect the dots with identity accounts and access entitlements down to a granular level.

A holistic approach like this helps with cost optimization. Combining all these elements lets you gain an overall 360-degree view that shows who has access to what. This creates a return on investment (ROI) in multiple ways. First, this approach enables you to see what's not being used but for which you're paying the software licensing costs. This helps reduce unnecessary identity costs.

Second, this approach makes the process of meeting compliance requirements more efficient. For example, many large companies undergo the Sarbanes-Oxley (SOX) 404 certification process. They receive a quarterly report listing all the access people have and must certify it. These entitlements can be very cryptic, and there’s a lot of rubber-stamping without understanding what's behind the access on that list. That's wasteful spending on resources that could be focused on more strategic initiatives.

Identity analytics can give organizations risk-based and AI/ML-powered certification, which tells a business owner when someone in a peer group has unusual access. You can revoke this access or have a rock-solid paper trail of an approved exception. Massive ROI is possible here, as you can reduce the time it takes for compliance, improve compliance and possibly even reduce fines.

Another potential area for cost and time savings is provisioning. With an identity analytics approach, the access certification process is streamlined and expedited using machine learning and automation even before the provisioning process begins. In many companies, when a new person comes on board, their manager requests the same access their predecessor had. That can seem sensible, but the new employee may not need all the same permissions and access, which means your team will spend valuable time and resources granting extraneous access. Many companies aren’t using automation for this process, so it can take up to a month or more to fully provision someone. That works out to a lot of wasted time.

A better approach is to initially limit and reduce overprivileged access to match the peer group and then only assign additional privileges for specific, documented reasons. An identity analytics solution can help with this; not only does this reduce the identity attack surface, but it also prevents unnecessary licensing costs.

Identity analytics makes business sense

In today's digital landscape, identities are proliferating like never before. All of these identities must be appropriately managed, or they become major security risks. Proper identity management can help reduce security risks and save money. Identity analytics represents a new approach to risk-based identity management that reduces the complexity, attack surface and expense while improving security and protection of sensitive data.

About the Author

Chris Scheels is Vice President of Product Marketing at Gurucul. Chris has been aligning people, processes and technology to drive companies forward for over 20 years. He has a decade of cybersecurity experience in product marketing and product management. His passion is helping businesses succeed through the strategic use of technology. Most recently he was helping customers accelerate their Zero Trust journey at Appgate, Inc. His background also includes experience in operations, sales, and new business development.

Chris can be reached at https://www.linkedin.com/in/scheeler/

Verified Trust Is the New Currency: Why Digital Platforms Must Prioritize Security and Transparency

By Raj Ananthanpillai, CEO and Founder, Trua

In an era dominated by apps and on-demand everything, convenience was once king. However, a new national consumer survey by Talker Research, commissioned by Trua, reveals that the tide is turning. Consumers are no longer content with trading security for speed or transparency for ease. Instead, they're demanding something more meaningful: trust.

From dating apps and rideshares to freelance marketplaces and home services, today's users want to know exactly who they're dealing with—and whether the platform has their back. Trua's survey, which gathered responses from a broad cross-section of American adults, sends a powerful message: digital platforms that fail to prioritize security, privacy and transparency are at serious risk of losing consumer confidence—and fast.

Let’s break down the numbers and explore why this shift matters more than ever.

A Crisis of Confidence in Vetting

One of the most eye-opening findings: only 18% of respondents expressed high confidence that service providers on popular platforms are thoroughly vetted. That means four out of five users are unsure—or outright skeptical—about whether the person delivering their groceries, fixing their sink or messaging them on a dating app has been properly checked out.

The trust gap is even more striking among older generations. Half of Gen X and 39% of Baby Boomers reported having little to no confidence in current vetting processes. For platform providers, this isn’t just a PR problem—it’s a business risk. Without trust, users hesitate. And hesitation means churn.

Users Are Willing to Pay for Peace of Mind

It’s easy to assume users always want services to be faster and cheaper. But Trua’s survey reveals a surprising twist: 60% of consumers say they’d pay extra if it meant enhanced background checks for service providers. That’s a wake-up call for platforms still operating under a “convenience-first” mindset.

In fact, users seem less concerned about cost than they are about safety and assurance. This insight opens up a whole new opportunity for companies willing to invest in better vetting tools. Enhanced security could become a selling point, not just a backend feature.

The Data Privacy Disconnect

When it comes to data, consumers aren’t just uneasy—they’re fed up. A staggering 87% of respondents believe platforms fail to clearly communicate how their personal information is used or protected. Even more troubling: many feel they have little to no control over how that data is shared.

The message here is simple: opaque data practices are killing trust. Users don’t just want to check a box and move on—they want to know what they’re signing up for, what information is being collected and how it’s being safeguarded. If they don’t feel respected, they’ll walk.

Fraud, Scams and AI Fakes: The Growing Fear Factor

Fraud and identity theft are no longer distant threats—they're daily concerns. According to the survey:

- 55% of consumers worry about scams
- 43% fear identity theft or account hacking
- 36% cite payment security as a major concern

Only 41% feel confident that their financial data is safe when transacting online. And it doesn't end there—75% of consumers now fear AI-generated accounts masquerading as real users.

Fake profiles, deepfakes and bots aren't just irritating—they're dangerous. They erode credibility, introduce safety risks and make genuine human connection feel impossible. Platforms that fail to identify and remove these threats are playing with fire.

What Platforms Must Do Now

It's clear the old rules no longer apply. Platforms can no longer get by with surface-level safety measures or one-time verifications. The public wants—and deserves—more.

Here are four actions digital platforms should prioritize:

1. Stronger Identity Verification

Implement ongoing, AI-enhanced verification tools—not just one-time checks. This means running background screenings, validating government-issued IDs and detecting behavioral red flags across the user lifecycle.

2. Radical Data Transparency

Be upfront. Explain in plain English what data is collected, why and how it's used. Give users real control over their information, including the ability to revoke access and delete records.

3. Smarter Fraud Prevention

Use robust technologies to automate tasks and actively detect anomalies, fake accounts and fraud signals. Flag suspicious behavior early and act fast. Make it clear to users that you're monitoring and protecting them.

4. Tools That Empower Users

Give users visibility into their own trust credentials—think verified badges, trust scores or opt-in safety tiers. Let them easily report abuse, track support requests and customize their safety settings.

Verified Trust Is the New Differentiator

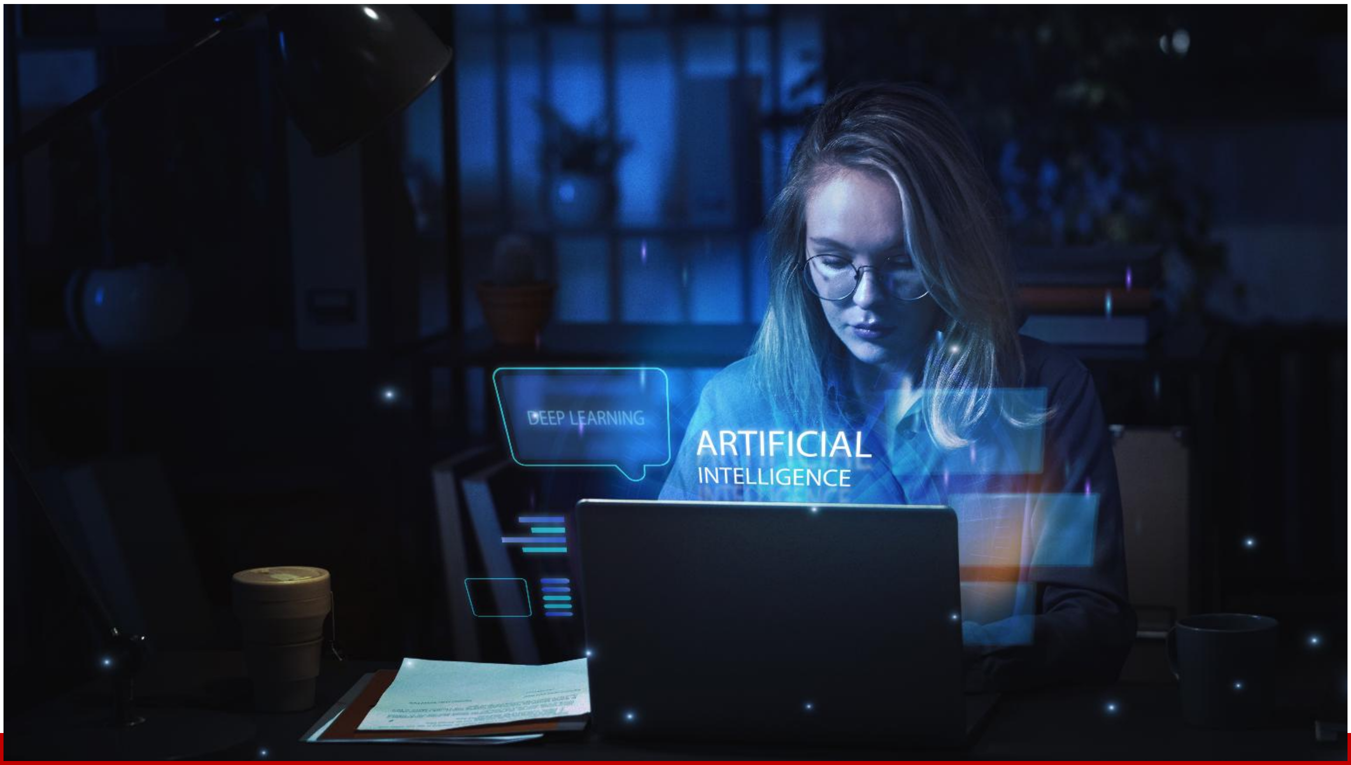
The days of competing solely on speed, choice or price are gone — trust now reigns supreme. Consumers are demanding platforms that deliver verified security, transparent practices and genuine connections, and they're ready to walk away from those that don't.

Imagine choosing a rideshare driver you know has been thoroughly vetted or a marketplace where every profile is real and accountable—doesn't that feel worth it? Platforms that weave trust into every interaction will not only keep users but inspire fierce loyalty. Don't let skepticism erode your business.

Act now: invest in robust verification, empower your users and make trust your defining feature—because consumers are watching, and they're ready to choose the platforms that choose them first.

About the Author

Raj Ananthanpillai, CEO and founder of Trua, is a technology entrepreneur and visionary leader with over 30 years of experience driving innovation and business transformation. He has built and scaled technology companies, leveraging his expertise in problem-solving, digital trust, and enterprise growth to shape the future of secure identity verification. Ananthanpillai leads the development of next-generation privacy-preserving Trust credentials, redefining digital identity and empowering individuals with greater control over their personal data. Previously, he served as CEO of Endera, which he founded in 2017, and spent 13 years as CEO of InfoZen, a risk management firm acquired in 2017. He also held leadership roles at ePlus Inc. (NASDAQ: PLUS), NetBalance, and AT&T. Raj can be reached online at https://www.linkedin.com/in/raj-ananthanpillai-trua/ https://x.com/AnanthanpillaiR and at our company website https://truame.com/



Where AI Meets Cybersecurity: Navigating 2025’s Top Threats with BeamSec

How email-based risks and human error can be solved by adopting AI-first approach

By Murat Guvenc, Managing Director, BeamSec

2025: A Year of Faster, Smarter Cyber Threats

As we move deeper into 2025, cyber threats are not only multiplying they’re evolving. From AI-generated phishing emails to personalized scams and adaptive malware, today's threat landscape is marked by speed, complexity, and unpredictability. Security leaders are being forced to rethink their approach not just by upgrading technical defences but by addressing the root of many breaches: human error.

Regulated industries such as banking, insurance, healthcare, Telco, and government are particularly exposed. They manage vast volumes of sensitive data, often across aging digital infrastructures. Even in well-protected environments, a single click on a malicious link can result in widespread disruption. The message is clear: modern cybersecurity must protect not only systems but also the people who use them.

The Growing Role of AI in Everyday Defense

Artificial intelligence has transitioned from buzzword to backbone in the cybersecurity space. It's now central to how organizations detect threats, analyze behaviour, and adapt to emerging attack patterns. But just as defenders harness AI to strengthen their systems, attackers are doing the same to sharpen their tactics, making them faster, harder to trace, and increasingly deceptive.

This duality places organizations at a crossroads. Protecting digital assets now demands a two-fold strategy: build smarter defenses and equip people to recognize and avoid threats in real time. It's here that real change begins.

When Awareness Breaks Down, Attacks Break Through

Phishing remains one of the most successful and damaging attack vectors and for good reason. These threats are designed to exploit the most vulnerable link in any security chain: human behavior. A user distracted by a busy workday or unaware of subtle red flags can unintentionally invite risk into the organization.

Solving this challenge requires more than one-off training videos or annual compliance modules. It demands dynamic, personalized, and persistent engagement, something that becomes a natural part of everyday work, rather than a forgotten checkbox.

AI-Powered Defense: How BeamSec Is Tackling Both Sides of the Problem

At GISEC 2025, BeamSec introduced a forward-thinking answer to this dual challenge with the official launch of MailX, an AI-driven email monitoring and behavioral analysis engine built to detect, learn, and act in real time.

MailX continuously scans organizational email environments, studying how teams communicate and identifying irregularities before they become threats. A misspelled domain, a mismatched tone, or an unusual attachment subtle clue that often slip past legacy filters are flagged and addressed instantly. MailX's strength lies in its ability to adapt to each organization's unique communication style, learning what's normal so it can spot what's not.

However, AI doesn't just belong behind the scenes. For a security strategy to truly work, it must also engage the people who live in their inboxes daily. That's where Alfred comes in. Alfred is BeamSec's Personal Cybersecurity Awareness AI Assistant built for human-centric cybersecurity awareness. Instead of static training, Alfred delivers real-time learning, contextual feedback, and intuitive guidance directly within the employee workflow. It helps users report suspicious emails, scan risky attachments, and receive instant tips all without leaving their inbox.

More than a chatbot, Alfred is a dynamic learning companion that adapts to user behaviour and builds security confidence over time. With every interaction, teams become more alert, more informed, and better prepared to respond when it matters most.

Looking Ahead

Cybersecurity in 2025 is no longer just about building walls. It’s about building smarter systems and smarter people. BeamSec’s AI-first approach combines advanced threat detection with behavioural awareness, forming an adaptive defense that evolves alongside modern threats. By helping organizations reduce risk exposure, elevate employee awareness, and respond in real time, BeamSec offers not just protection but peace of mind in a world where cyber threats show no signs of slowing down.

About the Author

Visionary IT Executive with 20+ years of business development, sales leadership, channel management, marketing, and consulting experience working for global organizations in Canada, USA, UK, Europe, and the Middle East. Murat has taken several leadership roles creating and implementing go-to-market strategies, driving revenue growth, and promoting innovation and organizational effectiveness. As Managing Director of BeamSec, Murat is responsible for the vision and strategic direction of the company, executing the overall business strategy, leading a high-performing team, and building strategic partnerships to ensure the company’s long-term success.

Murat Guvenc’s LinkedIn: https://www.linkedin.com/in/muratguvenc/ or visit www.beamsec.com to learn more.

Why Certification is Critical for Securing the Future of eSIM and IoT Connectivity

By Sönke Schröder, Director Go-To-Market Strategy and Innovation at Giesecke+Devrient (G+D)

The Internet of Things (IoT) has evolved from a visionary concept into a global reality. With over 38 billion connected devices projected by 2030[1], the IoT ecosystem has expanded into nearly every sector—healthcare, energy, automotive, logistics, and consumer tech. This interconnected future offers remarkable benefits in efficiency, automation, and data-driven decision-making. Yet it also raises unprecedented cybersecurity challenges.

In today's age of exponential device growth and digital modernization, trust in device connectivity is very important. Security can no longer be a secondary consideration; It must be embedded into the core of device design, manufacturing, and provisioning processes. Certification—particularly in the context of emerging technologies like eSIM and embedded Universal Integrated Circuit Cards (eUICC)—is proving to be an essential mechanism for ensuring that trust.

The Role of Certification in the Modern IoT Landscape

As IoT becomes further entrenched in critical infrastructure and daily life, the locations of cyber-attacks grow in both scale and complexity. Devices are no longer isolated endpoints—they are interconnected components in dynamic, real-time networks. This complexity makes them harder to secure, and vulnerabilities in even the smallest sensor can ripple across larger systems with severe consequences.

Security certification frameworks help address these risks by offering structured validation that devices and their embedded connectivity modules comply with robust technical and cryptographic standards. Rather than relying solely on vendor claims, certification provides third-party assurance that security expectations are met—before threats emerge.

In the case of eSIM and eUICC, certification validates the secure storage of credentials, secure remote provisioning, and tamper resistance. It also ensures that devices can safely switch network profiles across mobile operators worldwide. These assurances are foundational to reducing long-term operational risks and protecting data integrity across the device lifecycle.

Why Early Certification Matters

The acceleration of standards such as SGP.32—a recent Global System for Mobile Communications Association (GSMA) specification for IoT remote SIM provisioning—marks a watershed moment in IoT security and scalability. However, achieving compliance with these standards requires more than technical capability; it demands early planning, alignment with testing bodies, and a willingness to evolve with the ecosystem.

Early certification allows device manufacturers, SIM vendors, and operating system providers to implement secure protocols before market launch. This improves time to market and also reduces the cost and complexity of post-launch security retrofits. In fact, leading organizations that pursue dual certifications—spanning both security assurance and GRC (governance, risk, and compliance) standards—are better positioned to manage today’s complex regulatory landscape. As businesses expand internationally, staying aligned with local and cross-border regulations often requires dedicated teams to monitor and implement compliance protocols[2].

Importantly, these certifications are not handed down from regulatory bodies in isolation. They are the product of close collaboration between industry leaders, standards organizations, and security experts. This consensus-driven approach ensures that security frameworks are technically aligned with real-world deployment challenges, helping to drive broader ecosystem readiness.

Secure at Birth: The Power of In-Factory Provisioning

One of the most promising outcomes of standardized certification is the enablement of In-Factory Profile Provisioning (IFPP). This approach allows a secure digital identity to be embedded directly into a device during manufacturing, effectively making it “secure at birth.”

This model has multiple advantages. For one, it eliminates the need to ship devices with preloaded regional SIMs or provision profiles in the field, which can introduce security gaps. Instead, a universal device SKU can be produced and provisioned remotely with a local operator profile when deployed—streamlining production and improving logistics flexibility.

This also mitigates security risks by reducing the number of device variants in the field. Fewer SKUs mean fewer opportunities for configuration errors, firmware inconsistencies, or overlooked vulnerabilities—all common pain points in large-scale deployments.

Moreover, recent improvements in testing methodologies have shortened certification timelines dramatically, in some cases to under eight weeks. This increased speed reflects both the maturity of the underlying standards and the urgency of securing the IoT landscape at scale.

Long-Term Benefits of a Certified, Standards-Based Ecosystem

The benefits of pursuing certification for eSIM-based IoT devices extend well beyond regulatory compliance. Certification represents a strategic investment in resilience, flexibility, and global interoperability—key pillars for long-term success in the evolving IoT environment.

First and foremost, certified devices are designed with robust defenses against a wide array of cyber threats. From physical tampering to remote exploitation, they are built to maintain the integrity of sensitive data and credentials. Embedding this level of security from the outset minimizes long-term exposure and significantly reduces the costs associated with incident response and system recovery.

Additionally, organizations benefit from improved business continuity. Certified eSIM and remote provisioning frameworks allow devices to seamlessly switch profiles and connect to alternative networks. This capability supports uninterrupted service delivery, even in the face of localized network outages or geopolitical disruptions.

Global operability is another major advantage. Devices that adhere to internationally recognized certification standards are inherently more interoperable, capable of functioning across different countries and carrier networks without the need for region-specific adaptations. This facilitates global scalability and accelerates time to market.

From a regulatory standpoint, certified hardware and software solutions provide a clear path toward compliance with privacy laws, critical infrastructure protections, and cross-border data handling mandates. Certification signals to regulators and partners alike that an organization has taken proactive measures to secure its products.

Last, but certainly not least, the operational benefits are significant. Certified devices typically experience fewer vulnerabilities post-deployment, reducing the frequency of security patches and emergency updates. This leads to lower total cost of ownership, more predictable maintenance schedules, and fewer disruptions to service.

Preparing for the Next Phase of Digital Transformation

As edge computing, artificial intelligence, and machine learning become more tightly integrated into IoT applications, the importance of a secure foundation cannot be overstated. Cybersecurity will no longer be about locking down endpoints—it will be about protecting real-time, autonomous decision-making processes powered by billions of constantly communicating devices.

Industries ranging from smart healthcare to industrial automation rely on the integrity of their connectivity layers. Without certified assurance, these systems risk becoming vectors for attack instead of engines of innovation.

Now is the time for businesses to evaluate their connectivity and provisioning strategies through the lens of security certification. By aligning with globally recognized standards and engaging early with certification frameworks, organizations can foster trust across their ecosystems and scale confidently into the future.

As the IoT ecosystem matures, stakeholders must embrace certification not just as a technical requirement but as a strategic differentiator. In doing so, they'll help build a safer, smarter, and more secure digital future.

1: https://www.gsmaintelligence.com/research/iot-connections-forecast-to-2030

2: https://www.cio.com/article/242680/the-top-6-governance-risk-and-compliance-certifications.html

About the Author

Sönke Schröder is Director Go-To-Market Strategy and Innovation at Giesecke+Devrient (G+D), a global SecurityTech company located in Munich, Germany, with a global workforce of more than 14,000 employees. G+D makes the lives of billions of people more secure with built-in security tech in three segments: Digital Security, Financial Platforms and Currency Technology.

Sönke is an expert in the world of Connectivity and IoT with over 23 years of hands-on experience with Giesecke+Devrient and a highly technical educational background in physics having attended both the University of Hamburg and the Technical University of Munich. You can reach Sönke online at connectivity@gi-de.com and at our company website, https://www.gi-de.com.

Winning the Breach Intelligence Race: How CISOs Can Stay Ahead of Threats Using Public Data

How proactive CISOs are using public intelligence to detect breaches before they impact the organization

By Aditya Gupta, Industry Principal & Segment Delivery Head, Americas at Infosys Cybersecurity Practice

Introduction

In today's fast-evolving threat landscape, traditional breach detection systems often fall short in providing early warnings. CISOs are under pressure to not only respond to alerts faster but also to anticipate risks before they materialize. Public data, when harnessed correctly, provides a unique and critical early warning system for threats that have yet to trigger internal alerts. This article explores how leveraging public intelligence, including social media, open-source repositories, and curated feeds, can provide CISOs with valuable insights to stay ahead of potential threats.

Why Traditional Signals Come Too Late

Reliance on traditional threat detection systems can leave gaps in identifying emerging threats early. Public data, including social media chatter and open-source repositories, often provides critical early signals that formal alerts miss. High-profile breaches like SolarWinds (2020) and Log4Shell (2021) revealed that the first signs of a breach frequently surface in social media and GitHub before they are acknowledged by vendors or internal security systems. Relying solely on vendor advisories and internal alerts puts organizations at a disadvantage, exposing them to prolonged risks.

With the average breach dwell time hovering around 10 days globally, early detection is crucial. Public intelligence can help shorten response times and reduce exposure by enabling organizations to act sooner than traditional detection methods allow.

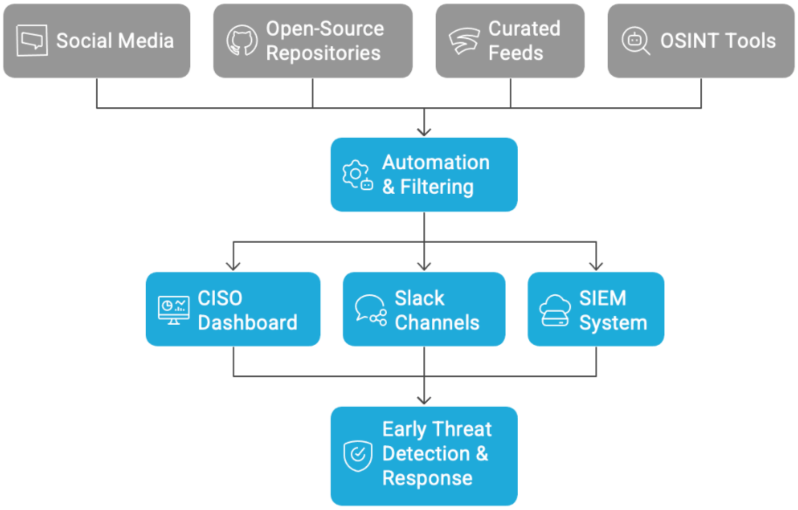
Turning Public Data into Early Signals

Proactive CISOs are integrating publicly available data into their early warning systems. Tools like Google Alerts, configured with phrases like “Fortinet zero-day” or “SAP breach,” offer instant visibility into emerging incidents. These alerts, routed to CISO dashboards or Slack channels, provide situational awareness without waiting on internal escalations.

Curated sources, such as Feedly Pro, can help filter out irrelevant content and focus on specific vendors, known exploit vectors, or niche research blogs. When paired with AI-powered assistants, these platforms can streamline the flow of critical insights and prioritize threats based on relevance to the organization’s infrastructure.

Open-source intelligence (OSINT) tools, such as Have I Been Pwned and Shodan, further enhance threat detection by tracking credential leaks and scanning public infrastructure for exposed vulnerabilities. By integrating these insights into existing security platforms, CISOs can automate threat prioritization and streamline incident response.

Public Intelligence Integration Flow

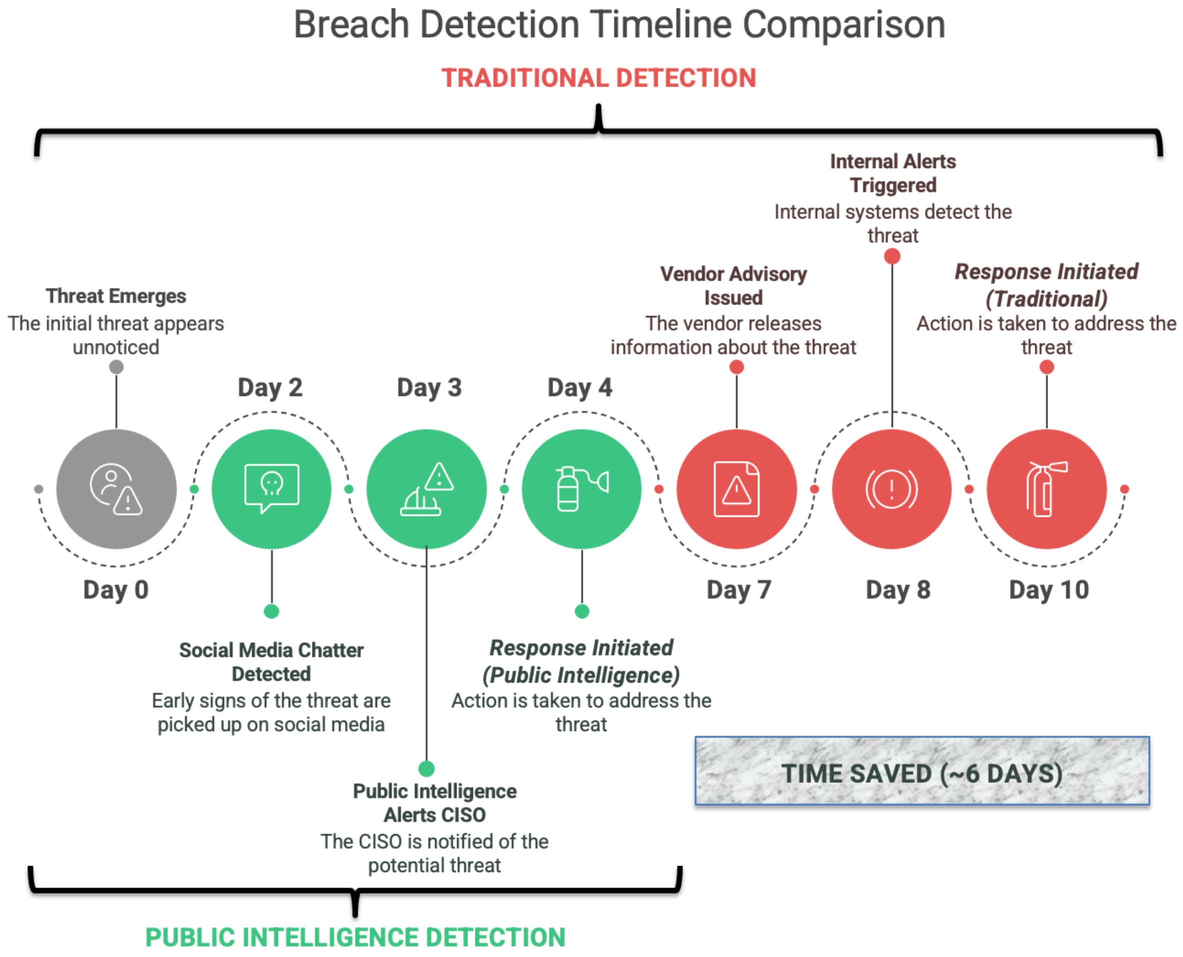


Social Signals: Where Real-Time Starts

Real-time risk intelligence now lives on platforms like X (formerly Twitter), Reddit, and GitHub. Researchers often disclose suspicious patterns hours, sometimes days, before formal publication. By monitoring specific hashtags like #cyberattack and following influential cybersecurity figures, CISOs can track the pulse of live threat activity.

Reddit forums like r/netsec and GitHub repositories often share actionable insights from practitioners in the field, including proof-of-concept exploits or vulnerable configurations. These real-time signals, while often unstructured, provide early indicators of potential breaches.

To scale this process, automation tools like Zapier or n8n can route social mentions, GitHub commits, or blog posts into triage workflows. These signals can then escalate into SIEM systems or trigger automated checks, helping organizations act before internal alerts are raised.


Breach Detection Timeline Comparison
TRADITIONAL DETECTION
Threat Emerges
The initial threat appears unnoticed
Day 0
Day 2
Social Media Chatter Detected
Early signs of the threat are picked up on social media
Day 3
Public Intelligence Alerts CISO
The CISO is notified of the potential threat
Day 4
Response Initiated (Public Intelligence)
Action is taken to address the threat
Vendor Advisory Issued
The vendor releases information about the threat
Day 7
Internal Alerts Triggered
Internal systems detect the threat
Day 8
Response Initiated (Traditional)
Action is taken to address the threat
Day 10
TIME SAVED (~6 DAYS)
PUBLIC INTELLIGENCE DETECTION

From Noise to Response: The Okta and MOVEit Lessons

Real-world breaches like Okta (2023) and MOVEit (2023) illustrate the value of public intelligence in early threat detection. In both cases, unusual activity was flagged on social media before the vendors acknowledged the issue. Organizations that acted on these early public signals were able to mitigate risk by isolating vulnerable systems or locking down accounts before formal advisories were issued.

While traditional alert systems are essential, public signals can enable faster responses and reduce an organization's exposure window. By tuning into social channels and open-source intelligence, CISOs can detect breaches long before they are formally acknowledged.

Aligning Public Intelligence with Executive Goals

The ability to act on public intelligence not only improves response times but also enhances an organization's security posture and reputation. According to IBM's 2023 breach cost study, companies leveraging automated threat intelligence saved an average of $1.76 million per incident. This underscores the value of proactively integrating public intelligence into a company's security strategy.

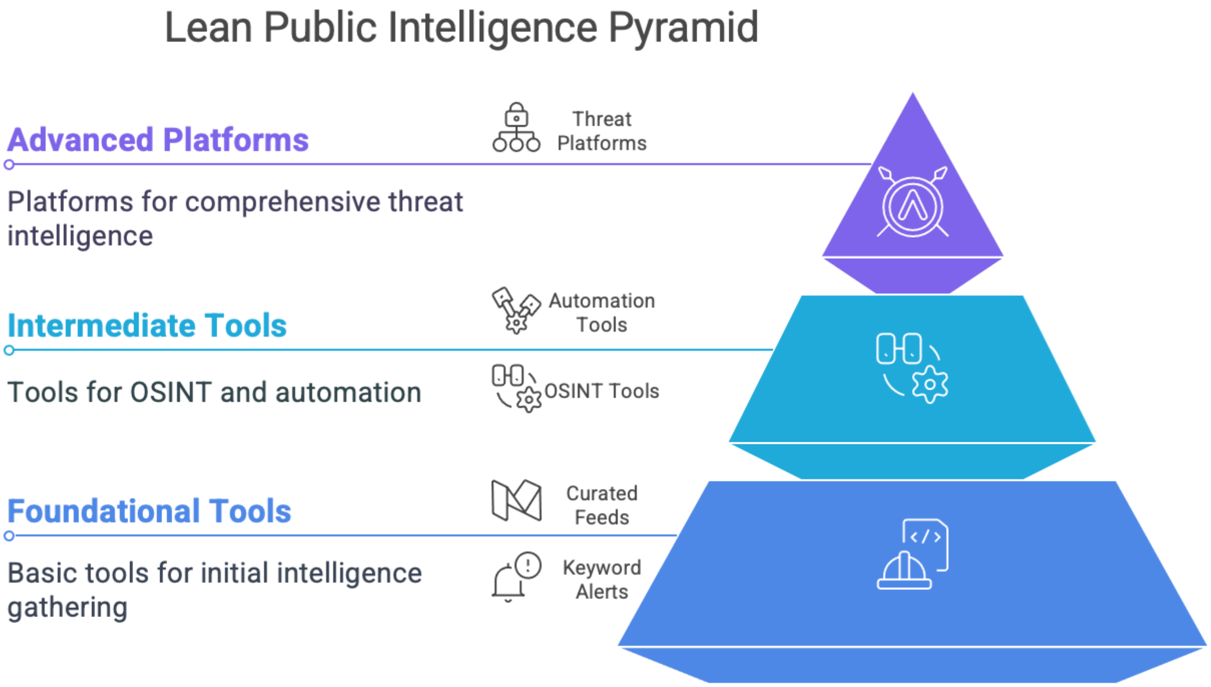
Public intelligence also allows CISOs to brief executives and boards before a breach becomes public, demonstrating foresight and proactive risk management. This helps build trust across the organization, positioning security as a key enabler of business continuity.

Build a Lean, Scalable Framework

To get started with integrating public intelligence, organizations don't need to overhaul their entire security strategy. Simple keyword alerts and curated feeds can provide immediate visibility into emerging threats. OSINT tools like Shodan, Have I Been Pwned, and others can be added as a layer on top of existing security infrastructure.

For more mature organizations, advanced threat intelligence platforms like Recorded Future or Flashpoint can be configured to reflect the specific technology stack in use, ensuring that alerts are tailored to the organization's unique needs.

Over time, this lean approach can be scaled into a robust intelligence layer that augments the capabilities of existing SOC and threat response teams, improving both detection and response times.


Lean Public Intelligence Pyramid

Advanced Platforms

Platforms for comprehensive threat intelligence

Intermediate Tools

Tools for OSINT and automation

Foundational Tools

Basic tools for initial intelligence gathering

Conclusion: From Reactive to Resilient

Today's CISOs are not only technologists—they are intelligence leaders. By integrating public breach intelligence into their operations, CISOs can shift from a reactive security posture to a proactive, risk management strategy. Public intelligence provides early warning signals that allow organizations to act before threats escalate, reducing impact and response time.

As threats continue to evolve and regulatory demands grow, public intelligence will become an increasingly essential tool for modern cybersecurity. It's no longer about faster detection—it's about smarter, more adaptive leadership in a fast-moving threat landscape.

About the Author

Aditya Gupta is a cybersecurity leader with over 21 years of global experience, specializing in identity security, breach response, risk management, and cybersecurity transformation. As Industry Principal and Segment Delivery Head for Americas at Infosys, he leads multi-million-dollar security programs for Fortune 100 clients. Aditya has won multiple industry awards, authored thought leadership articles, and served as a judge for global cybersecurity awards. He holds a Bachelor of Engineering and an MBA from FMS Delhi, along with certifications in CISSP, CCSP, and CCNA.

Aditya can be reached online at [LinkedIn]() and https://www.infosys.com

Zero Trust: A Strong Strategy for Secure Enterprise

By Surendra Narang, Senior Manager at Palo Alto Networks

Zero trust frameworks challenge traditional perimeter-based security models by adopting a “never trust, always verify” approach. Unlike legacy security systems, zero trust requires continuous identity verification, strict least-privilege access controls, and persistent monitoring to mitigate threats. Successful zero trust implementation involves a strategic approach that encompasses strong identity and access management (IAM), network security controls, endpoint protection, decryption for traffic visibility, and automated incident response. By enforcing robust security policies using micro-segmentation and leveraging technologies such as multifactor authentication (MFA), secure access service edge (SASE), and extended detection and response (XDR), organizations can enhance their cybersecurity and protect sensitive data from evolving threats.

The five pillars of zero trust

With the arrival of the Internet of Things (IoT), the realities of business needs across global networks, and multi-device remote access norms, legacy perimeter-based security is no longer adequate. Zero trust frameworks rely on a foundation of five pillars: 1) a reduced attack surface area, 2) policy enforcement at the point of request to mitigate risks to data integrity, 3) the application of advanced controls, 4) restricting the access of applications, and 5) ongoing monitoring. In its basic form, zero trust is a logical control that separates asset and control. The asset layer can only be accessed through a control plane via the policy engine, and each request for access to an asset or portion of the network is a policy enforcement point.

Pillar one: Identify attack surface area

An organization's digital presence has changed drastically with the pervasive shift toward edge computing in enterprise networks, where most computing is geographically dispersed. By minimizing the points of network access, resources can be better allocated to defense, and incident response times improved. The identification of access points is a critical concept for reducing the attack surface and focuses on user, device, and application identification. NIST 800-215 SP details the limitations of perimeter-based approaches and offers guidance for the implementation and monitoring of network configurations for contemporary networks.

Pillar two: Enforce least privilege

Least privilege is the premise that only the minimum required access for that role and task is given and no more. The concept of least privilege derives from the separation of duties. Zero trust employs this as the "never trust, always verify" ethos. It's critical to verify each request for access to assets according to a least-privilege principle for the user and task or process through identity and access management (IAM) solutions. If business requirements are clearly defined and roles are assigned through the separation of duties, then least privilege follows and becomes the basis for policy enforcement and verification of IAM.

Pillar three: Apply advanced security controls

The policy engine of zero trust models is an adaptable suite of security tools that can be deployed at the enforcement point and includes identity management, monitoring, analytics, and reporting tools. This flexible engine drives the adaptability of zero trust. It allows integration with diverse security solutions from multiple vendors to customize and optimize enterprise and context-specific security needs. Industry roadmaps such as the Zero Trust Maturity Model leverage zero trust to integrate various security solutions and resources to maintain an edge in security.

Pillar four: Restrict access of application

Micro-segmentation enables zero trust principles to be employed on a more granular level and provides a finer security screen for endpoint security, user access, and application monitoring. Restricting application access to business uses is a priority of zero trust that works to minimize the surface area and contributes to role definition. There is no need to expose the network to all access requests if users are from one region or specific tasks only occur during certain operating hours. Restricting the application decreases network exposure and optimizes the organization's digital presence, reducing incident response times and security complexity.

Pillar five: Monitoring and automation

Zero trust security solutions thrive on ongoing monitoring across zero trust controls, network segmentation, and business processes through data governance to conduct enforcement, verification, and data collection for analysis. These data assets realize internal value through advanced analytics and automation in security and operations. This increased security demands additional resources, and the performance impact of security solutions is best balanced with business needs and available resources. The growing pains of the transition to zero trust frameworks are worth the gains. It is a strategy that provides long-term secure habits on premises and in the cloud, promising adaptability to evolving threat landscapes.

Who is responsible for security?

Due to the increasing interconnection of operational changes affecting the financial and social health of digital enterprises, security is assuming a more prominent role in business discussions. Executive leadership is pivotal in ensuring enterprise security. It's vital for business operations and security to be aligned and coordinated to maintain security. Data governance is integral in coordinating cross-functional activity to achieve this requirement. Executive leadership buy-in coordinates and supports security initiatives, and executive sponsorship sets the tone and provides the resources necessary for program success.

As a result, security professionals are increasingly represented in board seats and C-suite positions. In public acknowledgment of this responsibility, executive leadership is increasingly held accountable for security breaches, with some being found personally liable for negligence. Today, enterprise security is the responsibility of multiple teams. IT infrastructure, IT enterprise, information security, product teams, and cloud teams work together in functional unity but require a sponsor for the security program.

Zero trust security complements operations due to its strict role definition, process mapping, and monitoring practices, making compliance more manageable and automatable. Whatever the region, the trend is toward increased reporting and compliance. As a result, data governance and security are closely intertwined. For example, compliance with the General Data Protection Regulation (GDPR) requires strict monitoring. The data governance and security monitoring practices can overlap in this task and serve a dual function. Ensuring sensitive and confidential data through verified requests, ongoing monitoring, and iterative development enables advanced zero trust data governance.

AI in enterprise security solutions

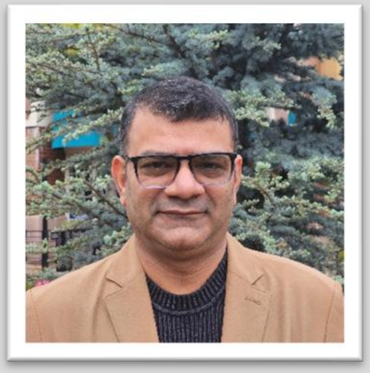
Many companies utilize artificial intelligence (AI) to address their security needs, but AI also presents challenges. AI provides access to significant amounts of data when security practitioners enable large language model (LLM)-based AI. This approach represents a loss of the least privilege pillar buried under the broad access agreements required by the design of LLMs. If the LLM becomes compromised, the entire system is compromised. AI and machine learning can improve workflows, development and remediation times, and provide invaluable analytics insights for incident response and prediction. As threat landscapes evolve, remediation efforts are becoming increasingly essential, particularly in the context of automated cloud service remediation. Remediation advancements are central to zero trust frameworks as security and DevOps work closely to stay ahead of increasingly sophisticated cybercriminals.

Implementation and challenges

The cultural shift to zero trust is an iterative and continual journey. The question of where to start can be daunting, especially for small companies and when the need for security solutions is pressing. Cataloging users, endpoints, applications, and infrastructures is the initial step in defining which business processes, tasks, and roles to utilize in building the pillars for zero trust frameworks. No organization has a 100 percent complete inventory of its digital presence. The inventory process is an ongoing task that involves data management and governance efforts. Zero trust works iteratively and synergistically to achieve greater efficacy in governance and security.

Securing digital assets takes precedence for operations and decision-making. As the security profession matures and enterprise technology advances, the adaptable frameworks of zero trust architecture are the mainstay of contemporary security practices. Security is prominent in C-suite decision-making and a standard feature of budgetary discussions. Securing the organization’s digital presence is a priority that requires resilience and reliability. Zero trust frameworks provide a foundation that can withstand the sophistication of contemporary cybercriminals and leverage emerging technologies. The journey of zero trust is an ongoing practice for securing resilience in modern enterprises.

About the Author



Surendra Narang is a cybersecurity leader with 20 years of experience, currently Senior Manager at Palo Alto Networks. He is responsible for business transformation, information security strategy, and executive-level reporting. He holds a bachelor's degree in applied computing from Boston College and a master's in applied computing from the Institute of Advanced Technology and Science. Connect with Surendra on LinkedIn.

EVENTS

Infosecurity® Europe | 3-5 June 2025 ExCel London

Building a Safer Cyber World

Infosecurity Europe is one of the leading European cybersecurity events, hosting over 13,000 cyber professionals and over 380 vendors each year.

Witness innovation firsthand: Test and benchmark solutions, and make informed product choices by meeting top exhibitors on our show floor.

Be inspired by industry experts: Our new and improved conference programme will equip you with the insights you need to counter threats and prevent data breaches.

Build valuable connections: Grow meaningful relationships with our wide range of networking opportunities, including roundtables, workshops and 1:1 meetings.

Expand your knowledge: Learn valuable new skills, attend immersive tutorials, and earn CPE & CPD credits to advance your career in cybersecurity.

REGISTER NOW →

www.infosecurityeurope.com

Built by RX In the business of building businesses

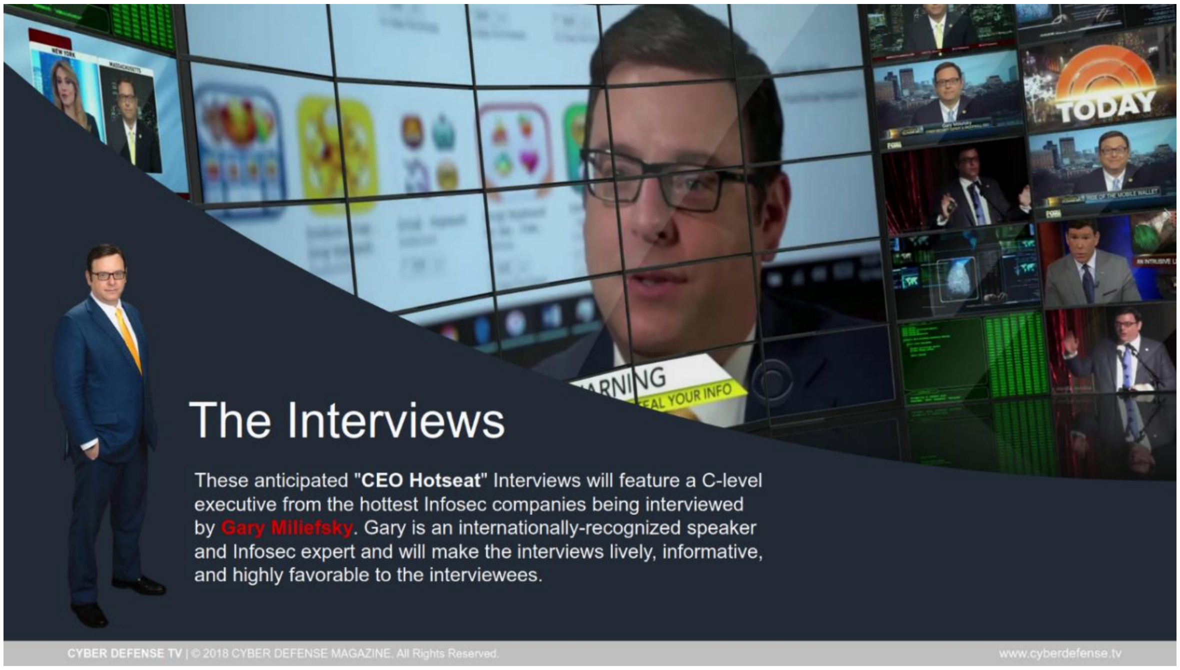
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



The Interviews

These anticipated "**CEO Hotseat**" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by Gary Miliefsky. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

TODAY
WARNING
STEAL YOUR INFO
CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved.
www.cyberdefense.tv

Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Copyright (C) 2025, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com,and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com

Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

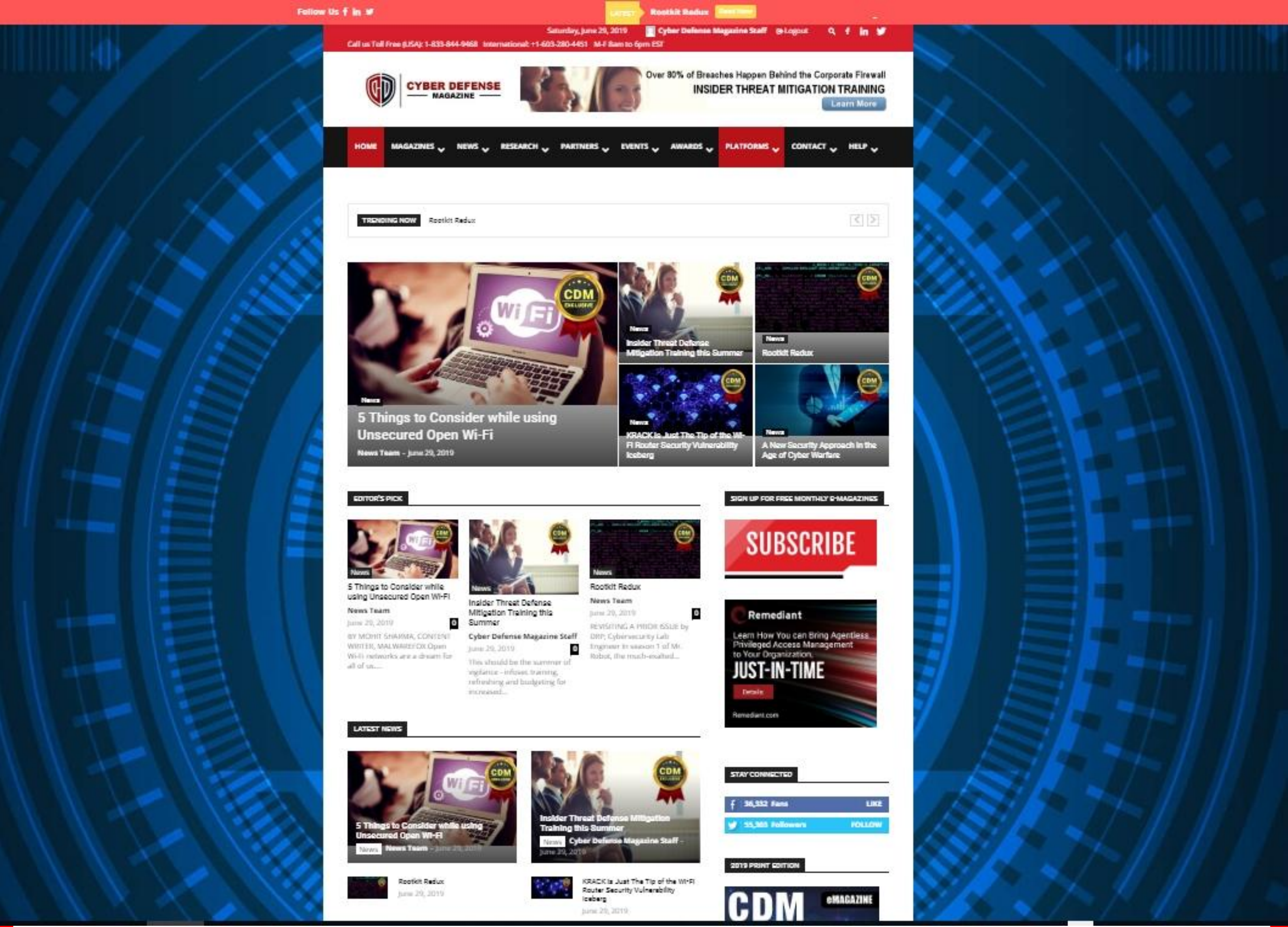
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

https://www.cyberdefensemagazine.com/

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 06/02/2025


Follow Us
LATEST Rootkit Redux
Saturday, June 29, 2019 Cyber Defense Magazine Staff Logout
Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST
CYBER DEFENSE MAGAZINE
Over 80% of Breaches Happen Behind the Corporate Firewall
INSIDER THREAT MITIGATION TRAINING
Learn More
HOME
MAGAZINES
NEWS
RESEARCH
PARTNERS
EVENTS
AWARDS
PLATFORMS
CONTACT
HELP
TRENDING NOW Rootkit Redux
5 Things to Consider while using Unsecured Open Wi-Fi
News Team - June 29, 2019
Insider Threat Defense Mitigation Training this Summer
Rootkit Redux
KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
A New Security Approach in the Age of Cyber Warfare
EDITOR'S PICK
SIGN UP FOR FREE MONTHLY E-MAGAZINES
SUBSCRIBE
Remediant
Learn How You can Bring Agentless Privileged Access Management to Your Organization.
JUST-IN-TIME
Details
Remediant.com
LATEST NEWS
STAY CONNECTED
LIKE
FOLLOW
2019 PRINT EDITION
CDM eMAGAZINE

Books by our Publisher: [Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook : Miliefsky, Gary: Kindle Store, Kindle Store, Cybersecurity Simplified, The AI Singularity: When Machines Dream of Dominion with others coming soon...]

13 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and [CyberDefenseMagazine.com] up and running as an array of live mirror sites. We successfully launched [https://cyberdefenseconferences.com/] and our new platform [https://cyberdefensewire.com/]

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
eMAGAZINE
www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."
Gary S. Miliefsky, Publisher & Cybersecurity Expert

Shadow IT May Leave You at Risk.

Unauthorized or unknown internet-facing assets in your network can expose sensitive defense information to our adversaries.

NSA's no-cost cybersecurity services can help you find and protect your assets to better secure your network.

GET STARTED TODAY AT
nsa.gov/ccc

NATIONAL SECURITY AGENCY ★ UNITED STATES OF AMERICA ★

CYBERSECURITY COLLABORATION CENTER

* with help from writers
and friends all over the Globe.