



CYBER DEFENSE
MAGAZINE

2025 SPECIAL EDITION

RSAC | 2025
Conference

Welcome to CDM's RSAC Conference 2025 Special Edition

The 34th annual RSAC™ Conference kicks off on April 28 in San Francisco, where we'll come together to celebrate "**Many Voices. One Community.**" This year, we're embracing the strength that comes from uniting the community under a common goal: a safer digital world for all.

The challenges we face in cybersecurity are more complex and multifaceted than ever. But the answer has always been the same—*we're stronger together*. From the brightest minds in the industry to the emerging voices driving innovation, our collective expertise, shared experiences, and different ideas are what make us resilient. As we look toward the future, this theme of unity is more than a rallying cry; it's the blueprint for progress.

At RSAC™ 2025 Conference, we're proud to offer a space where these many voices can be heard, where collaboration can spark the next breakthrough, and where every participant can contribute to shaping the future of cybersecurity. Whether you're attending to learn, network, or share your own insights, we're all part of something bigger.

As we continue our mission to empower cybersecurity professionals worldwide, we know that knowledge and relationships are the keys to progress. From in-depth sessions to hands-on workshops, we offer the resources you need to tackle today's challenges and prepare for the unknowns of tomorrow. The learning doesn't stop after the Conference, either. With the RSAC™ Membership, our commitment to year-round education means you have access to a wealth of content, tools, and connections throughout the year.

Take full advantage of the many opportunities to connect with others throughout the week—from the Welcome Reception to the dynamic networking events in the Expo. It's in these moments of exchange that our community truly thrives. The relationships you build here can become lasting partnerships that help you, your team, and your organization succeed in an ever-evolving digital landscape.

I look forward to seeing you soon at RSAC™ 2025 Conference!

Warm regards,

Linda Gray Martin
Chief of Staff, RSAC & Senior Vice President
RSAC™ Conference



RSAC | 2025 Conference

Contents

Welcome to CDM's RSAC Conference 2025 Special Edition	2
The Global InfoSec Awards for 2025	10
Women In Cybersecurity Scholarship Fund Sponsorship Packages for 2025	16
The Current by Deloitte	25
<i>By Andrew Berg, US Identity & Access Management (IAM) Solution Offering Leader Principal at Deloitte & Touche LLP</i>	
How can Organizations Secure Low-Code No-Code Development	29
<i>By Aparna Achanta, Principal Security Architect at IBM Federal Consulting</i>	
Preparing for the Quantum Age: What Security Leaders Need to Know Now	33
<i>By Jason Rader</i>	
Navigating the Future of Network Security with Secure Access Service Edge (SASE).....	36
<i>By Akarsh Jain, Product Marketing Manager for SASE, Sangfor Technologies</i>	
Red Piranha's Unified Approach to Modern Threat Defense	43
<i>By Adam Bennett, CEO, Red Piranha</i>	
Rethinking Vulnerability Prioritization	50
<i>By Omer Tal, Security Researcher in the CTO Office at Seemplicity</i>	
Endpoint Security In 2025	55
<i>By Namrata Barpanda, Staff Information Security Engineer, ServiceNow INC</i>	
The Essential Guide to Third-Party Risk Management (TPRM)	60
<i>By Dasha Davies, President/CISO, Stealth-ISS Group Inc.</i>	
Cognitive Domain Monitoring, Analysis and Control.....	66
<i>By Fernando Escudero, Marketing and Communications, ISID</i>	
Addressing The Need for Integrated FICO-DT Scoring for All Digital Services	70
<i>By Lalit Ahluwalia, CEO & Founder, DigitalXForce & iTrustXForce</i>	

Bridging The Cybersecurity Skills Gap: Why Partnering with An MSSP Is A Strategic Imperative	76
<i>By Sachin Jain, Sr. Vice President Technology, Eventus Security</i>	
Streamlining PCI DSS 4.0.1 Adoption in 2025	81
<i>By Héctor Guillermo Martínez, President of GM Sectec</i>	
Next-Generation Data Protection: What Is it? Why Should Enterprise Tech Buyers Care?	86
<i>By Eric Herzog, CMO of Infinidat</i>	
Cyber Risks Associated with Adoption of Generative AI Tools	90
<i>By Dustin Hutchison, Senior Vice President of Services and CISO, Pondurance</i>	
7 Benefits of Using RPAM In Multi-Cloud Security	95
<i>By Roy Kikuchi, Director of Strategic Alliances at Safous, Internet Initiative Japan (IIJ) Inc.</i>	
Wielding AI As a Teammate in Cybersecurity	101
<i>By Dan Cole, VP of Product Marketing, ThreatConnect</i>	
The Art and Science of Being a CISO	105
<i>By Ira Winkler, Vice President & Field CISO, CYE</i>	
3 Reasons Onion Routing is Required for 'Truly' Secure Messaging.....	110
<i>By Kee Jefferys, Co-Founder of Session</i>	
Building a Resilient Cyber Ecosystem.....	113
<i>By Blake Benson, Senior Director, Cybersecurity Practice Lead for ABS Consulting</i>	
All-Time High: Confronting The Escalating Threat of Medical Data Breaches.....	116
<i>By Scott Speranza, CEO of HealthLock</i>	
Beyond Zero Trust: How to Eliminate Backup Access and Elevate Your Cyber Security.....	120
<i>By Robert Marett, Chief Technology Officer, Cobalt Iron</i>	
Browser Security Must Anchor Your Defense Strategy	125
<i>By Dakshitaa Babu, Security Researcher, SquareX</i>	

How Critical Infrastructure Can Prepare for an Uptick in Cyberattacks in 2025	127
<i>By Dr. Bill Anderson, Principal Product Manager, Mattermost</i>	
Deep Learning-Based Solutions Help Enterprises Avoid Zero-day Attacks	130
<i>By Dave Floyd, Vice President of Cybersecurity Sales and Service, Hughes Network Systems</i>	
Securing Success in a Data-Driven World	133
<i>By Yoav Regev, CEO and Co-Founder, Sentra</i>	
Lights, Camera, Safety - The Video Surveillance Revolution	136
<i>By Freddy Kuo, Chairman, Luminy</i>	
Customer Trust Is a Business Imperative: It's Not Enough to Just Protect Customer Data, Businesses Must Show Proof of Their Efforts as Well.....	142
<i>By Sam Rehman, Chief Information Security Officer, SVP at EPAM Systems, Inc.</i>	
Cyber Security Threats vs. Insider Threats	146
<i>By Jim Henderson, Founder / Chairman of the National Insider Threat Special Interest Group (NITSIG) CEO Insider Threat Defense Group, Inc. (ITDG)</i>	
Cybersecurity Due Diligence in Mergers and Acquisitions: Essential Focus Areas.....	149
<i>By Tom Cockriel, co-leader of Trenam Law's Business Transactions practice group, Trenam Law</i>	
Dark Web Threats: How Your Data Is Compromised and Monetized by Cybercriminals	154
<i>By Ankit Sharma, Senior Director and Head - Solutions Engineering, Cyble</i>	
DeepSeek's AI Revolution: Cost Efficiency Meets Security Concerns	158
<i>By Alix Melchy, VP of AI at Jumio</i>	
Fake REAL Ids Have Already Arrived, Here's How to Protect Your Business	161
<i>By Jillian Kossman, Vice President of Marketing & Policy, IDScan.net</i>	
Five Crucial Insights to Combat Today's Deepfake Phenomenon.....	166
<i>By Dominic Forrest, Chief Technology Officer, iProov</i>	
From Factory Floor to Second Life: Why Platform Security Must Be Managed Throughout the Lifecycle of a Device	170
<i>By Boris Balacheff, Chief Technologist for Security Research and Innovation at HP Inc.</i>	

The Future of Automotive Cybersecurity Safeguarding the Next Generation of Mobility.....	174
<i>By Bhushan Dhumal</i>	
How to Adopt Advanced Edge Cybersecurity to Protect Smart Buildings	178
<i>By Fabio Zaniboni, Founder & Chief Executive Officer at BubblyNet</i>	
How To Leverage Cloud Analytics to Detect and Prevent Cybersecurity Threats in Real-Time	182
<i>By Laurence Dale, CISO, Surveil</i>	
How to Stop Infostealers and Next-Gen Ransomware with an Identity-Centric Security Approach	185
<i>By Trevor Hilligoss, SVP of Security Research, SpyCloud Labs at SpyCloud</i>	
How To Strengthen the Security of Your Symphony-Based Solution.....	189
<i>By Roman Davydov, Technology Observer, Itransition</i>	
How to Use Risk Management to Strengthen Business Cybersecurity	193
<i>By Taylor McKnight, Digital PR Specialist for CLDigital</i>	
Implementing Effective AI Guardrails: A Cybersecurity Framework	196
<i>By Sourabh Satish, Co-Founder & CTO of Pangea</i>	
Scaling Smart: Federal Leaders Prioritize AI Security and Resilience	201
<i>By MeriTalk Staff</i>	
Modernizing Critical Infrastructure Security to Meet Today's Threats	204
<i>By John Kindervag, Chief Evangelist and Creator of Zero Trust, Illumio</i>	
One Piece of the Puzzle: How a Single Digital Identifier Can Unravel Your Entire Online Life	208
<i>By Raphael Marchand, CEO, ChatOdyssey</i>	
On Constant Community Improvements	214
<i>By Maxime Lamothe-Brassard, Founder and CEO, LimaCharlie</i>	

Securing the Connected Factory Floor	217
<i>By Almog Apirion, CEO and Co-Founder of Cyolo</i>	
Small Manufacturers, Big Target: The Growing Cyber Threat and How to Defend Against It	221
<i>By Brian Winters, Chief Technology Officer, ECI Software Solutions</i>	
The Cost of Ignoring Patches: How State and Local Governments Can Mitigate Damaging Security Breaches	225
<i>By Joao Correia, Technical Evangelist, TuxCare</i>	
The Growing Threat of AI-powered Cyberattacks in 2025	228
<i>By Stephen Kines, COO and Co-Founder of Goldilock</i>	
The Impact of Quantum Decryption	232
<i>By Alyssa Walton, Senior Information Security Analyst, Deep Dive Cyber</i>	
Ongoing Money Laundering Insights	239
<i>By Milica D. Djekic, Independent Researcher, Subotica, Serbia</i>	
The Quantum Supply Chain Risk: How Quantum Computing Will Disrupt Global Commerce	243
<i>By Blake Lazarus, Security Insights Contributor, Zeroproof</i>	
The Rise of Identity Risk Intelligence.....	246
<i>By Andres Andreu, COO and CISO, Constella Intelligence</i>	
The Rising Deepfake Risk for Businesses: A Step-By-Step Defense Strategy Built Around the Basics of Security	251
<i>By Matthew Martin, CEO, Two Candlesticks</i>	
The Digital Pandemic: Inside 2024's Most Devastating Cyber Breaches	254
<i>By Ashwany Pillai, Global Head of Marketing, Network Intelligence</i>	
The Evolving Cloud Security Landscape: Empowering Startups in a Post-Acquisition World	257
<i>By Allan Thompson, CEO & President, AcceleTrex Corporation</i>	

Why CISOs Need an AI-Native Strategy 261

By Tom Tovar, CEO, Appdome

Why Network Disaster Recovery Solutions Are a Non-negotiable for Modern Businesses.. 264

By Howard Simpson, CTO, CENTREL Solutions

Why Scale Matters in Today's Cybersecurity Landscape Futureproofing for Better Outcomes 267

By Glen Williams, CEO, Cyberfort

How to Use Open-Source AI in Defense Tech: Cybersecurity Safeguards for Developers ... 270

By Yuliia Verhun, Technology & Business Lawyer, General Counsel for Tech Startups

Zero-Trust Architecture in the Era of Quantum Computing: A Proactive Defense Strategy . 274

By Dinesh Besiahgari, FrontEnd Engineer II, Amazon Web Services

The background of the left half of the page is a dark blue abstract graphic. It features a stylized globe on the right side, partially obscured by a complex network of glowing blue and green lines and dots, resembling a digital or cybernetic theme. The overall shape of the graphic is roughly triangular, pointing towards the top left.

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): +1-646-586-9545
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

Copyright © 2025, Cyber Defense Magazine
(CDM), a Cyber Defense Media Group (CDMG)
publication of the Steven G. Samuels LLC Media Corporation.

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

Welcome to CDM's RSAC Conference 2025 Special Edition

From the Editor's desk, we are delighted to present this combined RSAC™/May 2025 issue of Cyber Defense Magazine. The RSAC™ theme of "Many Voices, One Community" is reflected in the continued broadening of our publication's topics.

As our readership grows and includes both cybersecurity professionals and many non-technical readers, our contributing authors have expanded the subjects of their articles. Fortunately, we also continue to enjoy an increasing number of submissions, to the benefit of our entire audience.

This issue's focus on the RSAC™ Conference and articles contributed by RSA participants once again brings home to us the importance of recognizing the topics of primary interest to practitioners of cybersecurity, as well those who support their efforts.

Rapid growth in various types of artificial intelligence, leading to greater cyber risks and risk management needs, including prevention, insurance coverage, and recognition of new threats, are echoed in the submissions we receive from within the profession.

As always, we strive to be the best and most actionable set of resources for the CISO community in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group. With appreciation for the support of our contributors and readers, we continue to pursue our role as the premier provider of news, opinion, and forums in cybersecurity.

Wishing you all success in your cybersecurity endeavors,

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the Author

Yan Ross, J.D., is a Cybersecurity Journalist & 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



The Global InfoSec Awards for 2025

As we go to press on this annual RSAC issue of Cyber Defense Magazine, on behalf of Cyber Defense Media Group, we celebrate our strong relationship with the RSA Conference organization. Among the many valuable services and affiliations, we enjoy, the RSA connection is one of our most important.

It is with great pleasure that we dedicate this RSAC/May 2025 issue of Cyber Defense Magazine to our support and participation in the RSAC Conference set for April 28 - May 1, 2025, in San Francisco.

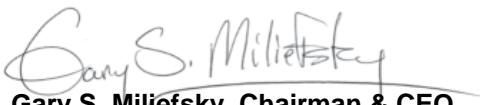
We have worked diligently at our end to produce one of the largest and most comprehensive issues of Cyber Defense Magazine in our 13-year history. With dozens of articles from cyber security professionals, many of them planning to attend RSAC 2025, we continue to grow in distribution and actionable intelligence for our contributors and readers. We continue to monitor closely and respond to the needs of our audience.

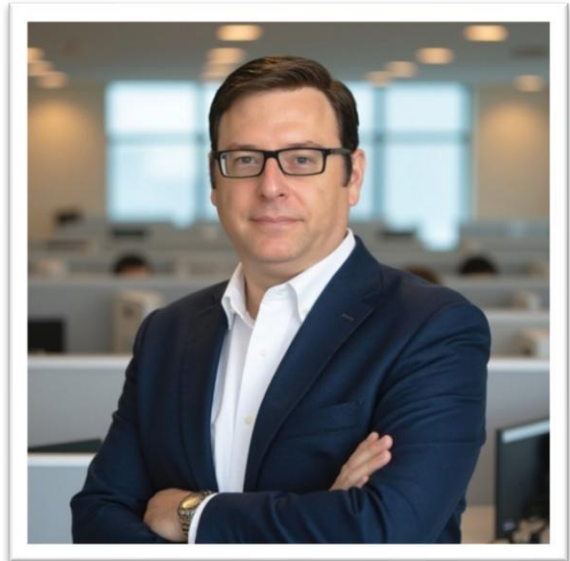
Accordingly, the scope of CDMG's activities has grown into many media endeavors to meet these growing needs. We offer Cyber Defense Magazine, Cyber Defense Awards; Cyber Defense Conferences; Cyber Defense Professionals (job postings); Cyber Defense TV, Radio, Wire and Webinars. The full list, with links, can be accessed at:

<https://www.cyberdefensemagazine.com/cyber-defense-media-group-13-year-anniversary-2025/>

Cybersecurity is on the front line of the ongoing protection of our economy and critical infrastructure. It's no surprise that there are now hundreds of thousands of career openings and unlimited opportunities for those who wish to make a positive impact on today's digital world. Cyber Defense Media Group is dedicated to providing information and tools for professionals to create resilient and sustainable cyber systems.

Congratulations to all our winners!


Gary S. Miliefsky, Chairman & CEO
Cyber Defense Media Group
Publisher, Cyber Defense Magazine



Award Winners



About The Global InfoSec Awards

This is Cyber Defense Magazine's thirteenth year of honoring InfoSec innovators from around the Globe. Our submission requirements are for any startup, early stage, later stage, or public companies in the INFORMATION SECURITY (INFOSEC) space who believe they have a unique and compelling value proposition for their product or service. Learn more at www.cyberdefenseawards.com

About the Judging

The judges are CISSP, FMDHS, CEH, certified security professionals who voted based on their independent review of the company submitted materials on the website of each submission including but not limited to data sheets, white papers, product literature and other market variables. CDM has a flexible philosophy to find more innovative players with new and unique technologies, than the one with the most customers or money in the bank. CDM is always asking "What's Next?" so we are looking for best of breed, next generation InfoSec solutions.

Award Winners Listed by Category

Award Winners Listed by Company

Award Winners



Women in Cybersecurity Scholarship Winners

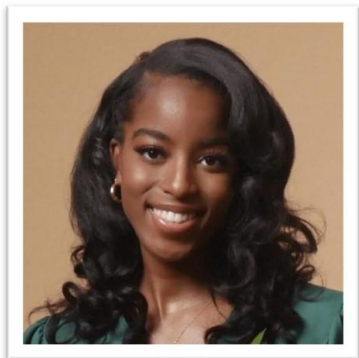
The Young Women in Cybersecurity Scholarship, provided by Cyber Defense Awards, is a multi-staged scholarship opportunity for young women in cybersecurity who are in college or planning to attend college for a degree in cybersecurity.

The benefits of the scholarship include cash scholarship funding to help cover the cost of tuition, fees, and other expenses related to their cybersecurity education or career development. We provide opportunities to travel, expenses paid, to major cybersecurity conferences like RSAC, BlackHat, Defcon, and CyberDefenseCon to network with other women in cybersecurity and industry leaders. Prior winners can provide mentorship to new winners.

As a member of our community, winners are part of a growing network of women who are working to make cybersecurity a more inclusive and diverse field.

[Learn more...](#)

About Victoria Hargrove



Victoria is a 2024 graduate of George Mason University, where she earned a Bachelor of Science in Management Information Systems. Her academic journey included a comprehensive focus on cybersecurity, with coursework in networks and security, information security and assurance, programming, and networking, among other areas. Building on this foundation, she will begin her Master's degree in Cybersecurity at Old Dominion University in the spring, while concurrently pursuing the CompTIA Security+ certification.

Currently employed as a full-time Security Analyst at TJX Companies, Victoria's role involves critical responsibilities such as identifying security threats, investigating phishing attacks, and remediating various security issues. Her experience in these areas allows her to apply her theoretical knowledge to real-world challenges, positioning her as a skilled professional in the cybersecurity domain.

In addition to her academic and professional goals, Victoria is deeply committed to community engagement, particularly in supporting underrepresented groups in technology. She believes that education is a powerful tool for creating opportunities, and she is passionate about mentoring and outreach. In her own words: "Education has opened doors for me, and I aspire to do the same for others. Mentorship and outreach for underrepresented groups in technology is something I'm passionate about. I know true success is measured by how much we can lift others as we climb."

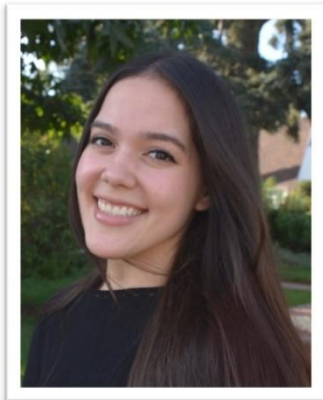
As she continues to advance her knowledge and expertise, Victoria remains eager to engage in research and tackle the evolving challenges of the cybersecurity landscape.

Winning this cybersecurity scholarship for graduate school will allow me to take a transformative step in my journey to becoming a leader in the field. As someone with a Bachelor's degree in Management Information Systems and working as a Security Analyst, I have already seen firsthand the impact of cybersecurity on businesses and individuals. This scholarship will enable me to pursue a Master's in Cybersecurity at Old Dominion University, where I plan to deepen my understanding of network security, risk management, and digital forensics.

The financial support will also allow me to focus fully on my studies, gaining the advanced knowledge and skills needed to contribute meaningfully to the field. Additionally, earning this scholarship has inspired me to continue my outreach efforts in advocating for underrepresented groups in technology. I am passionate about creating opportunities for others to break into this vital field and believe that more diverse voices can only strengthen our industry's ability to address evolving cyber threats.

With the knowledge gained from graduate school, I intend to develop innovative solutions that can protect critical systems, not just for businesses but for society as a whole. Winning this scholarship is an incredible honor, empowering me to fulfill my potential and make a lasting impact.

About Angela Apolinar



I am incredibly thrilled and excited to be awarded the Cyber Defense Magazine Women in Cybersecurity scholarship. This recognition not only supports my ongoing master's studies in Cybersecurity and Information Assurance at Western Governors University, but it also strengthens my resolve to make meaningful contributions to the cybersecurity field. With this opportunity, I am more driven than ever to help safeguard digital infrastructure and inspire more women to enter and excel in this vital industry. I look forward to using this platform to continue expanding my knowledge and skills!

Angela Apolinar is a first-generation college graduate with a Bachelor's degree in psychology from Cal State Fullerton. With a growing fascination for technology, she transitioned to the study of cybersecurity. Since then, she has earned certifications in Information Technology, Cyber Defense, Cybersecurity, and Cisco Networking from CompTIA, Cisco, and Cypress College. She is advancing her expertise by pursuing a Master's in Cybersecurity and Information Assurance at Western Governors University.

Angela has demonstrated exceptional leadership throughout her academic career, notably as her college's first female Computer Science and Cybersecurity Club president. In this role, she organized workshops and events that featured speakers from prominent organizations such as the FBI and AWS. Her commitment to mentorship and education is further exemplified by her position as a Cyber Mentor and Professor's Assistant at Cypress College.

Currently a NASA Aerospace Scholar, she is diving into the world of space exploration and technology. Through this program, Angela is gaining invaluable insights into NASA's cutting-edge technologies, space exploration strategies, and the role of cybersecurity in protecting critical systems that support these missions.

Her dedication to cybersecurity, leadership, and mentorship roles reflect her commitment to shaping a more secure and inclusive tech landscape. As she continues to grow in her field, Angela remains passionate about empowering the next generation of women and underrepresented groups in STEM, proving that with determination and vision, the sky is truly not the limit—it's just the beginning!

Women In Cybersecurity Scholarship Fund Sponsorship Packages for 2025



Empower the Future of Cybersecurity:

[Become a Scholarship Partner Today!](#)

Meet prior winners and help us continue to sponsor them and new winners this year:





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



AN INTEGRATED GLOBAL, STAGE-AGNOSTIC CYBERSECURITY
INVESTMENT PLATFORM SPANNING SEED THROUGH
GROWTH.

The first dedicated cybersecurity venture firm in the world

About us

For 20 years, AllegisCyber Capital has offered a proven investment platform that actively engages with the most promising entrepreneurs in cyber and delivers the market access, team building, and operating experience essential to their success.

BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER



www.allegiscyber.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

2012

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

2014

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

2016

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

2018

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

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

2013

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

2015

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

2017

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

2020

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



"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

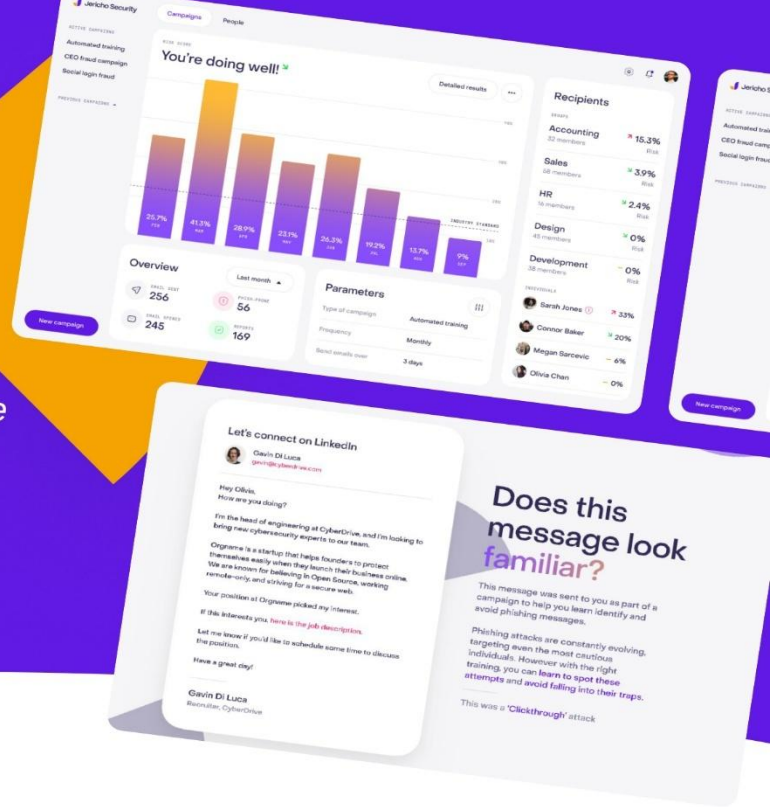
We monitor the
DARKWEB
so that your
BUSINESS has
no stops



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.



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

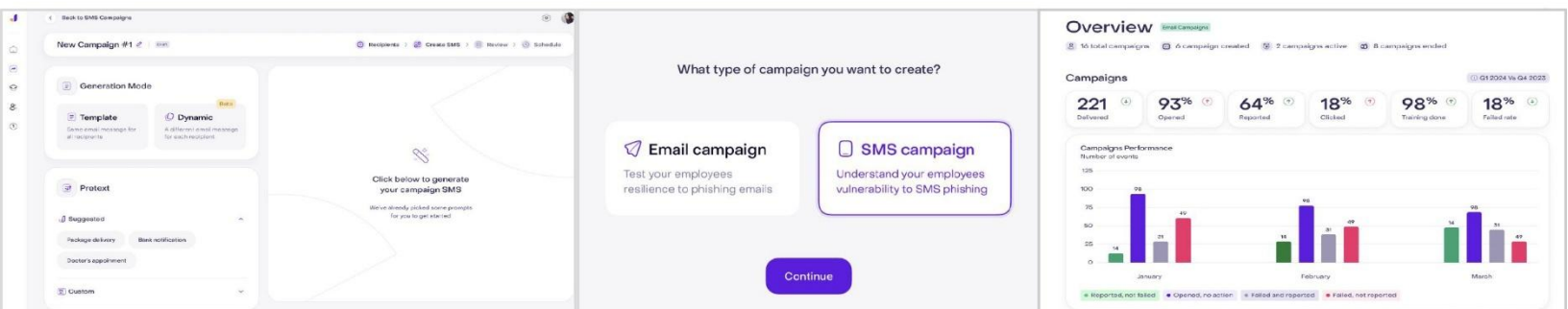
Dynamically customize training based on employee risk profiles and attack patterns, ensuring tailored, effective learning experiences.

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.



Secure Agentic AI with Cequence

AI agents' autonomous decision-making capabilities present unique security challenges that traditional measures may not fully address. Fortify your AI use against emerging threats with Cequence.



**Go to cequence.ai/assessment
or scan the QR code
to start a free assessment
of your vulnerabilities.**





CYBER DEFENSE — MAGAZINE —

WHERE INFOSEC KNOWLEDGE IS POWER



www.cyberdefensetv.com

www.cyberdefenseradio.com

www.cyberdefenseawards.com

www.cyberdefenseconferences.com

www.cyberdefensemagazine.com



The Current by Deloitte

Trusted news and views on cybersecurity

What Does Identity Security Look Like In 2025?

Our [joint survey with SailPoint](#) reveals the latest identity security insights from 400+ executives.

**By Andrew Berg, US Identity & Access Management (IAM) Solution Offering Leader
Principal at Deloitte & Touche LLP**

Plus, a Q&A with Chris Gossett, Chief Growth Officer at SailPoint

As threats such as phishing, social engineering, and malware grow in complexity, cyber professionals should evolve identity security practices to better protect user data. [Deloitte and SailPoint conducted a survey](#) of more than 400 executives across a diverse range of industries to understand how they'll respond to increasing risk in the coming year.

The takeaway? Cyber executives are ready to grow their identity programs, but they're facing bottlenecks. The report looks at some of the key challenges and how leaders can overcome them with AI-driven solutions.

Insights into Identity Security: SailPoint and Deloitte Survey

Identity security survey highlights

- **Phishing is the No. 1 threat, according to respondents**
- **75% of respondents plan to adopt an AI-driven solution**
- **50% rate their identity management as mature**

Currently speaking

Q&A with Chris Gossett, Chief Growth Officer at SailPoint

With identity-based threats on the rise, how do you see the role of identity security evolving in modern cybersecurity strategies?

Identity security has gone from being just one piece of cybersecurity to being the foundation. Attackers aren't breaking in anymore—they're logging in and using stolen credentials, over-permissioned accounts, or AI-driven phishing attacks that are scarily convincing.

The future of cybersecurity is about identity-first security. That means enforcing least privilege access, so access isn't accumulating over time, and managing every identity—whether it's human, bot, or AI. Organizations also need full visibility into who has access to what across all applications. If you don't know that, you're flying blind. In 2025, protecting identity is protecting the business.

Many organizations are shifting to an 'identity-first' security approach. What challenges do organizations face in implementing this model, and how can they address them?

One big challenge? Cultural resistance. Businesses and people don't love having their access restricted, even if it's for security. A fix? Strong identity governance-automated least privilege enforcement and clear communication. Show teams that tighter identity controls aren't about slowing them down—they're about keeping organizations safe.

The survey indicates that AI is playing a growing role in identity governance. How can organizations leverage AI for identity threat detection and risk mitigation?

AI in identity governance is like having a security guard who never sleeps, never takes coffee breaks, and understands your environment better than you do. One of the biggest challenges in identity security

is knowing exactly what access an identity should have—and enforcing that across every application in the enterprise. Manually managing this at scale is impossible, which is why AI-powered solutions are becoming essential. AI can analyze patterns, detect excessive permissions, and automate least privilege enforcement, reducing the attack surface. Without AI, organizations sometimes guessed—and in cybersecurity, guessing can result in something being missed.

With the increasing sophistication of insider threats, what measures should organizations take to balance security with user experience while managing internal access controls?

Insider threats are tough—because these users already have access. Lock things down too much, and productivity grinds to a halt. Leave things too open, and you're inviting risk. The key is making sure the business understands why users have the access they do. That starts with clear entitlement and role descriptions—so there's no guesswork about who needs what. Organizations also need to prevent access creep—employees shouldn't accumulate permissions as they change roles. And with privileged accounts, bots, and AI agents expanding the attack surface, it's critical to map out effective access across identities, not just humans.

What are the key metrics or indicators you recommend measuring the effectiveness of an identity security program?

Measuring identity security isn't just about counting how many accounts you've locked down—it's about understanding who has access to what and whether that access makes sense. Some key metrics to track:

- Percentage of users with least privileged access: Are employees only getting the access they actually need?
- Access creep rate: How often do users retain old permissions when they change roles?
- Time to revoke access: How quickly are accounts deprovisioned when someone leaves or changes jobs?
- Privileged access visibility: Do you know who owns, the purpose and access for every privileged account, including bots and AI agents?
- Orphaned accounts: How many unused accounts are floating around, waiting to be exploited?
- Percentage of applications under identity management: How many apps are actually covered by identity security controls? If you're only managing a fraction, the rest are blind spots.

If you're not tracking these, you're not measuring identity security—you're just hoping for the best.

In the next issue: Resiliency reimagined

Uncover strategies and solutions to help your business prepare for, respond to, and recover from disruptions.

[Subscribe to The Current](#)

Sign up for our monthly newsletter to keep pace with the latest in cybersecurity strategies, insights, news, and views.

About the Author

Anthony Berg is a principal in Deloitte's Cyber practice, serving as the Solution Offering Leader for Identity & Access Management (IAM). He focuses on helping clients secure their enterprises by enabling trusted identities in a connected and open world. With more than 15 years at Deloitte, Anthony oversees IAM strategy, revenue growth, talent development, technology innovation, and key client relationships.

[Anthony Berg](#)

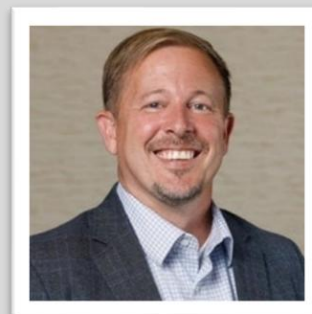
US Identity & Access Management (IAM) Solution Offering Leader

Principal

Deloitte & Touche LLP

antberg@deloitte.com

[+1 404 395 6340](tel:+14043956340)





How can Organizations Secure Low-Code No-Code Development

By Aparna Achanta, Principal Security Architect at IBM Federal Consulting

Applications developed by citizen developers are on the rise. Low-code and no-code (LCNC) platforms are reshaping the development ecosystem. These tools are broadening horizons and enabling citizen developers to create powerful applications.

LCNC development is a way of developing apps in which developers use existing system design elements that can be added onto a visual interface.

These platforms focus on swift development that can automate processes, empowering users with minimal or no technical knowledge to build their apps innovatively.

However, security is not often at the forefront of app development when using LCNC platforms, as business users often lack a strong understanding of secure development methods.

Strategies to Secure LCNC Platforms

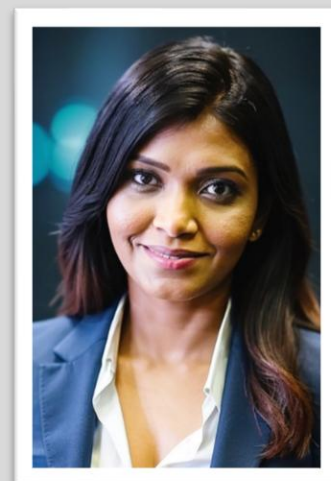
A breach of the LCNC platform could result in financial losses, damage to the organization's reputation, and violation of compliance regulations. Below are some ways in which the security of the LCNC platforms can be preserved-

1. **LCNC vendor assessment:** Before procuring an LCNC platform, the organization's security team must review the vendor's security policies, data backup and recovery policies, and controls for securing the platform against vulnerabilities. Organizations should have an inventory of approved LCNC tools vetted by the security teams and prevent employees from installing and using unapproved LCNC tools that can expose the organization to compliance and security risks.
2. **Citizen Developer Training:** Before building apps, citizen developers must thoroughly familiarize themselves with the LCNC tool and its security best practices.
3. **Identity management:** Organizations can implement Single Sign-On (SSO) with multifactor authentication (MFA) so that users use a single password to log in to the network but confirm their identity every time they log in to the LCNC application, thereby ensuring security.
4. **Access management:** Enforce role-based access in all environments in combination with the principle of least privilege to bolster overall security. System administrators must assign administrator privileges to only a few citizen developers who have taken the organization's security training and monitor user accounts to track for suspicious behavior.
5. **Enforce Static and dynamic application security testing:** Technical developers can perform static and dynamic application scanning to ensure no new vulnerabilities have been introduced in citizen-developed applications.
6. **Incident response plan:** Create a robust incident response plan and execute the tabletop exercises, simulation attacks, and testing included in the plan to prepare for threats or security incidents.
7. **Push the latest updates and security patches:** Technical developers need to update the LCNC tools with the latest vendor patches, as these provide fixes for code flaws. **Conclusion**

As Low-code and no-code (LCNC) platforms reshape the development ecosystem, it's important to assure that developers and users of LCNC platforms integrate appropriate security strategies into their application.

About the Author

Aparna Achanta is a Principal Security Architect at IBM Federal Consulting. Aparna oversaw mission-critical projects for US Federal Agencies. While at IBM, she successfully implemented the Zero Trust framework in federal agencies. Aparna spearheaded the Center of Excellence for SaaS applications at federal agencies like Department of Veterans Affairs, which is tasked with implementing the Zero Trust framework, thereby enhancing the security posture of these agencies. This Center of Excellence equips numerous citizen developer professionals with the necessary tools and security and governance frameworks to develop applications using low-code, no-code platforms, such as Power BI and Microsoft Co-Pilot, and establishes guidelines to ensure the responsible and secure implementation of GenAI apps. Aparna also established an Architecture Review Board for D365 and Power Platform applications, defining security requirements and shaping application architecture best practices for development teams. With 10+ years of experience, Aparna has designed secure digital transformation projects for large federal clients that have greatly streamlines processes. Aparna is a motivated person who is committed to giving back to the cybersecurity industry. She is an active mentor, author, peer reviewer, and speaker.

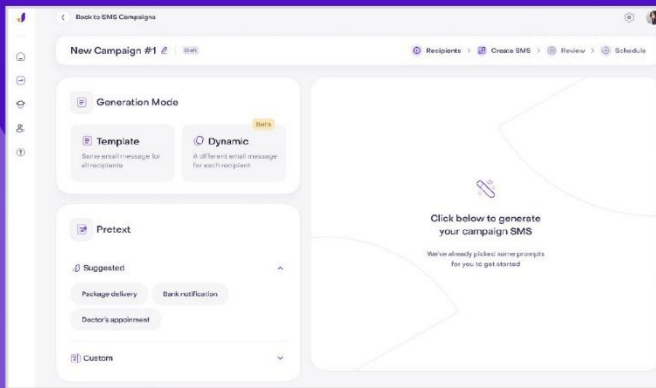


Aparna can be reached online at her website <https://aparnaachanta.com/> or her LinkedIn <https://www.linkedin.com/in/aparna-achanta-41741739/>

Meet Jericho Security.

The World's First Agentic AI for Real-World Phishing Defense

Empower employees to detect conversational phishing **by simulating real-world threats**



Analyze employee responses to identify risk and readiness and further fine-tune simulations

Manage your organization's security actions & performance **from a single dashboard**



Simulate real-world threats, gain deep insights, and scale your security

Start your 7-day free trial today:
jerichosecurity.com/free-trial



Preparing for the Quantum Age: What Security Leaders Need to Know Now

By Jason Rader

The race toward quantum computing is accelerating – and the security implications are something we should consider now. When Google unveiled its latest quantum breakthrough with [Willow](#), in December 2024, it marked a significant step forward in the quantum journey. But amid the buzz, it's important to recognize that Willow represents just the second of six critical milestones toward scalable, usable quantum hardware and software. We're still in the early innings, but now is the time for security leaders to get serious about preparing for a quantum future.

Why does this matter? Because quantum computing, once realized at scale, threatens to fundamentally disrupt the cryptographic foundations of our digital world. Today's encryption standards, from RSA to elliptic curve algorithms, are considered secure not because they're unbreakable, but because breaking them would take thousands of years with current classical computing power. Quantum systems, however, could shorten that timeline dramatically.



Consider a simple HTTPS connection between a user and a website. The secure handshake that protects the session relies on asymmetric key exchange algorithms. These algorithms are resilient today because brute-force attacks would take longer than the universe has existed. But a sufficiently powerful quantum computer could, in theory, solve those same problems exponentially faster – potentially rendering much of today’s encryption obsolete.

While quantum hardware isn’t in the hands of adversaries yet, government agencies and high-security industries aren’t waiting. They’re already investing in post-quantum cryptography (PQC) – encryption designed to resist quantum attacks. In fact, in 2024 the U.S. National Institute of Standards and Technology (NIST) [finalized](#) its first group of post-quantum encryption standards, following a years-long global vetting process. Adoption of these standards will play a vital role in future-proofing digital security.

The good news? PQC isn’t theoretical. It’s available today and relatively straightforward to implement. Security teams can begin evaluating and testing post-quantum algorithms without needing a wholesale overhaul of infrastructure. In most cases, PQC can be integrated at the protocol or software layer, without visible impact to users or systems.

Still, quantum preparedness isn’t just a technology question, it’s a strategic one. Organizations must build quantum resilience into their roadmaps now. That means staying close to evolving standards, investing in cryptographic agility, and ensuring teams are prepared to pivot quickly as quantum capabilities mature.

For most consumers and businesses, post-quantum encryption won’t be a pressing issue – yet. But for CISOs, CIOs, and security professionals, the time to act is before the tipping point arrives. Just as we’ve seen with AI, technological inflection points can come faster than anticipated, bringing rapid shifts in threat models and risk profiles.

Quantum computing may not be ready to rewrite the rules of cybersecurity tomorrow, but the smart move is to start preparing today. Because when the breakthrough comes, the organizations that have already laid the groundwork will be the ones best equipped to thrive in a post-quantum world.

About the Author

Jason Rader is the CISO of Insight Enterprises. He assumed the role in 2021 after joining the company in 2015 to build the security consulting group. Today, he builds upon more than 25 years of experience to develop Insight’s end-to-end security consulting portfolio and share Insight’s transformation journey with fellow security leaders. Jason can be reached online on [LinkedIn](#) and at our company website www.insight.com.



Delinea

Securing identities at every interaction

Seamless, intelligent, centralized authorization to better secure the modern enterprise in the age of AI

- | Privileged Remote Access
- | Secure Credentials
- | Privilege & Entitlement Elevation
- | Identity Threat Protection
- | Identity Governance

Learn more about how to secure all human and machine identities with Delinea.

We're On It





Navigating the Future of Network Security with Secure Access Service Edge (SASE)

Simplify Your Journey with Sangfor Access Secure

By Akarsh Jain, Product Marketing Manager for SASE, Sangfor Technologies

The business world is undergoing a profound transformation, driven by rapid technological advancement. At the heart of this transformation are two major forces reshaping workplace dynamics: the increased adoption of cloud services and the rise of hybrid work culture.

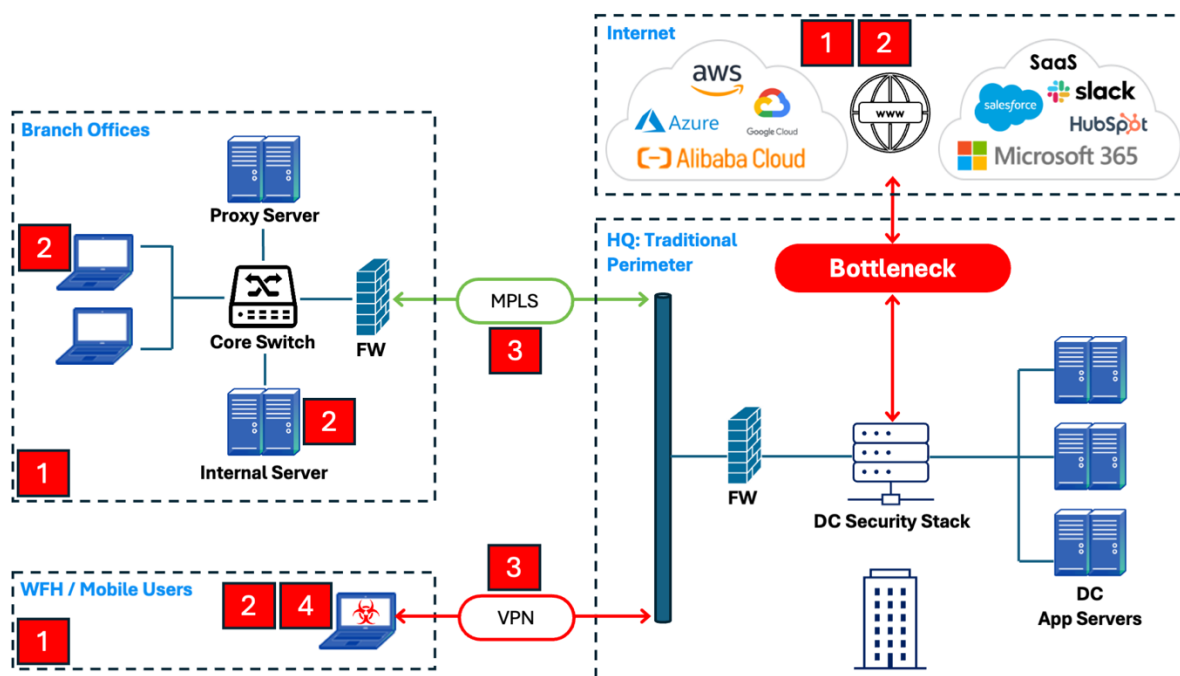
Cloud services will evolve from a technology innovation to a competitive necessity for 90% of businesses by 2028, as per Gartner. Organizations are embracing cloud services to increase agility, scale operations, and reduce infrastructure costs. The COVID-19 pandemic accelerated the shift to remote work, and now, hybrid work models—where employees split time between remote and on-site locations—have become a new standard. In 2025, 65% of employees will work remotely at least one day per week, and the trend is expected to grow, as per Gartner.

Cloud adoption and a hybrid work workforce significantly benefit organizations in terms of business scalability and continuity, as well as employee productivity and satisfaction. However, they also introduce unique challenges, such as data privacy, access security, compliance, and connectivity.

As businesses expand their digital footprint, cyber attackers increasingly target unsecured cloud resources and remote endpoints. Traditional perimeter-based network and security architectures are not capable of protecting distributed environments. Therefore, organizations must adopt a holistic, future-proof network and cybersecurity architecture to succeed in this rapidly changing business landscape.

The Challenges

Perimeter-based security revolves around defending the network's boundary. It assumes that anyone who has gained access to the network is trusted and that everything outside the network is a potential threat. While this model worked well when applications, data, and users were contained within corporate walls, it is not adequate in a world where cloud applications and hybrid work are the norm. Here are the key reasons, and how they map to a typical enterprise's IT environment:



1. Decentralized Management: Traditional network and security architectures are disjointed, leading to inconsistent security policies across cloud, on-premises, and remote environments. This fragmentation results in policy silos with no unified governance or visibility. IT administrators are forced to manually synchronize security policies across diverse environments and security tools—a resource-intensive process prone to human error, increasing the risk of misconfigurations and breaches.

2. Data Siloes: For distributed organizations, sensitive data resides across multiple clouds, SaaS applications, and remote endpoints, creating visibility gaps and inconsistencies in where the data is

stored, how it is accessed, and who is using it—often precursors of data exfiltration, unauthorized sharing, and insider threats.

3. MPLS and VPN Limitations: Traditional MPLS and VPN solutions were not designed for the cloud or global remote access, leading to latency and performance bottlenecks. These architectures are costly and complex to scale. They often result in poor end-user experience when accessing resources remotely or on the cloud.

4. Remote Access Exploits: Sophisticated cyberattacks increasingly target cloud workloads and remote endpoints because they lie outside traditional perimeter defenses. Modern attackers often compromise identities from remote endpoints to appear as legitimate users for targeting cloud and on-premises workloads.

The Solution

To resolve the network and security challenges posed by increasing cloud adoption, remote work, and distributed organizations, Gartner proposed a modern, cloud-delivered architecture in 2019. This architecture, called Secure Access Service Edge (SASE), converges networking and security services into a unified framework.

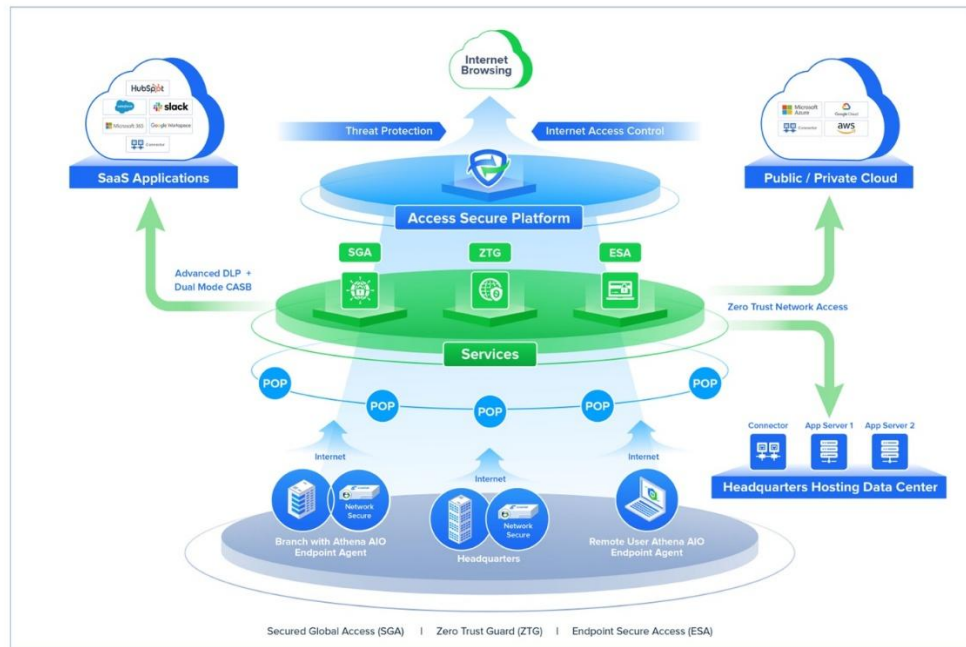
SASE is an architecture comprising a broad spectrum of technologies, including Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), and Software-Defined Wide Area Networking (SD-WAN). Everything is embodied into a single, cloud-native platform that provides advanced cyber protection and seamless network performance for highly distributed applications and users.

Sangfor Access Secure: The Smarter, Simpler, And More Secure Way To Connect

SASE represents a shift from traditional perimeter-based architectures. However, the path to SASE is far from straightforward; it requires a gradual, step-by-step approach. Each enterprise has its own starting point, requiring careful planning, flexibility, and customization.

With Sangfor Access Secure—the flagship SASE offering from Sangfor Technologies—you gain an experienced and reliable partner to help you navigate the complexities of SASE implementation at your own pace.

Sangfor Access Secure High-Level Architecture



Sangfor Access Secure is a comprehensive SASE platform that integrates advanced, AI-powered security features (ZTNA, SWG, FWaaS, DLP, EDR) with wide-area network (WAN) agility, empowering modern businesses with a Smarter, Simpler, and more Secure way to connect. Our cloud-native platform ensures users and edge resources enjoy fast, secure, and reliable access to the internet, cloud, and on-premises anytime, anywhere, and on any device.

Sangfor Access Secure Key Features and Benefits



Future Outlook: The Evolution of Sangfor Access Secure

Sangfor Access Secure has a proven track record of transforming organizations' network and security infrastructures by delivering a resilient yet flexible SASE platform. As buyer needs evolve, we continue to enhance the platform with new technologies through robust R&D. At Sangfor, we believe that the future of SASE is promising, driven by our innovations in the following areas:

AI and Machine Learning Integration: AI and ML will play an integral role in Sangfor Access Secure, adding value through automated policy configurations, behavioral analytics, and automation to detect, diagnose, and resolve performance and security issues in real time.

Edge Computing and 5G Integration: Our vision is to extend robust security to the edge, ensuring seamless protection and connectivity for IoT devices, remote sites, and branch offices.

Quantum-Resilient Security: Quantum computing is a potential threat to existing encryption models. A SASE solution should secure data transmissions and safeguard critical systems against quantum-based attacks.

Additionally, the emergence of open SASE ecosystems will foster interoperability between solutions, and Sangfor will also be part of that ecosystem.

Conclusion

As the threat landscape evolves and organizations embrace digital transformation, SASE will become the de facto architecture for securing and optimizing modern networks. Businesses that invest in a reliable and visionary SASE platform like Sangfor Access Secure will be better positioned to protect their assets, improve operational efficiency, and deliver secure access across dynamic and distributed environments. The future of Sangfor Access Secure is promising, driven by innovations in AI, edge computing, and Zero Trust. By selecting Sangfor as your partner on your SASE journey, you can meet the security demands of today and lay a solid foundation for the demands of tomorrow.

Sources:

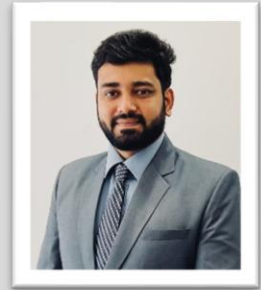
<https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028>

<https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025>

<https://www.gartner.com/en/documents/5598759>

About the Author

Akarsh Jain is the Security Product Marketing Manager at Sangfor Technologies. He has over eight years of experience with leading technology firms, including Senior Product Manager at Citrix and Commercial Product Manager at Oracle, constantly developing his technical expertise in the fields of network security and cloud infrastructure. Akarsh can be reached online at akarsh.jain@sangfor.com and at our company website <https://www.sangfor.com/>.



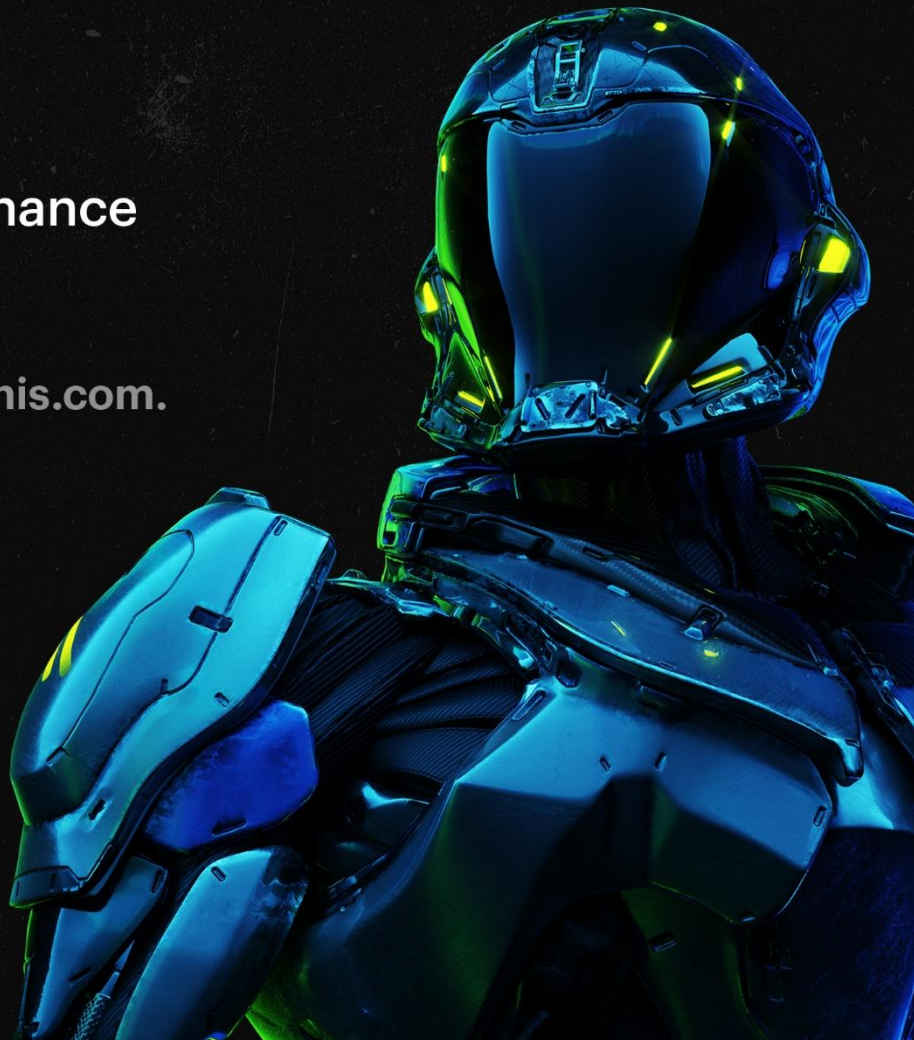


DATA SECURITY FOR THE AI ERA

SAAS | IAAS | FILE STORAGE

- + DSPM
- + Data discovery & classification
- + AI security
- + Data-centric UEBA
- + SSPM
- + Data access governance
- + MDDR

Learn more at www.varonis.com.



Red Piranha's **Unified Approach** to Modern Threat Defense



Adversarial Machine Learning
Lateral movement
Zero-Click
Fileless Malware
Supply Chain Backdoors
Temporal Exploitation
Firmware Rootkits

Red Piranha's Unified Approach to Modern Threat Defense

By Adam Bennett, CEO, Red Piranha

[Red Piranha](#), headquartered in Australia, is a premier developer and manufacturer of cybersecurity technologies and solutions. As an esteemed member of Team Defence Australia, the company specializes in advanced cybersecurity solutions. Committed to ensuring robust information protection, Red Piranha leverages automation, cutting-edge technology, and a team of skilled professionals to deliver unparalleled security solutions to businesses across various industries.

The Challenge of Cybersecurity Fragmentation and Point Solutions

Many organizations face challenges with cybersecurity fragmentation, juggling different security solutions from different vendors. This leads to operational inefficiencies and security blind spots. This disjointed approach results in a tangled mess of products, where critical alerts are often missed, and attacks detected by one system might not trigger defenses in another, delaying incident response.

Red Piranha eliminates these challenges with Crystal Eye, a fully integrated "single pane of glass" security platform that unifies Threat Detection, Investigation, and Response (TDIR), Network Detection and Response (NDR), Crystal Eye WireGuard integrated with Microsoft Entra ID SSO, and Declarative Authorization Service (CASB) with more under one comprehensive system.

Crystal Eye consolidates cloud, network, and endpoint security ensuring all security events whether a network intrusion, an endpoint compromise, or a privileged access anomaly are correlated in real-time for immediate action.

By merging these capabilities into a single platform, Crystal Eye eliminates security silos, enhances compliance, and accelerates threat containment. Organizations gain centralized visibility, automated enforcement, and adaptive security, ensuring a proactive defense against evolving threats, all managed through one intuitive interface.

This holistic approach makes Crystal Eye a best-in-class cybersecurity solution, meeting global compliance standards while simplifying security operations.

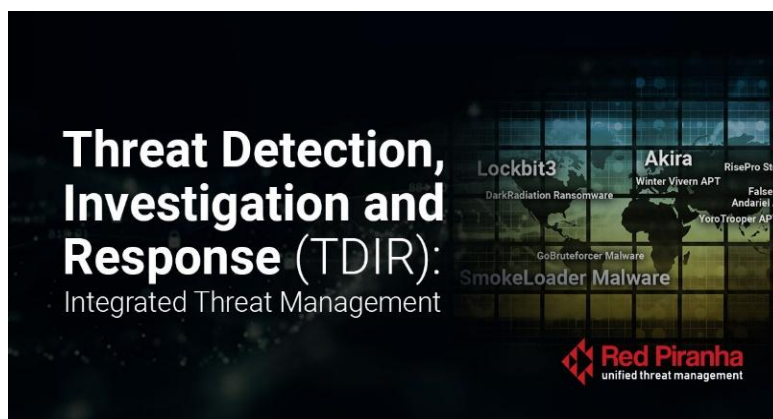
Crystal Eye Advantages:

- **10x Threat Visibility:** Combat APTs and unknown threats with network behavioral analytics for unparalleled insight.
- **Universal Malware Detection:** detect all known malware families and CnC communications (e.g., Cobalt Strike).
- **Automated Threat Intelligence:** Deploy contextualized intel and actionable insights to proactively protect, detect, and respond.
- **Human-Machine Collaboration:** Prioritize alerts and accelerate incident response through seamless teamwork.
- **Proactive Threat Hunting:** Uncover hidden APTs and reduce dwell time with advanced detection.
- **Unified Sensor Platform:** Enhance East-West traffic visibility and detection engineering across multi stages of the attack process.
- **Integrated PCAP Analysis:** Streamline threat investigation and response with deep packet capture insights.
- **On-Demand SOC Support:** Rapidly resolve incidents with digital forensics and SOC expertise.
- **AI/ML-Driven Confidence:** Boost alert accuracy with advanced heuristics and contextualized threat intelligence.

Threat Detection, Investigation and Response (TDIR): Integrated Threat Management

The [Threat Detection, Investigation and Response \(TDIR\)](#) component is the brains of Crystal Eye's unified defense – it's where threats are identified, analyzed, and swiftly neutralized in a coordinated way. Red Piranha's TDIR capability is *best-in-class* in correlating events and spotting advanced threats that evade traditional tools.

Unlike standalone solutions or intrusion systems that might only look at one piece



of the puzzle, TDIR pulls in telemetry from across the network, endpoints, cloud services, and applications.

It uses advanced analytics (including AI/ML techniques and behavioral analysis) and continuously updated threat intelligence feeds to recognize both known malware and novel attacker behaviors.

For instance, Crystal Eye can detect subtle signs of an attack such as a normally quiet server suddenly communicating with a command-and-control server or unusual patterns that suggest a threat. With over 70,000 IDS/IPS threat detection rules updated daily feeding into the system, the platform stays current with the latest indicators of compromise.

This means even stealthy tactics like fileless malware or *living-off-the-land* (where attackers use legitimate admin tools maliciously) can be uncovered, as the platform looks for anomalies in usage patterns rather than just known virus signatures.

Network Detection & Response (NDR): Deep Network-Level Visibility and Defense

A standout feature of Red Piranha's unified solution is its strong focus on [Network Detection and Response \(NDR\)](#): An area often overlooked by companies that rely solely on endpoint security.

Crystal Eye NDR acts as the eyes and ears of the network, continuously monitoring traffic flowing in and out, as well as laterally within the environment. It uses a combination of machine learning, advanced analytics, and rule-based matching to flag anomalous or suspicious activities on the network.

This means it can catch threats that don't necessarily install malware on a device. For example, an attacker probing your network, an IoT device behaving oddly, or a hacker exfiltrating data through an encrypted channel. Network-wide visibility is crucial because sophisticated attackers often try to hide their tracks using encryption or by leveraging legitimate network protocols.

Crystal Eye's NDR is capable of analyzing over 3,200 network protocols (including specialized industrial/SCADA protocols) out-of-the-box and even inspects encrypted traffic for deviations from normal patterns. By doing so, it secures organizations against *zero-day threats* and *APTs* that might not trigger any signature on an endpoint but do create anomalies in network behavior.

Crystal Eye WireGuard + Microsoft Entra ID SSO: Secure Remote Access, Simplified

The shift to remote work has made VPNs a prime target for attackers. Red Piranha's Crystal Eye WireGuard is now integrated with Microsoft Entra ID Single Sign-On (SSO). Now, why this sets us apart from other solutions?

As remote work becomes the norm, secure VPN access is more critical than ever. WireGuard VPN has gained popularity due to its lightweight design, high-speed performance, and strong encryption. However, by default, WireGuard relies on static cryptographic keys, which lack enterprise identity management integration. To address this limitation, Crystal Eye has integrated WireGuard with Microsoft Entra ID

(formerly Azure AD) Single Sign-On (SSO), providing seamless and secure authentication for remote users.

Crystal Eye WireGuard with Entra ID SSO ensures that employees authenticate using Azure AD credentials instead of standalone VPN passwords. This integration eliminates password fatigue, reduces the risk of credential reuse attacks, and improves user experience.



By enforcing Multi-Factor Authentication (MFA) and Conditional Access policies, organizations can add another layer of security, ensuring that only authorized users on compliant devices can connect to the corporate network.

Security administrators benefit from centralized access control and audit logging, as all VPN authentication requests are managed through Azure AD groups. This means that access can be easily revoked when an employee leaves or changes roles, reducing the risk of forgotten or stale VPN accounts. Additionally, organizations can enforce Zero Trust principles by requiring VPN users to meet specific security criteria before establishing a connection.

For businesses, integrating Crystal Eye WireGuard with Entra ID SSO delivers a seamless, secure, and scalable remote access solution. Employees experience frictionless login, while IT teams gain enhanced control over VPN security and compliance. The combination of strong encryption, single sign-on, and adaptive access controls ensures that remote access remains both secure and user-friendly.

Declarative Authorization Service (DAS): Enforcing Zero Trust with Precision

One cornerstone of Red Piranha's Crystal Eye platform is the integration of Declarative Authorization Service (**DAS**). Crystal Eye's Declarative Authorization Service (DAS) distinguishes itself from others by providing a scalable, automated framework that protects software services with precise, "allow on need basis" access control, reducing manual effort and revenue loss while enhancing availability.

Integrated within Crystal Eye's platform featuring a next-generation firewall, NDR, EDR, and SIEM, DAS leverages real-time threat intelligence (updated four times daily with 70,000+ IDPS rules) and Automated Actionable Intelligence to dynamically block unauthorized access to REST endpoints, offering granular protection beyond many alternatives.

Managed by a DAS Administrator, it oversees Cloud Tenant Access (integrating Azure AD for users/groups), Enterprise Application Details (FQDN, IP, ports), Resources (endpoint protection), and Policies (blocking rules). Affordable and MSP-friendly, DAS supports compliance (e.g., GDPR, ISO

27001) and pairs with CESOC for 24/7 monitoring, delivering a unified, cost-effective, and adaptive security solution unmatched by less integrated or pricier options.

Managed Detection and Response (MDR): Augmenting Crystal Eye with 24/7 Human-Machine Security Operations

Red Piranha's [Managed Detection and Response \(MDR\)](#) service extends the Crystal Eye platform into a full-spectrum SOC-as-a-Service, purpose-built to help organizations detect, investigate, and respond to threats at machine speed. Seamlessly integrated with Crystal Eye's TDIR, NDR, endpoint, and identity telemetry, MDR delivers 24x7 monitoring, rapid incident response, digital forensics (DFIR), proactive threat hunting, and automated threat intelligence correlation.

Unlike traditional MSSPs, it offers deep, identity-aware and east-west traffic visibility, enabling early detection of advanced threats like APTs and insider attacks. Its built-in SOAR capability automates triage and mitigation, allowing expert analysts to focus on high-risk incidents while maintaining consistent, scripted response actions. With ISO 27001-certified global SOC's, no extra integration or licensing overhead, and use-case-driven tuning, Crystal Eye's plug-and-play MDR delivers enterprise-grade detection and response with lower operational burden making advanced security accessible even to resource-constrained teams.

How Red Piranha's Integrated Security Framework Works?

Red Piranha's Declarative Authorization Service (DAS), Threat Detection and Incident Response (TDIR), and Network Detection and Response (NDR), and Wireguard integrated with Entra ID SSO work together to form a unified defense system that ensures comprehensive visibility, proactive mitigation, and automated response.

When a security incident occurs, TDIR detects unusual user behavior, such as a compromised endpoint attempting unauthorized access. This information is immediately correlated across the platform, enabling DAS to revoke access rights in real-time and NDR to monitor and block any suspicious network activity. By integrating these capabilities, Red Piranha eliminates security gaps and enables an adaptive, Zero Trust-aligned security posture.

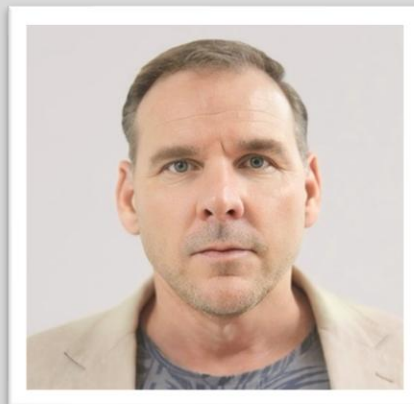
Technical Implementation in Action

1. **Threat Detection:** TDIR identifies anomalous activity from an endpoint, signaling a possible credential compromise.
2. **Automated Response:** DAS instantly revokes the compromised user's access, while NDR prevents unauthorized lateral movement by monitoring and blocking malicious network traffic.
3. **Correlated Insights:** Data from DAS, TDIR, and NDR, and Wireguard is aggregated, providing a detailed incident report for faster investigation and response.
4. **Ongoing Protection:** Security policies are dynamically updated across the system, ensuring proactive mitigation of similar threats in the future.

By integrating real-time detection, automated access control, and network-wide monitoring, Red Piranha's framework streamlines incident response, reduces operational overhead, and fortifies security at every layer.

About the Author

Adam Bennett, CEO Red Piranha Limited. Adam Bennett is a globally recognised cybersecurity leader, innovator, ethical hacker, and qualified industry expert. As the Founder and Chief Executive Officer, Adam has led Red Piranha from its conception in 2013 to become one of Australia's renowned and awarded cybersecurity organisations. Adam's passion and driving vision is to provide comprehensive cybersecurity protection from the growing threat landscape by offering enterprise-grade cybersecurity solutions to businesses of all sizes.



A prolific contributor to the IT and Developer industry, Adam is a professional presenter and industry advocate, actively participating within the cybersecurity community industry since the late 1980s. He has authored and contributed to multiple industry papers, including being published with NATO cyber security research, industry research with INTEL and professional blogs, podcasts, amongst other publications.

Years Experience 30+

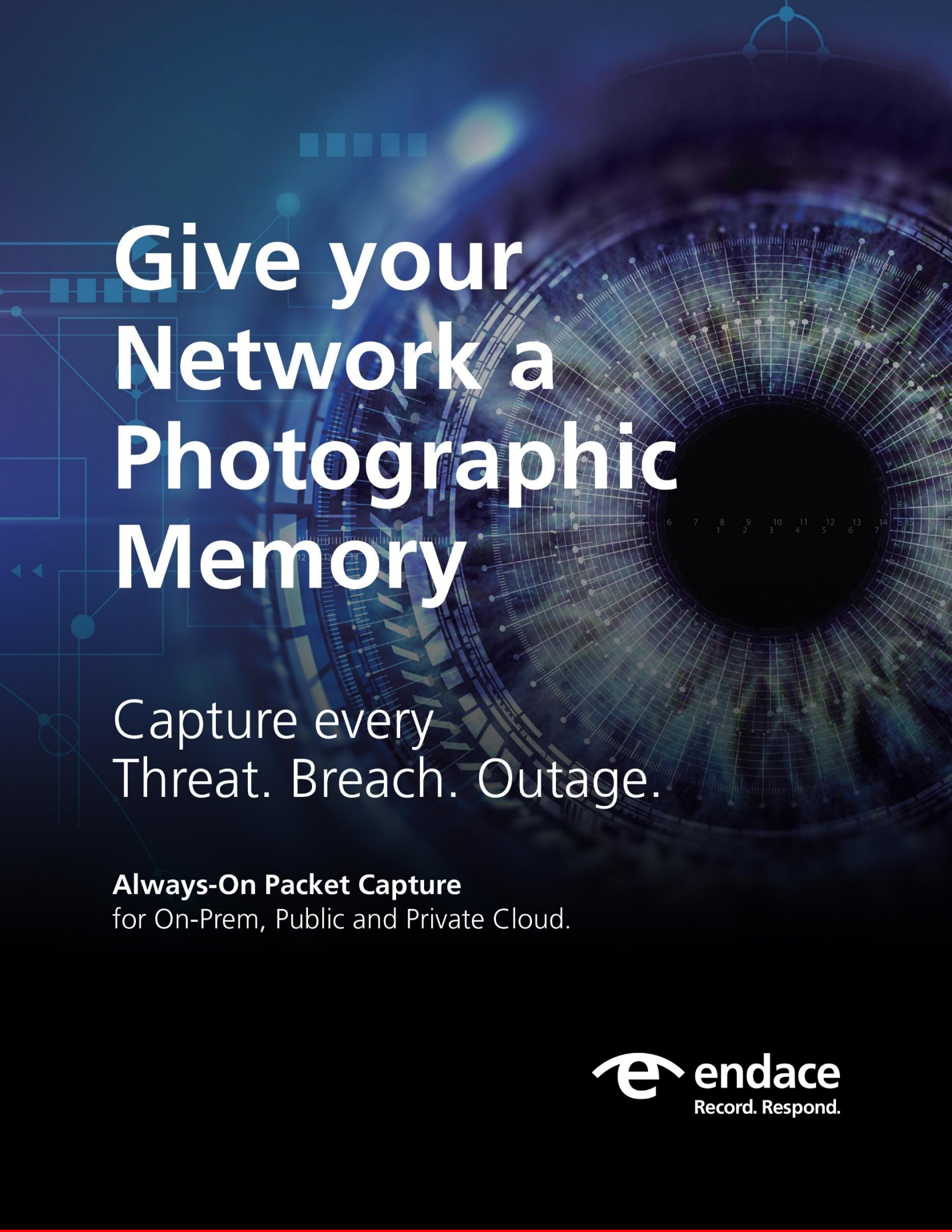
Services Expertise Professional Management, Security and Risk Management, Project Management

Region APAC

Qualifications ISACA CDPSE, CISSP, GIAC, LFS101, LFS201, CCNA, CEH, MAS S69 Big Data and Social Physicals Mathematics and Comp Science MIT, Cert Cyberwar, Surveillance and Security, PMP, MVA Defence in Depth Windows 8.1 Security, MVA Powershell 3.0, Cert Training Officer, PUACOM001C, PUAOPE002B, Cert 1 & 2 CISCO, AMTC IPV6, ITILv2, ITILv3, CECE, CEE 1 & 2, RPCSAT

Professional Affiliations ISACA, ACS, ASIA, PMI, DFA, EFA

Adam can be reached online at info@redpiranha.net and at our company website <https://www.redpiranha.net>



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.



Rethinking Vulnerability Prioritization

Moving Beyond the CVSS Crutch

By Omer Tal, Security Researcher in the CTO Office at Seemplicity

The Volume Problem

Security teams are inundated with vulnerabilities. Between scanners, penetration tests, and bug bounty programs, the list of issues grows faster than most organizations can address. And while “just fix everything” sounds heroic in theory, it’s unrealistic in practice; especially for large organizations with sprawling environments and limited remediation bandwidth.

This reality makes prioritization essential. The objective is to reduce the most significant risk in the least amount of time. But how teams approach that goal varies widely, and not all methods are equally effective. Overly simplistic models can mislead efforts, diverting valuable resources toward issues that may not pose a meaningful threat.

To make real progress, organizations need a prioritization strategy that accounts for more than just severity scores. One that reflects both technical and business realities – and keeps pace with a dynamic threat landscape.

The Flawed Simplicity of CVSS-Only Approaches

For many organizations, vulnerability prioritization begins – and ends – with the Common Vulnerability Scoring System (CVSS). It's a convenient starting point: standardized, widely adopted, and built into most scanning tools. But while CVSS helps categorize severity, it's not a risk score.

CVSS ratings don't consider whether a vulnerability is actually being exploited in the wild. They don't reflect how critical the affected asset is to business operations. And they don't account for how difficult remediation might be in a given environment. In short, CVSS provides a measure of theoretical impact under idealized conditions, but that's not a practical roadmap for action.

Relying solely on CVSS often leads to noisy queues filled with “critical” issues that aren't exploitable, while real threats slip through the cracks. It's a one-size-fits-all approach in a world that demands nuance.

To prioritize effectively, security teams need to bring additional context into the equation.

Context Matters

To move beyond surface-level severity, many organizations are turning to contextual risk scoring. This approach enriches vulnerability data with factors specific to the organization, such as asset criticality, business function, exposure level, and internal connectivity.

A vulnerability on a test server might not warrant immediate attention. That same vulnerability on a production-facing application tied to customer data? A very different story. Context transforms generic findings into meaningful insights by aligning technical issues with operational impact.

This shift allows teams to prioritize vulnerabilities not just by how dangerous they are in theory, but by how much risk they pose in practice. It also helps bridge the gap between security and the business by tying remediation decisions to the protection of key assets and services.

In other words: CVSS provides a baseline; context gives it meaning.

The Role of Exploit Intelligence

While context sharpens the picture internally, threat intelligence adds a critical external dimension: understanding which vulnerabilities are actively being exploited. Not all vulnerabilities are equal in the eyes of attackers. Some are widely weaponized within hours of disclosure; others may never be targeted at all.

Exploit intelligence provides a critical lens for prioritizing vulnerabilities, not just by what *can* be exploited, but by what *is* or *likely will be*.

At one end of the spectrum are known, in-the-wild exploits. Resources like CISA's Known Exploited Vulnerabilities (KEV) catalog help security teams pinpoint issues actively targeted by threat actors. These vulnerabilities represent immediate, proven risk and often require the fastest response.

On the predictive side, frameworks like the Exploit Prediction Scoring System (EPSS) assess the likelihood that a vulnerability will be exploited in the near future, even if no public exploitation has occurred yet. This adds an important dimension for anticipating risk before it materializes.

Together, these signals help security teams stay ahead of attackers, not just by responding to today's threats, but by preparing for tomorrow's. Exploit intelligence, both reactive and predictive, adds vital depth to prioritization strategies grounded in real-world behavior.

A Unified Approach

Each signal – CVSS, business context, exploit intelligence – offers a valuable perspective. But the real power comes from combining them. An effective prioritization strategy draws from multiple data points to create a fuller, more actionable picture of risk.

This doesn't mean layering on complexity for its own sake. It means designing a system that elevates the right issues by weighing what's exploitable, what's exposed, and what's important to the business. When these elements are considered together, prioritization shifts from a ranking exercise to a decision-making framework.

For example, a vulnerability with a high CVSS score, active exploitation in the wild, and presence on a business-critical system clearly demands urgent attention. By contrast, a similar vulnerability on an isolated, low-value asset can safely wait without compromising the organization's risk posture.

Prioritization Is a Strategy, Not a Score

Vulnerability management isn't a numbers game, it's a risk management discipline. Relying on a single metric or static threshold is no longer sufficient in today's threat environment. Attackers are adaptive. Environments are dynamic. And risk is inherently contextual.

Effective prioritization requires a shift in mindset. It's not about reacting to every high score or new scan result. It's about applying consistent, defensible logic to determine what gets fixed, when, and why. That means integrating multiple signals, understanding business impact, and staying attuned to external threats, all within a process that supports timely, coordinated action.

Security teams that treat prioritization as a strategic function and not just a technical task are better positioned to reduce real risk, improve remediation velocity, and focus resources where they matter most.

In the end, the goal isn't to fix everything. It's to fix the right things first.

About the Author

Omer Tal is a Security Researcher in the CTO Office at Seemplicity. Omer has spent the last ten years deep in the world of cybersecurity research. He's been part of teams at startups like Argus, VisibleRisk, and BitSight. Now, he's at Seemplicity, diving into the nuts and bolts of vulnerability prioritization and remediation. Omer Tal can be reached online at [linkedin.com/in/the-omertal](https://www.linkedin.com/in/the-omertal) and at our company website <https://www.seemplicity.com/>



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.



www.unknowncyber.com



Endpoint Security In 2025

The Necessity of EDR for Organizational Protection

By Namrata Barpanda, Staff Information Security Engineer, ServiceNow INC

Introduction

As organizations navigate the complexities of modern cyber threats in 2025, endpoint security has emerged as a cornerstone of effective defense strategies. The growing sophistication of attacks, the shift to hybrid work environments, and the increasing reliance on digital infrastructure have made it imperative for businesses to secure every potential entry point into their networks. One of the most critical tools in this effort is Endpoint Detection and Response (EDR) a security technology designed to provide real-time monitoring, threat detection, and rapid incident response. With the rise of advanced threats like file-less malware, zero-day exploits, and ransomware, traditional antivirus solutions rooted in signature-based detection are no longer enough. This article explores the evolution and growing importance of EDR, the risks organizations face without it, and how implementing EDR can safeguard operations in today's fast-moving cyber threat landscape.

Abstract

Endpoint security, particularly using Endpoint Detection and Response solutions, has become indispensable in the fight against advanced cyber threats. This article examines the critical role of EDR in safeguarding organizational data, preventing breaches, and maintaining operational continuity. By understanding the challenges that organizations face without EDR and the benefits of its deployment, businesses can make informed decisions about adopting robust endpoint security strategies to protect against modern threats.

Background of EDR

Endpoint Detection and Response (EDR) represents a proactive approach to endpoint security. Unlike traditional security solutions that primarily rely on signature-based detection methods, EDR employs advanced technologies such as machine learning, artificial intelligence (AI), and behavioral analytics. This allows EDR systems to identify suspicious activity, even from previously unseen threats, by analyzing patterns in data and behavior rather than matching them to known virus definitions.

EDR solutions continuously monitor endpoints such as laptops, desktops, and mobile devices and respond to potential threats in real-time. With the shift towards remote work, EDR has become even more critical, as it offers a centralized method for monitoring devices regardless of their location. The evolution of EDR technologies has provided businesses with the ability to not only detect but also respond to threats in a timely and efficient manner, thus significantly reducing the likelihood of a successful cyberattack.

Why EDR is Important for Organizational Security

In the current landscape of cybersecurity, where attacks are becoming more complex and frequent, EDR is no longer just a luxury; it is a necessity. The importance of EDR can be understood by considering the following factors:

1. **Rising Sophistication of Cyber Threats:** Traditional antivirus solutions are often inadequate against new types of threats like fileless malware, polymorphic attacks, and zero-day vulnerabilities. EDR systems can detect such attacks by recognizing abnormal behaviors, providing an advanced layer of defense that signature-based tools cannot offer.
2. **Growing Attack Surface:** As organizations embrace digital transformation, the attack surface has expanded significantly. Remote work, cloud adoption, and the increased use of Internet of Things (IoT) devices have introduced more potential points of vulnerability. EDR helps monitor and protect these endpoints, ensuring that all devices are secure.
3. **Proactive Threat Hunting:** EDR not only provides reactive protection but also allows security teams to proactively hunt for threats. This can involve analyzing the data from past incidents to identify patterns and uncover hidden threats that may have evaded detection initially.

Operational Challenges Without EDR

While EDR offers comprehensive protection, many organizations still operate without such solutions, relying on traditional methods like firewalls and basic antivirus software. However, the absence of EDR introduces several operational challenges:

1. **Increased Vulnerability to Advanced Threats:** Without EDR, businesses are more vulnerable to sophisticated attacks that can bypass traditional defenses. Cybercriminals are increasingly utilizing tactics that exploit weaknesses in legacy systems, making organizations without EDR prime targets for attacks like ransomware, phishing, and data breaches.
2. **Limited Visibility and Detection:** Traditional security measures often provide limited visibility into endpoint activities. Without real-time monitoring, it becomes difficult to detect attacks that do not match known signatures or exhibit unusual behavior. This delay in detection can result in significant data loss and operational disruption.
3. **Inadequate Protection for Remote Workers:** As more organizations embrace remote work, traditional endpoint security solutions become less effective. EDR, on the other hand, provides continuous monitoring for remote endpoints, ensuring that employees working from home or on the go are just as secure as those in the office.

How EDR Safeguards Organizational Data

The integration of EDR within an organization's security framework provides several key benefits in terms of data protection:

1. **Real-Time Threat Detection and Response:** EDR systems use behavioral analysis to detect unusual activity, such as file manipulation, unauthorized access attempts, and data exfiltration. This allows organizations to identify threats before they can cause significant damage.
2. **Automated Remediation:** One of the key features of modern EDR solutions is their ability to automatically respond to threats. If a potential threat is detected, EDR systems can isolate compromised devices, terminate malicious processes, and even roll back harmful changes to restore the system to its previous state. This automation reduces the time between detection and remediation, which is crucial in minimizing the impact of an attack.
3. **Enhanced Endpoint Visibility:** EDR platforms provide security teams with a centralized view of all endpoints, regardless of their location. This visibility makes it easier to detect anomalies, track attacks across devices, and ensure that every endpoint is adequately protected.
4. **Improved Threat Intelligence:** EDR solutions often integrate with threat intelligence feeds to provide contextual information about the nature of the threat. This helps organizations understand the broader attack landscape and prioritize their response accordingly.

How EDR Protects from Cyber Breaches

Cyber breaches can have devastating consequences, from financial loss to reputational damage. EDR significantly reduces the risk of a breach in several ways:

1. **Early Detection of Indicators of Compromise (IOCs):** EDR tools continuously monitor endpoints for IOCs, such as unusual network traffic, suspicious file changes, or unauthorized access attempts. Early detection of these indicators can stop an attack in its tracks before it escalates into a full-blown breach.
2. **Containment and Isolation:** Once a threat is detected, EDR systems can quickly contain and isolate affected endpoints, preventing the spread of malware or ransomware across the network. This containment is crucial in limiting the damage caused by a breach.
3. **Data Exfiltration Prevention:** EDR solutions can also monitor for signs of data exfiltration, where attackers attempt to steal sensitive information. By detecting abnormal data transfer patterns, EDR systems can block these attempts and alert security teams.
4. **Forensic Analysis:** In the aftermath of a breach, EDR platforms provide detailed logs and data for forensic analysis. This helps organizations understand the scope of the attack, identify how the breach occurred, and take steps to prevent similar incidents in the future.

Conclusion

As we move further into 2025, the importance of endpoint security cannot be overstated. Endpoint Detection and Response (EDR) has emerged as a critical tool in the fight against cyber threats, offering organizations advanced protection against increasingly sophisticated attacks. By providing real-time detection, automated remediation, and enhanced visibility, EDR empowers organizations to protect their data, prevent breaches, and maintain uninterrupted operations in the face of ever-evolving cyber threats. Ignoring its importance is no longer an option—doing so leaves businesses vulnerable to costly attacks, reputational damage, and regulatory fallout. In today's digital landscape, where threats are more frequent and sophisticated than ever, EDR stands as a critical safeguard for any organization committed to security and resilience.

About the Author

Namrata Barpanda, works as a Staff Security Engineer specializing in threat detection, mitigation, and vulnerability prevention. She excels in building automated defenses through Detection-as-Code, with a focus on strengthening IDS/IPS, WAF, and MFA systems to safeguard against OWASP Top 10 vulnerabilities, phishing attacks, and zero-day exploits. Her work revolves around cyber kill chain framework, helping organizations counter advanced threats. Namrata also enhances attack surface management to secure critical assets. Passionate about mentorship and knowledge sharing, she actively engages with cybersecurity communities to promote inclusive dialogue, digital equity, and innovation making security not just a technical goal but a social responsibility. Namrata can be reached at LinkedIn: <https://tinyurl.com/itsnamrata>



ERTICO Presents:



**EUROPEAN
CONGRESS**
SEVILLE
19-21 May 2025

Europe's leading event for **Smart Mobility & Intelligent Transport Systems**

Visit our website



REGISTRATION IS OPEN!

Secure your spot today!

ITS European Congress | 19-21 May | FIBES, Seville



+200
Speakers



Up to 3,500
ITS Experts



+120
Innovations Showcased



+100
Expert Sessions

ORGANISED BY:



IN PARTNERSHIP WITH:



HOSTED BY:



SUPPORTED BY:





The Essential Guide to Third-Party Risk Management (TPRM)

Protecting Organizations in an Outsourced World

By Dasha Davies, President/CISO, Stealth-ISS Group Inc.

The expanding use of digital and cloud-based services alongside outsourcing trends makes Third-Party Risk Management (TPRM) essential for maintaining organizational security in today's business world. Organizations' systems, networks, and sensitive data are exposed to potential access by vendors, suppliers, contractors, and service providers through direct and indirect means. Alarming cybersecurity incidents and hefty regulatory fines have underscored a sobering reality: Organizational security threats predominantly emerge from third-party relationships rather than internal company vulnerabilities.

The Growing Threat of Third-Party Data Breaches

Data breaches resulting from third-party vulnerabilities show increasing frequency and severity. The Target, SolarWinds and MOVEit breaches clearly show the extensive harm organizations can suffer from inadequate vendor supervision. The affected organizations suffered substantial damage to their reputations and finances as a result of these events. The introduction of regulatory standards such as GDPR and CCPA alongside NYDFS Cybersecurity Regulation has increased the stakes for businesses. Organizations must implement proactive risk management strategies to protect sensitive data and maintain operational stability because compliance alone is insufficient in the current regulatory environment.

What is Third-Party Risk Management (TPRM)?

TPRM is a systematic framework used by organizations to identify their third-party risks and evaluate and monitor these risks in order to minimize potential threats from vendors and service providers. Organizations face risks that include cybersecurity issues such as hacking and data breaches along with operational failures, financial instability, and data privacy violations which can damage a company's reputation and lead to major operational disruptions.

The growing dependency of businesses on third parties for improved operational efficiency and specialized skills has led to a proportional increase in partnership risks. Business resilience depends heavily on having a strong TPRM strategy that can adapt to changing conditions. An effective TPRM program goes beyond regulatory compliance to protect corporate reputation, build customer trust and equip organizations for upcoming challenges.

Elements of a Comprehensive TPRM Program

Successful TPRM requires continuous oversight. Organizations must approach risk management as an ongoing process rather than a single event. A vendor relationship demands rigorous processes and thorough risk assessment at every stage from selection through performance evaluation to effectively control potential threats.

Categorizing Vendors by Risk Level

The first step in successful TPRM involves categorizing vendors according to their risk levels. Companies providing essential services such as payroll or cloud storage present much higher risks compared to vendors supplying non-essential items like office supplies.

Organizations can direct their resources to areas of greatest need through vendor risk classification into high, medium, and low categories. Organizations must conduct more detailed evaluations and enforce stricter security controls while continuously monitoring high-risk vendors to mitigate potential threats. Medium and low-risk vendors do not need intensive monitoring yet periodic assessments remain

essential to maintain operational consistency. Organizations use a tiered method to distribute their focus appropriately while retaining control over vendor relationships.

Conducting Due Diligence

A strong TPRM strategy needs thorough due diligence to maintain its effectiveness. Organizations need to evaluate vendor qualifications before beginning the onboarding process.

- Vendors that hold ISO 27001 or SOC 2 Type II certifications or adhere to the NIST framework show their dedication to data security principles and regulatory compliance.
- Organizations need to check that vendors maintain strong systems for vulnerability management and disaster recovery and backup testing as part of their incident response and continuity plans.
- Analyzing a vendor's historical compliance with industry standards and regulations shows their dedication to risk management strategies.
- Analyzing a vendor's subcontracting network uncovers hidden risks throughout the supply chain.

Both financial stability and insurance coverage maintain vendor reliability during crises by fulfilling their commitments.

Secure Vendor Contracts

Vendor agreements establish a legal protection framework and define necessary security measures along with compliance and risk management requirements. Current security risks cannot be addressed solely by using standard contract templates. Organizations should ensure their contracts include:

- The data protection stipulations in the vendor contracts should match both security best practices and existing legal requirements.
- Service-level agreements must establish clear benchmarks for system availability and uptime as well as stipulate procedures for incident response.
- Audit provisions enable organizations to conduct inspections of vendor operations to verify compliance.
- Contracts should contain terms for termination in situations where vendors do not comply with security standards or regulatory requirements.

These elements help organizations establish defined accountability metrics and lower their risk exposure.

Continuous Monitoring

Organizations typically struggle with maintaining ongoing supervision. The landscape of vendor risks changes constantly because of emerging threats and operational shifts or updated legal requirements so regular risk assessments become vital.

Businesses establish continuous monitoring programs by applying tools like security questionnaires and performance metrics alongside penetration testing and regular audits. SLA compliance together with incident response times and vendor KPI performance metrics serve as essential tools for oversight maintenance.

Organizations need to utilize external experts to perform audits and configuration assessments while detecting hidden vulnerabilities. By implementing structured review processes businesses synchronize vendor performance with both operational needs and regulatory standards while preserving compliance and organizational strength.

Aligning TPRM with Enterprise Risk Management (ERM)

Integrating TPRM with comprehensive Enterprise Risk Management (ERM) strategies maximizes its effectiveness. The collaboration needs contributions from multiple departments such as procurement, IT security, compliance, and legal teams. Executive leadership and the board must receive regular reports to ensure strong risk governance. Vendor risk assessments aligned with organizational risk appetite and strategic goals enhance risk management capabilities while fulfilling regulatory requirements.

Incident Response: Be Prepared for Breaches

A TPRM program with the highest quality standards still leaves some risk uneliminated. Organizations should create powerful incident response strategies to handle incidents that involve third-party entities. Organizations need established escalation processes and transparent communication protocols with vendors to effectively manage security breaches and operational failures.

Through tabletop exercises organizations can evaluate their preparedness while discovering weaknesses and strengthening coordination across departments. Proactive actions work to reduce the effects of crises involving vendors.

Building a Culture of Vigilance

A successful TPRM program demands organizational cultural transformation beyond just implementing tools and policies. Staff training is essential for employees to properly identify third-party risks while adhering to escalation procedures and assisting risk management efforts. The IT, legal, and procurement departments must completely comprehend their vendor oversight responsibilities. Every company level upholds risk management responsibilities through a unified commitment to vigilance.

Consequences of Inaction: Regulatory Compliance and Financial Costs

Companies face substantial costs when they fail to manage vendor risks properly. Organizations must show regulatory bodies that they maintain detailed supervision of third-party access to sensitive data. Organizations that fail to manage third-party vendor risks face severe financial penalties and damage both to their reputation and customer trust.

About the Author

As a global cybersecurity consultant/CISO, President of Stealth-ISS Group Inc., and Board Advisor on several cyber security technology and consulting service delivery companies, Dasha is an expert in cybersecurity operations, delivery risk, and compliance and a U.S. Navy veteran.

With over 25 years of experience as a technology professional, she shaped cybersecurity practices within the US Defense Industry, NATO, various national and international government agencies, and the and the commercial sector, ensuring the security of sporting events as significant as the Olympic Games and Formula 1. Her expertise is in cybersecurity, GRC, incident response, smart cities, artificial intelligence, national security/cyber warfare, and C4I services.

She has a bachelor's degree in International Relations and Foreign Affairs, a MBA, and a MSc in Information Technology and Management and Cybersecurity, respectively, complemented by her pursuit of a Doctorate in Business and a PhD (ABD) in Cyber Warfare and National Security.

Her authority in cybersecurity is underscored by a suite of certifications such as CISSP, C|CISO, NSA/IAM/IEM, and CMMC CCA, among others, and by being honored as one of the Top 100 CISOs in 2020.

Her voice is respected at global conferences and events where she has presented on topics including cyber security, data protection, AI, and smart cities.

She is a published author of "Beyond Binary: AI and Cybersecurity," with upcoming books on cyberwarfare/national security and "Navigating the Unknown in Cyber and AI."

Dasha Davies

<https://www.linkedin.com/in/dasha-davies/>

<https://stealth-iss.com/>





RegTech Africa
Conference

    // @REGTECHAFRICA

2025 REGTECHAFRICA CONFERENCE & AWARDS

CONFERENCE - EXHIBITION - AWARDS

Theme

UNLOCKING AFRICA'S CROSS-BORDER PAYMENTS, TRADE
AND INVESTMENT OPPORTUNITIES THROUGH PUBLIC
PRIVATE PARTNERSHIPS

MAY 22ND – 23RD, 2025 // LAGOS, NIGERIA

MEDIA PARTNER



CYBER DEFENSE
MAGAZINE

GET A TICKET

WWW.REGTECHAFRICACONFERENCE.COM

PIONEERING PARTNER
BILL & MELINDA
GATES foundation



NDIC
Nigeria Deposit Insurance Corporation
Protecting your bank deposits



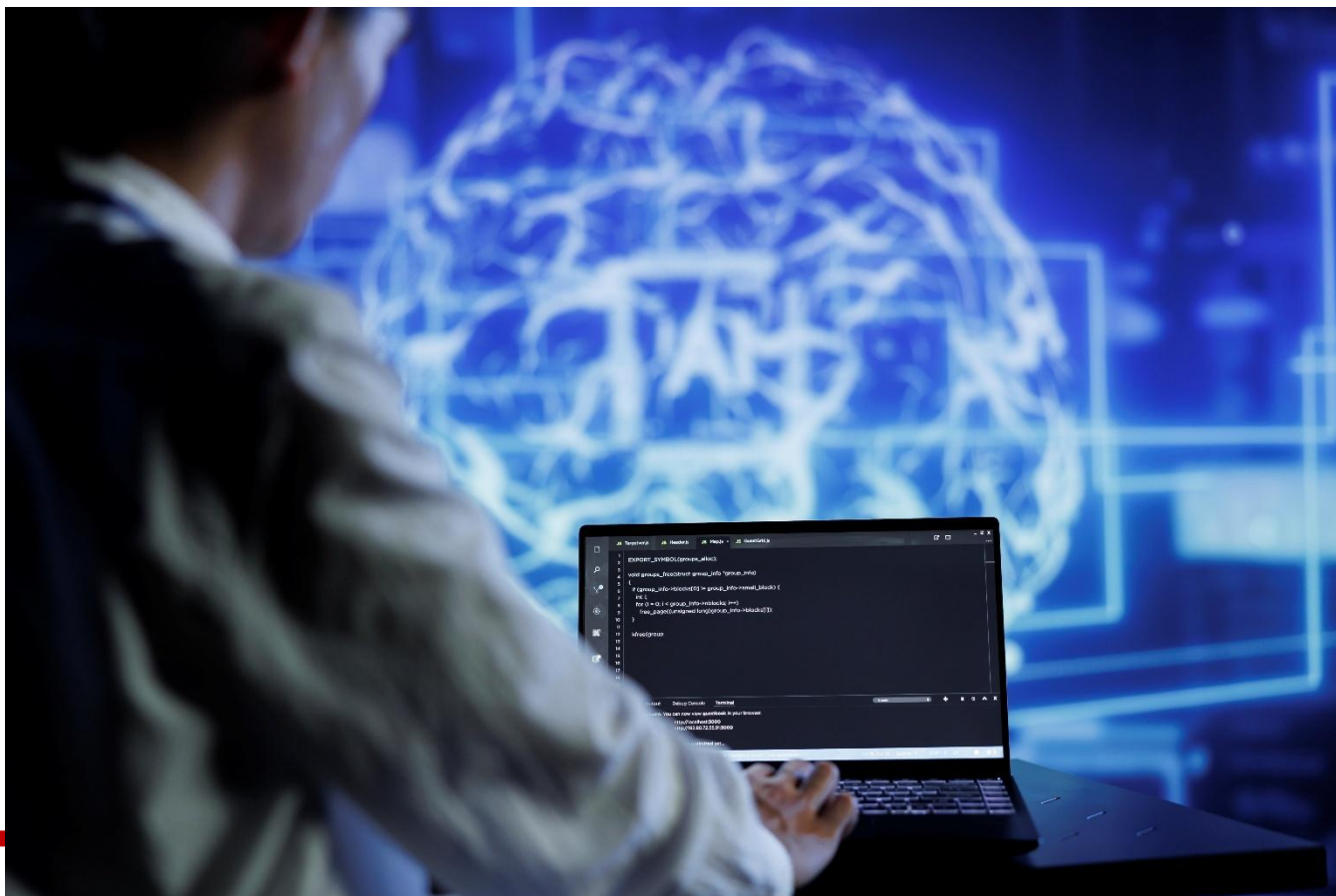
LASAA
Lagos State Asset Management Corporation



air
Alliance for
Innovative
Regulation



**Alliance of Digital Finance
and Fintech Associations**



Cognitive Domain Monitoring, Analysis and Control

By Fernando Escudero, Marketing and Communications, ISID

The importance of cognitive dominance

The information domain has always been of great importance in conflicts, both armed and unarmed. But especially since the Cold War and the emergence of the internet in the early 1990s, along with the advent of mobile technology and simple encryption, the conflict paradigm has changed substantially.

The complexity of 4th generation conflicts, which have become more decentralized than before, has opened up wider and more varied fronts in which it is necessary to engage, in order to control the development of the conflict. Mobile phones and social networks represent an extremely powerful tool for the population to make its opinion known, but they also allow general sentiment to be influenced, if appropriate techniques are employed. Along with the traditional domains of land, sea, air and space (the latter is a recent addition), the cognitive domain is developed in cyberspace and the "weaponry" used is

information (or disinformation) specifically directed at particular targets or groups to elicit reactions that favour the goals of the "attacker" (in the classical sense of the word).

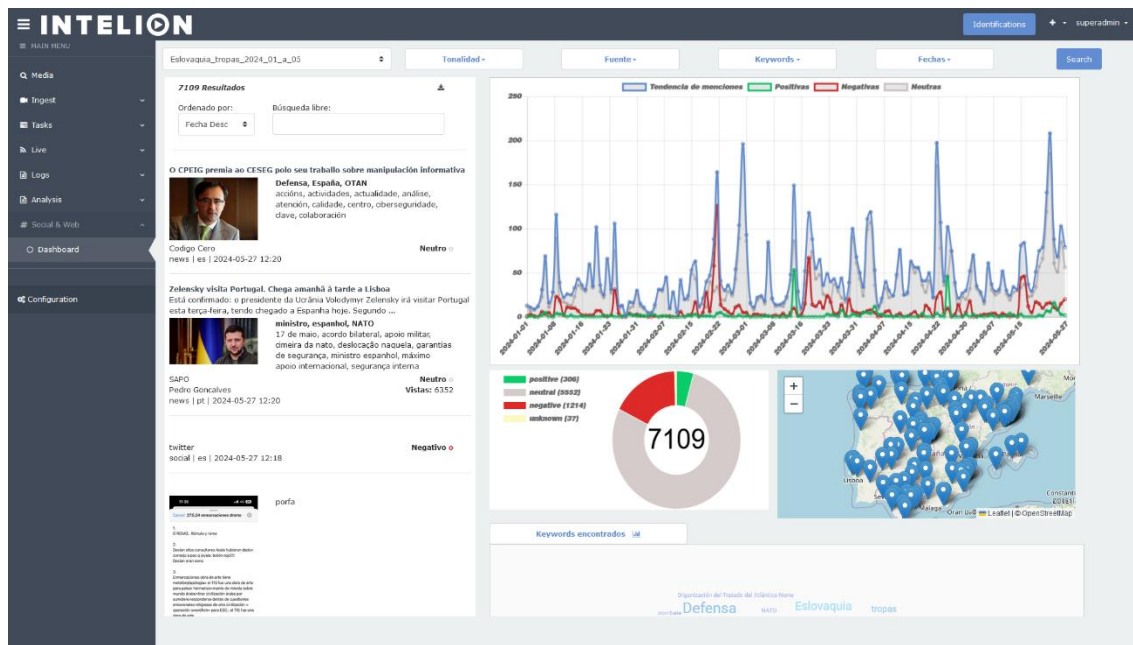
While some proponents already define conflicts that are "conducted through social engineering, disinformation, cyber-attacks, artificial intelligence and autonomous agents" as fifth generation, others lump them squarely into fourth generation. But regardless of the number, the cognitive domain has a clear strategic and tactical role in today's conflicts, especially low-intensity and asymmetric ones.

Monitoring, the first step in controlling the cognitive domain

As in all other military operations, the first step is a reconnaissance of the terrain on which one wants to act, although in this case the "terrain" is virtual. By knowing the state of the news in a geographical area (city, region or country), as well as the sentiment of the population, it is possible to design the appropriate strategies to achieve the desired objectives. In the case of the cognitive domain, these are usually related to forming a favourable or unfavourable opinion about something or assessing how a particular action would impact public opinion.

Such conflicts have a blurred line between political, intelligence and military actions, but this is the current paradigm. Fortunately, thanks to the Internet, monitoring cyberspace related to specific geographic areas is very easy. Platforms such as [Intelion](#) by ISID allow monitoring of open and private radio, television and streaming broadcasts, as well as social networks, automatically locating keywords on a 24/7 basis, with a system of alerts informing designated persons of the latest detections in a timely manner. With the monitoring and analysis of hundreds of simultaneous channels, staffing requirements for surveillance are greatly reduced and are limited to those operatives needed to attend, process and act when detections are made.

AI modules can perform audio transcription, translation of audio if it is not in the desired language, as well as facial or object recognition in video or image broadcasts, or the identification of voices or keywords in communication monitoring. Finally, Intelion can analyse public sentiment regarding certain news or actions using NLP (natural language processing), and determine whether it is positive, negative or neutral.



Intelion analyses the impact and sentiment of online news and social media.

StratCom, the second step

One of the ways to "fight back" in the cognitive domain is through strategic communications. This holistic view of communications uses values and interests to achieve specific objectives. Actions tend to be medium to long term, usually complex, as they take place in a highly competitive environment, such as the Internet, in which there are many other state and private actors, each with their own particular interests.

Given the volatility of current information, Intelion's constant monitoring allows for rapid feedback on the results of the actions carried out, in order to adapt them if necessary. It also makes it possible to gauge the impact of these actions on the public and on online sentiment.

These information conflicts are often quite wide-ranging and can easily cross over from the purely military to the economic and political spheres, which means that the legality of the actions taken must never be lost sight of, within the framework of national security.

Both information operations (INFOOPS) and psychological operations (PSYOPS) are part of the cognitive domain and can affect the economic and social sphere. They can be aimed at deterrence, neutralisation or even aggression, just as in the classic land, sea and air domains, but with very different implications and the possibility of including civilian targets intentionally or collaterally, as the internet does not distinguish to whom a message or news can reach, especially if the medium of transmission is social media.

In many cases StratCom should be used to prevent the dissemination of disinformation, nowadays known as fake news. Neutralising vectors and actors with hostile intent should be the main goal, along with other strategic objectives that advance one's own actions.

Conclusion

Today's military operations are no longer confined exclusively to physical domains, but are now often multi-domain. This requires giving more dimensionality to the strategies employed, because it requires taking into account not only state actors, but also non-state actors. Access to the cognitive domain is no longer limited exclusively to armed forces, but multiple actors, even individuals, can carry out actions that impact on it.

Beyond cyberattacks, impacting the news cycle or public sentiment is possible with some ease and not too many resources, making StratCom increasingly important not only to reinforce self-interest, but also to counter or dampen initiatives by opposing actors. Tools such as Intelion facilitate the analysis of the cognitive domain and make it possible to obtain the necessary intelligence by monitoring 24/7 TV broadcasts, radio, streaming or the social networks themselves, to determine sentiment, locate information vectors and find references to specific actors in a matter of minutes.

[ISID](#) is a Spanish and global company that develops solutions and platforms for the processing, analysis, management and storage of audio and video, whether file-based, streaming or live (TV). Its Intelion platform allows 24/7 monitoring of the cognitive domain, including TV broadcasts, radio, streaming, social networks or websites, analysing public sentiment or performing automatic searches for terms, words, faces or objects, with a system of alerts in case of positive detections.

About the Author

Fernando Escudero is an engineer and has been a technology journalist for over 30 years. He currently works in the Marketing and Communications department at ISID, a Spanish company that develops solutions and platforms for AI-powered audio and video processing and analysis.

Fernando Escudero can be reached online at contact@isid.com and at our company website www.isid.com





Addressing The Need for Integrated FICO-DT Scoring for All Digital Services

Introducing Digital Trust Score (FICO-DT)

By Lalit Ahluwahi, CEO & Founder, DigitalXForce & iTrustXForce

The Digital Trust (FICO-DT) framework is an attempt by DigitalXForce to bridge a critical gap: the absence of a standard metric for measuring and validating the trustworthiness of digital services. By adapting the principles of FICO scoring to digital services, DigitalXForce introduces a quantifiable, standardized method for evaluating the reliability, security, and compliance of online platforms and interactions.

This article explores the growing need for trust metrics in the digital era, the limitations of existing trust validation methods, and how the FICO-DT framework empowers businesses to mitigate risks and foster confidence.

The Current State of Digital Trust

According to ISACA's latest report, "Organizations lack confidence. Only half (53%) are confident in the digital trustworthiness of their organization". See: [2024 State of Digital Trust](#).

On the other hand, Deloitte reveals in recent research that 85% of executives consider digital trust crucial for business success, yet only 40% believe they have adequate measures to assess it. This gap between necessity and capability creates a critical vulnerability in our increasingly digital world. See: [Close the Trust Gap to Unlock Business Value](#)

Financial institutions rely on FICO scores to evaluate credit risk, and organizations now need a standardized, reliable metric to assess digital trustworthiness. Traditional security assessments provide only point-in-time snapshots rather than continuous, dynamic evaluation.

Why We Need a FICO Approach for Digital Services

The traditional FICO score revolutionized lending by providing standardized risk assessment, objective data-driven metrics, continuous monitoring and updates, and clear benchmarks for improvement.

Organizations desperately need these same principles in digital services, where:

- According to Gartner's 2022 Report, most companies take an average of 90 days to complete vendor due diligence. Organizations report difficulty in assessing vendor security posture.
- SecurityScorecard's 2023 report reveals: "98% of organizations globally have relationships with at least one breached third-party. Approximately 10% of third-party vendors receive an F rating among organizations that earn an A rating for their own security posture."
- UK National Cyber Strategy's 2024 Cyber Security Breaches Survey reported that "Half of businesses (50%) and around a third of charities (32%) report having experienced some form of cyber security breach or attack in the last 12 months."
- IBM's Cost of a Data Breach Report shows the average breach cost reached \$4.88 million in 2024.

The DigitalXForce Solution: FICO-DT Scoring

Validating trustworthiness across diverse digital services is increasingly complex, as evolving risks challenge traditional methods. DigitalXForce brings the reliability and clarity of FICO credit scoring to digital service evaluation through our Digital Trust (FICO-DT) scoring system.

By quantifying digital interactions' reliability, FICO-DT ensures trust, thus enhancing transparency and security in an interconnected digital ecosystem. This innovative approach delivers:

1. Real-Time Assessment

FICO-DT monitors digital trust metrics continuously and in real-time, surpassing traditional security audits. Organizations receive current, accurate data about their digital service providers and partners always.

2. Comprehensive Evaluation

FICO-DT examines multiple factors, including security posture and controls, compliance status, historical performance, incident response capabilities, and data protection measures.

3. Quantifiable Metrics

Like FICO scores ranging from 300-850, FICO-DT provides clear numerical rankings that enable organizations to:

- Compare service providers
- Set minimum acceptable thresholds
- Track improvements over time
- Make data-driven decisions



Copyright © 2025 DigitalXForce

Digital Trust Score Ranges

How DigitalXForce Enables FICO-DT Scoring

DigitalXForce leverages the following advanced technologies to power FICO-DT scoring:

i. AI-Powered Analysis

Our proprietary AI ShivAI – XForce GPT – analyzes security tool outputs, compliance data, threat intelligence, performance metrics, and historical data.

ii. **Automated Risk Quantification**

Through direct integration with over 150 security tools, we enable real-time risk assessment, automated compliance mapping, continuous control validation, and dynamic security blueprints.

iii. **Trust but Verify Approach**

The DigitalXForce platform executes a rigorous verification process, including live validation of security controls, continuous monitoring of digital assets, automated policy verification, and real-time compliance testing.

Practical Applications for FICO-DT Scores

Let's consider some practical applications of FICO-DT scores:

1. **Vendor Risk Management**

- Set minimum score requirements for vendors
- Monitor vendor security posture in real-time
- Make data-driven vendor selection decisions
- Automate vendor assessment processes

2. **Service Provider Evaluation**

- Compare security capabilities across providers
- Track provider performance over time
- Identify security gaps and improvements
- Streamline provider onboarding

3. **Internal Security Assessment**

- Monitor internal security posture
- Track security program effectiveness
- Identify areas for improvement
- Demonstrate security ROI

Is FICO-DT Scoring the Future of Digital Trust?

Digital services continue to grow, making standardized trust metrics critical. Our FICO-DT approach advances:

- Digital trust assessment standardization
- Security evaluation automation
- Data-driven decision making

- Digital ecosystem security improvement

But why is this important? A recent ISACA report reveals a stark reality: “82% of organizations say digital trust will be even more important in the next five years.” With DigitalXForce leading this transformative shift, organizations can now navigate the complexities of digital trust with clarity and assurance.

Organizations using DigitalXForce’s FICO-DT scoring report a 40% reduction in vendor assessment time, 60% improvement in risk visibility, 30% decrease in security incidents, and significant improvement in board-level security reporting.

Conclusion

FICO scoring integration transforms cybersecurity and digital trust. The DigitalXForce FICO-DT framework equips organizations with essential tools to evaluate, monitor, and improve digital trust across their ecosystem. As digital transformation accelerates, this standardized approach to measuring digital trust becomes increasingly vital for business success.

FICO scores transformed credit risk assessment, and now FICO-DT transforms how organizations approach digital trust. At DigitalXForce, we empower organizations to make informed decisions about their digital services and partners by providing clear, quantifiable metrics and continuous monitoring.

With the FICO-DT framework, we are ultimately building a more secure and trustworthy digital ecosystem.

About the Author

Lalit Ahluwalia is the CEO and Founder of DigitalXForce and iTRUSTXForce. He is the Commander-in-chief of the XForce Galaxy and is committed to redefine the future of cybersecurity by adding the new tenant “T - Trust “. Under his leadership, DigitalXForce and iTRUSTXForce leverages automation, AI/ML and innovative methods to bring tailored next gen cybersecurity solutions for its clients. Lalit is a Cybersecurity Servant Leader with professional track record of helping his clients be resilient in the face of constantly evolving cyber threat landscape.

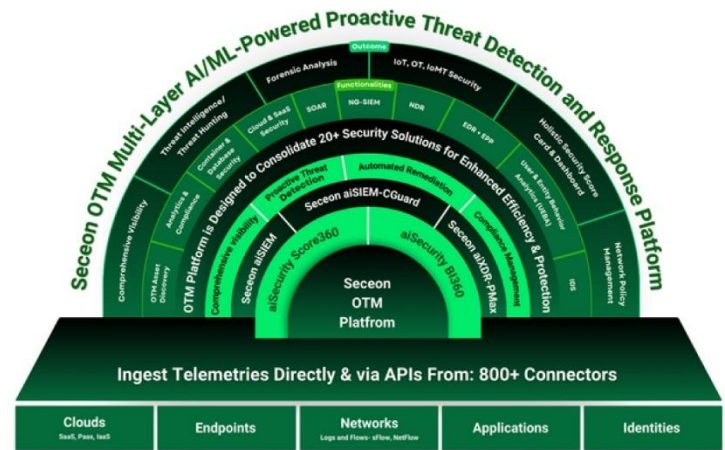


He is fully committed to redefine the future of Cybersecurity and help organizations of all sizes become Cyber Resilient Inside Out. In his own words, “Cybersecurity doesn’t have to be Complex or Costly Affair”. It’s rooted in his beliefs that “business isn’t about what you can get out of it, it’s about what you can give through it which would make an Impact in Community and People’s lives”.

Lalit can be reached online at EMAIL lalit.ahluwalia@cyberxforce.com, TWITTER <https://twitter.com/LalitKAhluwalia>, LINKEDIN <https://www.linkedin.com/in/lalit-ahluwalia/>, and at our company website www.digitalxforce.com & www.itrustxforce.com



The Cybersecurity Game Changer



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/>



Bridging The Cybersecurity Skills Gap: Why Partnering with An MSSP Is A Strategic Imperative

By Sachin Jain, Sr. Vice President Technology, Eventus Security

The Evolving Threat Landscape

The global cybersecurity landscape is undergoing a seismic shift, with threats becoming more sophisticated, persistent, and damaging. Cybercriminals now leverage AI, automation, and advanced attack techniques to exploit vulnerabilities at an unprecedented scale. Organizations today face a relentless wave of cyberattacks, including ransomware campaigns, supply chain breaches, and nation-state-sponsored intrusions.

These escalating threats pose significant risks—financial losses, reputational damage, and regulatory penalties. However, organizations are not just battling external attackers; they are also struggling with internal challenges such as alert fatigue, fragmented security tools, and a shortage of skilled professionals to detect and respond to incidents effectively.

The Growing Cybersecurity Skills Shortage

Compounding this challenge is the global cybersecurity talent deficit, which has reached a critical level, particularly in North America. Reports indicate that over 750,000 cybersecurity positions remain unfilled in the U.S. alone, leaving organizations without the expertise required to defend against modern cyber threats.

As attackers refine their methods, organizations without adequately staffed security teams find themselves at a severe disadvantage. Cyber defense gaps widen, increasing the likelihood of breaches that could compromise sensitive data and disrupt operations. Given the scale and complexity of today's threats, businesses must seek alternative strategies to secure their digital assets.

The Strategic Advantage of Partnering with an MSSP

In this evolving threat environment, Managed Security Service Providers (MSSPs) have emerged as a critical force multiplier for businesses seeking to strengthen their security posture. By offering expertise, advanced threat detection technologies, and 24/7 monitoring, MSSPs enable organizations to mitigate risks proactively and close the cybersecurity skills gap.

For enterprises serious about resilience, partnering with an MSSP is no longer just an option—it is a strategic necessity. MSSPs like Eventus Security provide a competitive edge by delivering comprehensive security solutions, integrating cutting-edge technologies, and deploying expert personnel to proactively defend against evolving cyber threats.

1. Access to Specialized Expertise

Cybersecurity requires niche expertise across multiple domains, from threat intelligence to compliance. MSSPs provide on-demand access to highly skilled professionals, eliminating the challenges of hiring, training, and retaining in-house security teams. These experts continuously monitor threats and respond to incidents, ensuring robust security.

2. Cutting-Edge Security Technology

Deploying and maintaining enterprise-grade security solutions can be costly. MSSPs offer next-gen tools, including XDR, SIEM, and SOAR, without the capital investment required for in-house solutions. The Eventus XDR-powered SOC integrates AI-driven analytics and machine learning for proactive threat detection and mitigation, ensuring comprehensive security across endpoints, cloud, email, and network infrastructures.

3. 24/7 Monitoring and Threat Response

Cyberattacks don't follow business hours. MSSPs provide round-the-clock monitoring and real-time incident response, ensuring continuous protection. Eventus's Cyber Defense Center (CDC) operates 24/7, identifying and neutralizing threats before they escalate, providing organizations with peace of mind.

4. Scalability and Cost Efficiency

Building an in-house security operations center (SOC) requires significant investment in talent acquisition, training, and technology. MSSPs offer a cost-effective, scalable alternative, allowing organizations to customize security services based on their evolving needs.

5. Simplified Compliance Management

With increasing regulatory scrutiny on data security, businesses must navigate complex compliance landscapes. MSSPs have deep expertise in industry regulations, ensuring organizations remain compliant while reducing the risk of costly penalties. Eventus Security's compliance-driven approach streamlines adherence to regulatory requirements.

Choosing the Right MSSP: Key Considerations

Selecting an MSSP is a critical decision that impacts an organization's cybersecurity resilience. Here are key factors to evaluate:

1. **Security Operations Maturity:** Use the Gartner Hype Cycle for Security Operations as a reference for assessing MSSPs.
2. **Technology Stack:** A next-gen MSSP should integrate XDR, SIEM, and SOAR, creating an AI-driven SOC.
3. **Scalability:** The MSSP should offer cloud-ready, scalable solutions that adapt to business growth.
4. **Expert-Led Threat Hunting:** Look for an MSSP with dedicated Threat Hunters and Incident Responders, not just SOC analysts.
5. **Integration Capabilities:** The MSSP should seamlessly integrate with existing security tools, simplifying management.
6. **Threat Intelligence:** A top-tier MSSP provides actionable threat intelligence and integrates feeds into security operations.
7. **Vulnerability Management:** The MSSP's approach should focus on prioritizing and remediating risks efficiently.
8. **Automation & AI:** The MSSP's platform should leverage automation to reduce false positives and enhance efficiency.
9. **Tailored Security Services:** The provider should customize services to address an organization's unique security challenges.
10. **Proven Track Record:** Evaluate the MSSP's history, successful implementations, and industry reputation.

The Eventus Security Advantage:

Eventus Security stands out as a trusted MSSP, delivering world-class cybersecurity solutions through a blend of technology, expertise, and customer-centric service.

- **Proprietary Eventus Platform** – A unified, AI-driven security platform integrating advanced threat intelligence, automation, and analytics for real-time cyber risk mitigation.
- **Proven Track Record** – With **1,000+ man-hours of incident response experience**, **150+ SOC projects**, and **2,500+ threat advisories issued**, Eventus has a history of delivering resilient security operations.
- **Global Presence with Local Expertise** – A **300+ strong team**, including **150+ cybersecurity specialists**, with dedicated SOCs in **Mumbai, Ahmedabad, and Riyadh**, ensuring region-specific solutions and global reach.
- **Comprehensive Service Portfolio** – Award-winning services including Managed XDR, SOC-as-a-Service, a suite of Cyber Resilience services including BAS, Continuous Automated Red Teaming(CART), Penetration Testing as a Service (PTaaS), and Incident Readiness & Response.

Conclusion: Can You Afford NOT to Partner with an MSSP?

The cybersecurity skills shortage is a pressing issue, but it doesn't have to leave your organization vulnerable. Partnering with a trusted MSSP like Eventus Security enables businesses to bridge the talent gap, enhance their security posture, and focus on their core operations without compromising cybersecurity.

In today's evolving threat landscape, the question is not whether you can afford to partner with an MSSP—it's whether you can afford not to. Let Eventus Security be your strategic cybersecurity partner in navigating the complexities of modern cyber threats.

About the Author

Sachin Jain is a seasoned Technology and Cybersecurity leader with over 25 years of experience in the professional services and technology industry. He currently serves as **SVP – Technology & Business Development at Eventus Security**, having previously held executive roles as **Founder, CEO & CTO at Cognyse** and **Global CIO & CISO at Evalueserve**, where he led global technology and cybersecurity functions for over two decades.



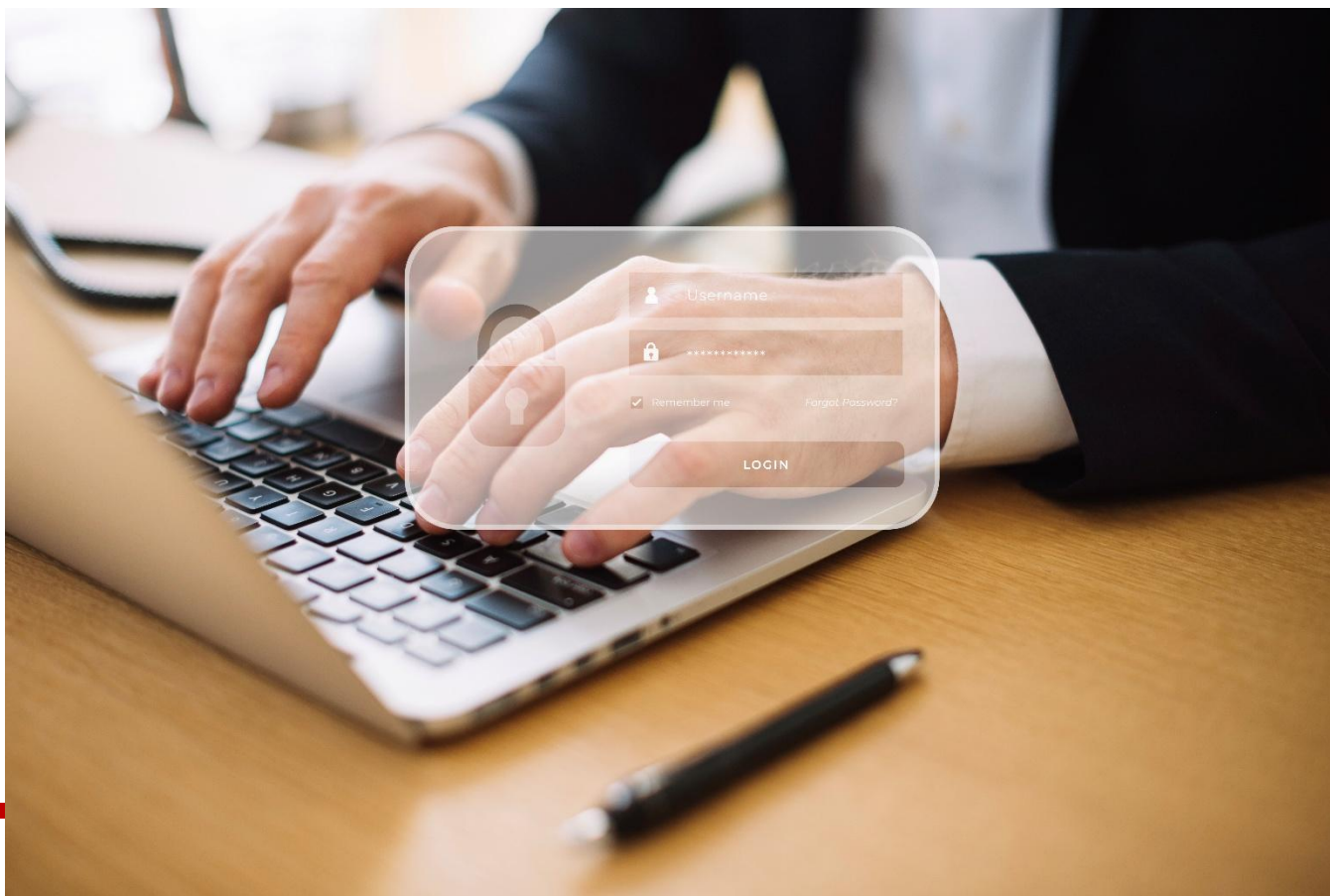
With deep expertise in **cybersecurity, risk management, cloud computing, automation, managed services, and data governance**, Sachin has successfully developed and executed robust security strategies to protect organizations from evolving cyber threats. His **practical, results-driven approach** has helped businesses navigate complex challenges, mitigate risks, and implement innovative solutions. His experience spans **cybersecurity strategy, threat intelligence, incident response, security architecture, business continuity management, and governance, risk, and compliance (GRC)**.

A recognized **industry thought leader**, Sachin has received multiple **awards** for his contributions to **innovation, business impact, technology transformation, and cybersecurity**. He actively engages in **industry forums, media, and CXO conferences** to share insights and drive thought leadership in the cybersecurity space.

Sachin holds a **science degree and an MBA** and is an **alumnus of the Indian School of Business**. He has also completed executive programs in **Leadership, Cybersecurity, Data Science, Digital, and Cloud Computing** at leading institutions in India and the USA.

Sachin can be reached online at LinkedIn [linkedin.com/in/jainsachin16](https://www.linkedin.com/in/jainsachin16) or through hello@eventussecurity.com.

For more information about Eventus Security, please visit: www.eventussecurity.com



Streamlining PCI DSS 4.0.1 Adoption in 2025

By Héctor Guillermo Martínez, President of GM Sectec

In 2025, the Payment Card Industry Data Security Standard (PCI DSS) 4.0.1 is the current benchmark for securing international credit and debit card transactions. Is your business effectively navigating its adoption?

PCI DSS 4.0.1 is the evolved version of the standard, designed to protect payment card information and mitigate fraud. While PCI DSS 4.0 was initially released in March 2022, the 4.0.1 update, released in June 2024, clarifies and refines requirements, making it the definitive standard to adhere to.

This version emphasizes security goals, offers greater flexibility in achieving compliance, introduces robust multi-factor authentication and online security measures, and places a strong emphasis on risk assessment and continuous security evaluation.

Compared to PCI DSS 3.2.1, PCI DSS 4.0.1 involves:

1. A focus on security objectives rather than solely prescriptive controls.
2. Enhanced flexibility to accommodate diverse compliance approaches.
3. Mandatory multi-factor authentication (MFA) and strengthened online security.
4. Updated terminology to align with current technological landscapes.
5. Refined compliance assessment and auditing, including a continuous assessment model.
6. A robust focus on risk assessment and ongoing security monitoring.
7. Increased scrutiny of supply chain security and vendor management.
8. Streamlined requirements for easier comprehension and implementation.
9. Heightened emphasis on data privacy and personal information protection.
10. Continuous compliance, not just annual audit preparation.

Accelerating Your Migration to PCI DSS 4.0.1

As 2025 progresses, companies must prioritize a smooth transition to PCI DSS 4.0.1. Procrastination is not an option.

Organizations need a strategic partner equipped with cutting-edge technology and expert consulting to streamline PCI compliance validation across all payment channels. This partner should offer a comprehensive service portfolio and a specialized certification program to support diagnosis, auditing, consulting, and certification, ensuring optimal compliance.

With the guidance of an expert partner, your team can:

1. Comprehend the nuances of PCI DSS 4.0.1 and its impact on your operations.
2. Conduct a thorough GAP analysis to assess your current compliance level.
3. Develop a detailed implementation plan to address compliance gaps.
4. Allocate sufficient resources for a seamless transition.
5. Ensure vendors and partners are aligned with PCI DSS 4.0.1 requirements. Partnering with a QSA-certified company is highly recommended.
6. Provide comprehensive training on PCI DSS 4.0.1 changes.
7. Perform rigorous testing and audits before official assessment.
8. Prepare meticulously for the formal compliance assessment.

The shift from PCI DSS 3.2.1 to 4.0.1 is a strategic investment in enhanced payment card data security, flexibility, and a risk-based approach. While it demands resources, it ultimately delivers superior protection and peace of mind for both customers and businesses.

About the Author

Héctor Guillermo Martínez is President and Board Member at GM Sectec. Hector G is responsible for the growth, vision, and execution of the company. GM Sectec creates innovative tailored solutions that help accelerate business breakthroughs in the areas of cyber defense, managed detection and response services, digital forensics, multi-tenancy, business continuity, information security, automation, and process orchestration to ultimately deliver outstanding cost efficiencies to our customers and partner community. GM Sectec is a global company with Headquarters in Puerto Rico and offices in Florida, Mexico, Panama, Colombia, Brazil, Chile, Spain, and Australia with clients in over 50 countries. Hector G. has an MBA from CUNY, Zicklin School of Business, and is an alumnus of Harvard Business School.



Héctor Guillermo can be reached online at [LinkedIn](#) and in X @HGMartinez and at our company website 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 RESEARCH
TECHNOLOGY AND RESEARCH
INSTIT & POLYTECHNIC
UNIVERSITY OF FR



PREFERRED PARTNER



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



21 – 23
MAY 2025
MESSE BERLIN
— SOUTH ENTRANCE —

FEATURING



Germany's Largest Tech, Startup & Digital Investment Event

2,000+
EXHIBITORS

1,000+
STARTUPS

800+
INVESTORS

100+
COUNTRIES

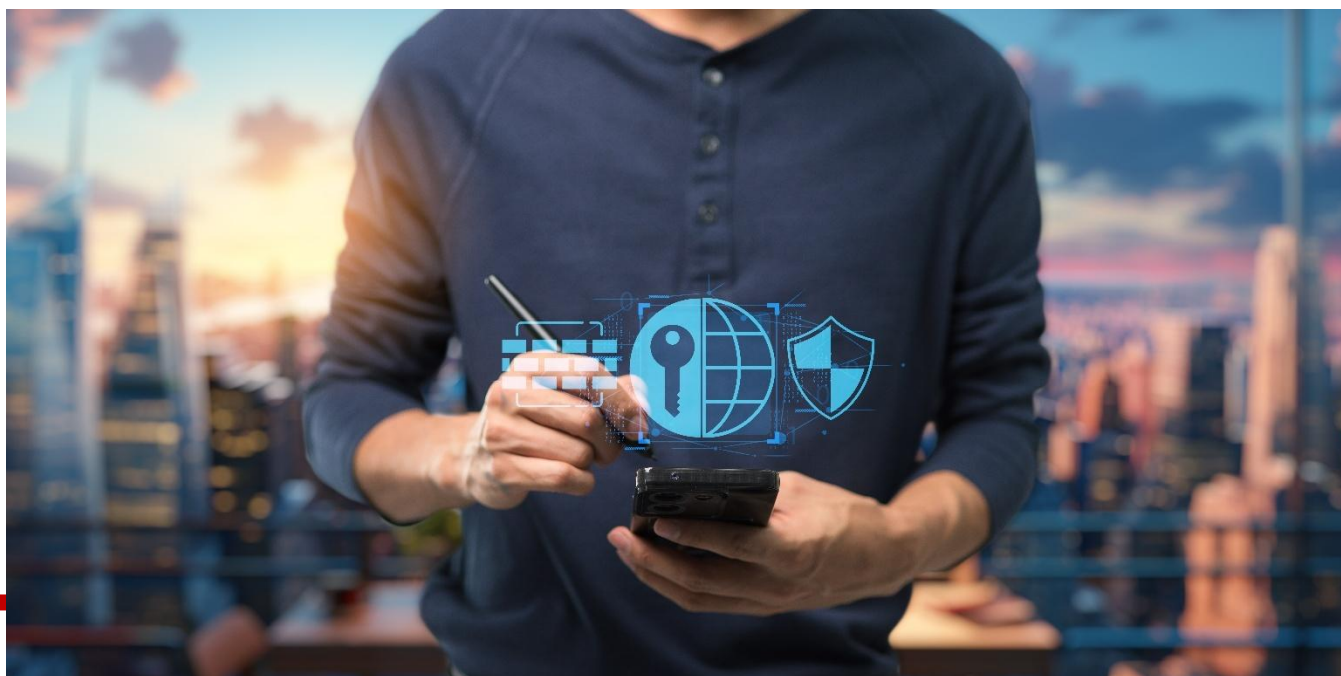
ENDORSED BY



GET INVOLVED



#GITEXEUROPE
gitex-europe.com



Next-Generation Data Protection: What Is it? Why Should Enterprise Tech Buyers Care?

By Eric Herzog, CMO of Infinidat

When a cyberattack happens, such as a ransomware or malware attack, the CEO and the entire senior leadership team of an enterprise anywhere in the world want to know how fast the business can recover. It is a critical issue for all enterprises.

In the U.S. and Europe, if an organization has been hit by a cyberattack, it is required to file legal documentation, which means companies have to reveal the impact of the cyberattack. Recently, in the U.S., a large enterprise noted in their public filing that a cyberattack cost them \$2.9 billion — a huge and unplanned expense.

This reality has put data protection in a bigger spotlight. Because companies continue to pay the ransom for data that has been taken “hostage” or pay for the damages caused by a largescale cyberattack, it’s clear that the conventional approach to data protection is not effective at combating cyber threats. They need to be augmented by something else that complements it with newer, more effective capabilities.

This is where next-generation data protection comes in.

What is Next-Generation Data Protection?

Next-generation data protection was built with today's most sophisticated and dangerous cyberattacks as a primary issue to fix. It expands the purview of what is protected and how it is protected within an enterprise data infrastructure. It adds preemptive and predictive capabilities that help mitigate the effects of massive cyberattacks.

Moreover, next-generation data protection is the last line of defense against the most vicious, unscrupulous cyber criminals who want nothing more than to take down and harm a large company, either for monetary gain or a notch on their belt. It's truly important to understand what next-generation data protection is.

If you are only going to remember one thing from this article, remember the point in this paragraph: Next-generation data protection includes the traditional aspects of data protection, such as being able to handle backup repositories and being able to snapshot and replicate data. But the next generation of data protection includes cyber storage resilience and ultra-rapid cyber recovery. That's it!

To expand on it, next-gen data protection provides a cyber-focused, recovery-first methodology. Immutability of the data is key. It calls for true immutability of data. You have to have immutable copies of data, so you can analyze it without the possibility of the data being compromised after a cyberattack.

This goes far beyond the traditional outlook, which basically only saw immutability as a compliance issue or would even have a "backdoor" to circumvent the immutability and be able to unlock the data – a measure that leaves open the possibility of compromise and misuse. However, with next-gen data protection, preserving true immutability is key to recovery. The data cannot be altered or changed in any way. There is no "backdoor."

"Recovery-first" means the endpoint has to be first. How can you leverage immutable snapshots to do your recovery as quickly as possible? Leverage immutable snaps and make sure that the data is proactively verified and validated. So, you don't have to do it after the fact.

To make data protection highly effective today for the datasets that you deem most critical, it has to be highly integrated and orchestrated. You don't want a manual process making a weak spot for your organization. To resolve this issue, one of the breakthrough capabilities of next-generation data protection is automated cyber protection.

Automated cyber protection seamlessly integrates cyber storage resilience into a cyber security operation center (SOC) and data center-wide cyber security applications, such as SIEM and SOAR cyber applications. At the first signal of a cyberattack, an immutable snapshot of your data is taken automatically. There is no manual process of the security team calling up the storage admin to say that there is a potential cyberattack underway. It's now all automated, merging data center cybersecurity with cyber resilient storage.

Indeed, automated cyber protection is the thing that paves the way to rapid cyber recovery because it kicks off the process of obtaining a known clean copy of data that can be validated as 100% free of corruption.

Why Should Enterprise Tech Buyers Care?

Now that you know what next-generation data protection is vs traditional / modern data protection schemes, the next question is: why should you care?

The answer revolves around your gaining leverage over cyber attackers by taking a cyber focused, recovery-first approach, which will enable you to get your data back in as quickly as the snap of your fingers. Literally! We have publicly recovered >2 PB of data in ONLY four seconds. Now that is a Recovery Time Objective (RTO)!

Below are five points that give you reasons to care:

[1] *Achieving the best possible outcome if you get attacked by malware or ransomware.*

- A cyber-focused, recovery-first methodology is a proven approach to making the best of a bad situation. You know your organization will get hit with an attack at some point, if not already. You can recover, if you take an outcome-centric viewpoint that guides your next move.

[2] *Backups are target attack points.*

- If cybercriminals compromise your backup system, they will disable them before they corrupt your data on primary storage. This is the reason you have to be proactive and do it on an ongoing basis. Conventional backup systems are optimized for backup, not for restore. The size and amount of data that needs to be recovered is not a great situation for traditional restore methodologies. They are slow and cumbersome. You have to restore data back to every individual server, which is time-consuming and complex. Next-generation data protection solves these challenges.

[3] *When you think about recovery first, protecting the data becomes easier.*

- Being proactive to optimize for restoration of data makes it simpler on the backend. You won't be caught flat-footed. It's a must-have knowing that your company has the appropriate amount of automation to safeguard your data infrastructure. With automated cyber protection and cyber detection on primary storage, you — and the CIO, CTO, CEO, and CFO — will sleep better at night.

[4] *Get your data back in the snap of your fingers.*

- Recovery of data has to be fast. Indeed, it needs to be ultra-fast. If it's slow (i.e. days to recover data), then it's not working at the speed of enterprise business. It's not working at the speed of compute. With the right cyber storage resilient capability built into your storage infrastructure, you can get your data back within seconds.

[5] *You have gained leverage back from the attackers.*

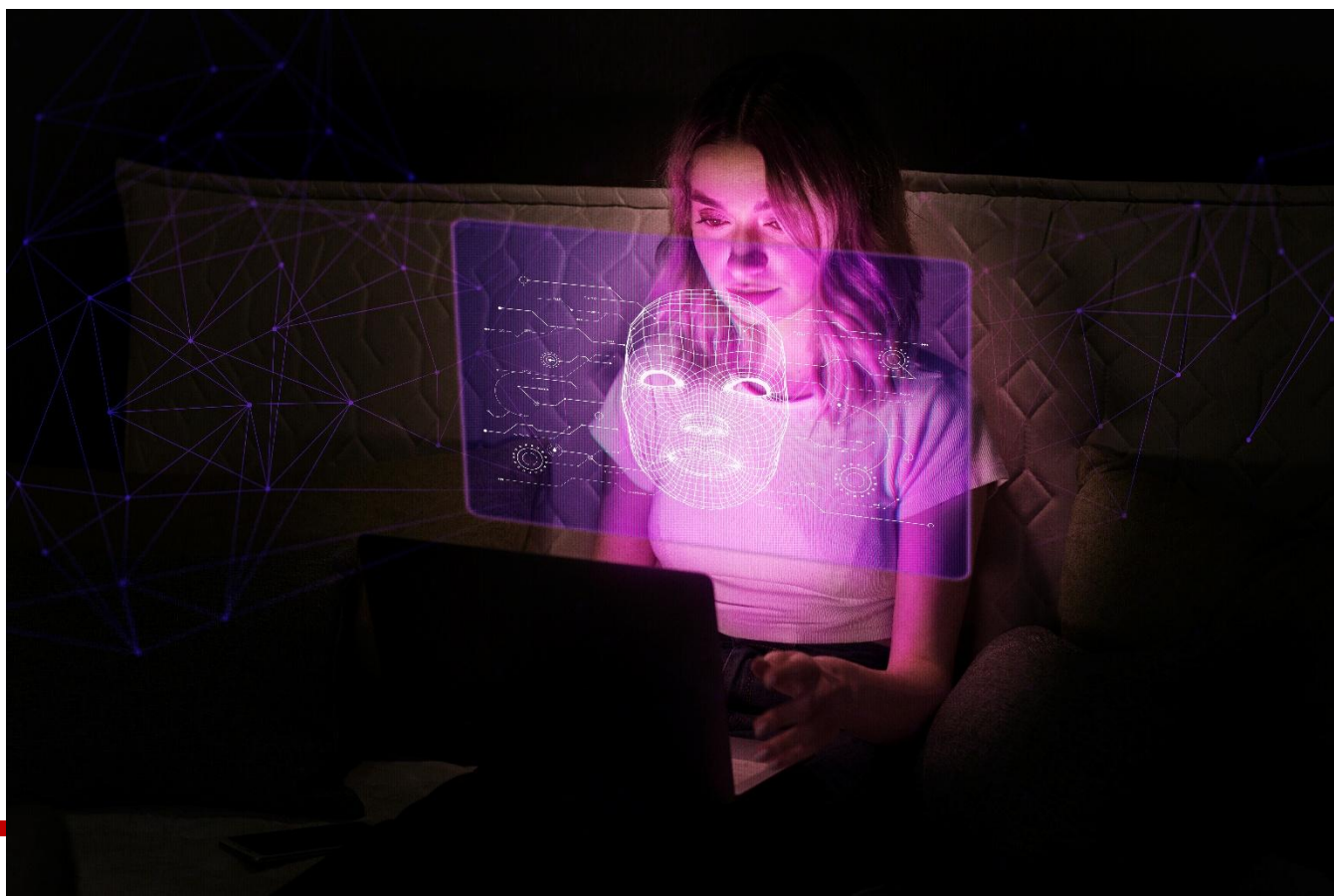
- Do not underestimate your ability to gain an advantage on cyber criminals. Cyber resilient storage is the first place to look for your tool to gain leverage.

Don't settle for bolt-on solutions. Bolt-ons simply help to show what is happening in backup. Instead, you need cyber storage resilience to be built into the primary storage systems. It's best to put cyber recovery at the forefront of your thinking.

About the Author

Eric Herzog is the Chief Marketing Officer at Infinidat. Prior to joining Infinidat, Herzog was CMO and VP of Global Storage Channels at IBM Storage Solutions. His executive leadership experience also includes: CMO and Senior VP of Alliances for all-flash storage provider Violin Memory, and Senior Vice President of Product Management and Product Marketing for EMC's Enterprise & Mid-range Systems Division. Eric can be reached online at @zoginstor on X or <https://www.linkedin.com/in/erherzog/> on LinkedIn and at our company website www.infinidat.com.





Cyber Risks Associated with Adoption of Generative AI Tools

Steps Your Organization Can Take to Eliminate Breach and Other Risks

By Dustin Hutchison, Senior Vice President of Services and CISO, Pondurance

As artificial intelligence (AI) continues to revolutionize the business landscape, mid-sized organizations find themselves at a crossroads, balancing the transformative potential of AI against the heightened risks it introduces. While forward-thinking companies leverage generative and agentic AI to enhance operational efficiency, they must remain vigilant against the growing sophistication of AI-driven cyber threats.

In this piece, we will explore the vulnerabilities associated with AI, offer frameworks for assessing AI-related risks, and detail best practices for safeguarding organizational data. As a finalist for SC Awards 2025 Best Managed Detection and Response (MDR) Service, Pondurance is dedicated to equipping organizations with the tools they need to eliminate breach risks in this ever-evolving threat landscape.

Understanding the Vulnerabilities of Generative AI in Cybersecurity

AI serves as a double-edged sword for midsize organizations, empowering them to innovate while simultaneously exposing them to new vulnerabilities. Key risks arising from generative AI include:

1. **Enhanced Cyberattacks:** Cybercriminals are leveraging AI to execute more effective and challenging-to-detect attacks. AI algorithms streamline the gathering of open-source intelligence, enabling attackers to craft highly personalized phishing attempts that mimic legitimate business communications.
2. **Internal Data Risks:** As organizations incorporate AI tools into their workflows, the handling of sensitive information becomes a critical concern. Using open-source AI applications can expose confidential data if not carefully managed.

The Impact of Smarter Cyberattacks

AI increases the effectiveness of cyberattacks by facilitating sophisticated phishing techniques that produce messages indistinguishable from authentic communications. The rise of business email compromise (BEC) scams exemplifies this threat, where attackers, utilizing generative AI capabilities, can create convincing correspondence that evades detection.

Additionally, emerging technologies like deepfake voice and video complicate the verification process, rendering traditional methods, such as phone calls, less reliable and creating new opportunities for deception.

Assessing AI Risks: A Framework for Organizations

To address the risks presented by AI adoption, organizations must implement a structured approach to risk management. The World Economic Forum's recent report outlines essential questions for business leaders to consider:

- Is there a clear understanding of risk tolerance among stakeholders?
- How are the risks of AI weighed against potential rewards?
- Are effective governance policies established for the deployment of AI projects?
- Are organizations aware of their unique vulnerabilities associated with AI technologies?

At Pondurance, we encourage adherence to established standards such as the NIST Cybersecurity Framework (CSF) 2.0 and NIST SP 800-53. These frameworks provide essential governance structures for AI security, ensuring comprehensive protection measures.

A Risk-Based Approach: The Foundation of Our MDR Services

In the current threat landscape, organizations must adopt a risk-based methodology for cybersecurity. Our managed detection and rResponse (MDR) service is tailored to tackle the unique challenges posed by AI-driven cyber threats. By employing a risk-based strategy, Pondurance enables organizations to:

- **Prioritize Cybersecurity Investments:** Identify and assess vulnerabilities, allowing organizations to allocate resources effectively where they are needed most.
- **Foster Continuous Monitoring:** Provide ongoing surveillance of your environment, ensuring real-time identification and response to potential threats.
- **Enhance Incident Response:** Equip organizations with robust incident response plans that adapt to emerging threats, including AI-driven attacks.

By integrating risk management into our MDR architecture, we empower organizations to respond proactively to the evolving landscape of cyber threats while minimizing risks associated with their adoption of generative AI technologies.

Best Practices for Secure AI Implementation

As organizations deploy AI technologies, adhering to these best practices can significantly reduce breach risks:

- **Integrate AI Governance:** Align AI governance policies with acceptable use policies to strengthen data protection initiatives.
- **Enhance Cybersecurity Training:** Implement ongoing training programs that address emerging threats, particularly those posed by AI advancements.
- **Conduct Regular Vendor Assessments:** Establish robust vendor risk assessment practices for third-party AI access, ensuring continuous evaluation.
- **Strengthen User Access Controls:** Limit access to sensitive data and improve identity management practices to mitigate risks associated with AI-generated attacks.
- **Adopt a Zero Trust Approach:** Ensure that all access points, including third-party applications, adhere to zero trust principles.

Embrace AI Responsibly

AI is now an integral aspect of business operations, and mid-sized organizations must adopt its capabilities with a strategic focus on security and compliance. As a finalist for Best MDR Services, Pondurance is committed to guiding organizations on their cybersecurity journey. Our innovative platform offers tailored managed detection and response solutions designed specifically to protect sensitive data against AI-fueled threats.

By establishing a proactive cybersecurity posture today, organizations can reap the benefits of AI while effectively managing the associated risks of tomorrow.

About the Author

Dustin Hutchison is the Vice President of Services and Chief Information Security Officer at Pondurance. Dustin has over 20 years of experience in information security, risk management, and regulatory compliance. Prior to joining Pondurance, Dustin was a risk and compliance professional focusing on HIPAA, Payment Card Industry Data Security Standard, and risk assessments for new technology acquisitions ranging from infrastructure solutions to patient care devices. Dustin is also currently an adjunct professor at Ivy Tech Community College, Sullivan University, Embry-Riddle Aeronautical University, and University of the Cumberlands, teaching undergraduate through doctoral level technology and cybersecurity courses. Dustin's Ph.D. dissertation topic focused on the adoption of cloud computing in healthcare. Dustin can be reached at our company website <https://www.pondurance.com/>



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



7 Benefits of Using RPAM In Multi-Cloud Security

Centralize and secure privileged remote access across AWS, Azure, GCP, and private clouds with RPAM to strengthen your multi-cloud security.

By Roy Kikuchi, Director of Strategic Alliances at Safous, Internet Initiative Japan (IIJ) Inc.

Business leaders are no longer asking whether to move to the cloud—they're deciding how best to manage multiple cloud environments. According to Flexera's 2024 State of the Cloud Report, **nearly 90% of organizations have already adopted a multi-cloud strategy.**¹ This widespread adoption makes sense: leveraging two or more cloud platforms can help businesses build more scalable, flexible, and resilient operations.

Unfortunately, managing access to sensitive data becomes increasingly complex as organizations spread resources across multiple cloud providers. This guide will explain how [Remote Privileged Access Management \(RPAM\)](#) can help you overcome these challenges and strengthen multi-cloud security.

What Is RPAM's Role in Multi-Cloud Security?

A 2024 survey found that **65% of business leaders say cloud security is their organization's top priority.**² RPAM – a cybersecurity solution that protects and controls remote access to privileged data and systems – is a critical component in protecting cloud environments. It ensures that only users with proper authorization can access sensitive resources while maintaining strict security controls against unauthorized activity.

In multi-cloud environments, RPAM centralizes remote access management across Google Cloud Platform (GCP), Amazon Web Services (AWS), Microsoft Azure, and private cloud infrastructures. This unified approach eliminates the security gaps that often appear when organizations handle identity management and access policies separately for each platform.

Security Challenges in Multi-Cloud Environments

Multi-cloud environments come with their own set of security hurdles that increase breach risks, which could be why **40% of data breaches in 2024 involved data stored across multiple cloud environments.**³ Some of the most common multi-cloud security challenges include:

Identity Sprawl

Managing privileged accounts across multiple cloud providers creates identity sprawl, where credentials are scattered across various platforms. This makes it difficult to track access rights and identify security vulnerabilities.

Unauthorized Access Risks

Without strict access controls, cybercriminals can exploit misconfigured permissions to gain unauthorized access to cloud resources. Insider threats, compromised credentials, and supply chain attacks multiply this risk.

Compliance and Audit Challenges

Modern businesses must navigate regulations like GDPR, HIPAA, PCI-DSS, and ISO 27001, which demand strict control over privileged access. Multiple cloud platforms with different policies make maintaining and demonstrating compliance particularly difficult.

Lack of Centralized Monitoring

Traditional security solutions fail to provide complete visibility across multiple cloud platforms. Security teams need real-time monitoring and session tracking capabilities for effective threat detection and response.

7 Ways RPAM Strengthens Multi-Cloud Security

RPAM offers a unified, secure approach for managing remote privileged access in cloud environments. Here's how:

1. Centralized Access Management

RPAM consolidates privileged access management across multiple cloud platforms to ensure consistent and enforceable security policies. Features like role-based access control (RBAC) and least privilege principles enable organizations to maintain consistent security policies while limiting user access to only the resources users need.

2. Secure Credential Management

RPAM reduces the risk of account exposure by storing privileged credentials through secure vaulting and encryption. Regular automated password rotation adds an extra layer of protection against credential compromise.

3. Privileged Session Monitoring

Real-time session monitoring makes it easy to track privileged activities in the cloud as they happen. Security teams can watch user actions, spot unusual behavior, and generate audit logs for compliance purposes.

4. Advanced Access Controls

RPAM offers advanced access controls like just-in-time (JIT) privileged access, which grants users temporary permissions only when needed. It also works with multi-factor authentication (MFA) solutions to verify user identities before granting access. Even if credentials fall into the wrong hands, unauthorized users remain locked out of privileged accounts.

5. Automated Policy Enforcement

RPAM automatically enforces security policies across all cloud platforms, which eliminates human error and helps ensure consistent security standards. Additionally, the system can revoke access when suspicious activities are detected, or access periods expire.

6. Cross-Platform Activity Correlation

Advanced RPAM solutions can correlate user activities across different cloud platforms to help security teams identify potential threats that might go unnoticed when examining each platform separately.

7. Emergency Access Management

RPAM provides controlled break-glass access procedures for emergency situations, ensuring organizations can quickly grant necessary access during incidents while creating detailed audit trails of emergency access events.

How Can Businesses Use RPAM in Cloud Security?

There are several ways businesses use RPAM to enhance their multi-cloud security strategies, including:

Insider Threat Prevention

Insider threats pose a major security risk in cloud environments, with **83% of organizations reporting at least one insider attack in 2024**.⁴ RPAM mitigates this risk by monitoring privileged access, enforcing strict session controls, and detecting suspicious activities in real time.

Cloud Infrastructure Management

Cloud administrators and DevSecOps teams often need remote privileged access for infrastructure configuration, deployment management, and troubleshooting. RPAM provides this access securely through time-based controls and comprehensive activity logging.

Third-Party and Vendor Access Control

Many organizations rely on external vendors, contractors, and service providers for cloud-based operations. RPAM enables granular, role-based access for these third parties, ensuring vendors can only access authorized resources for a limited time.

Strengthen Your Cloud Cybersecurity With Safous

As more businesses expand their cloud presence, RPAM offers the comprehensive controls and visibility needed to protect sensitive data across multiple cloud environments. The ability to centrally manage, monitor, and secure remote privileged access has become indispensable for maintaining a strong security posture in today's complex cloud landscape.

Safous Zero Trust Access integrates powerful RPAM capabilities with a user-friendly platform designed specifically for enterprise environments. Key features include:

- Granular access control with role-based permissions
- Integrated MFA for privileged access attempts
- Session monitoring with real-time recording and analysis capabilities
- Centralized management of privileged remote access across all systems

Struggling to navigate the challenges of multi-cloud security? [Contact us today](#) to learn how Safous can secure remote privileged access across your entire enterprise.

Sources:

<https://info.flexera.com/CM-REPORT-State-of-the-Cloud>

<https://cpl.thalesgroup.com/cloud-security-research>

<https://www.ibm.com/reports/data-breach>

<https://securityintelligence.com/articles/83-percent-organizations-reported-insider-threats-2024>

About the Author

Roy Kikuchi is the Director of Strategic Alliances at Safous, Internet Initiative Japan (IIJ) Inc. He holds an MBA degree from IE Business School. Roy has over 15 years of experience in the IT services industry as a project manager and business creator. He heads partnership expansion and zero trust access solution development - bringing innovation to IT, OT, and API protection. He expanded the company's business reach into emerging markets by leading innovative projects like tax recording systems for African governments, Laos' first-ever data center, and an IoT-aquaculture project in Thailand. Roy builds partnerships to bring cutting-edge technologies to global markets by leveraging his technical knowledge and business acumen.



Roy can be reached online at roy@safous.com , on [LinkedIn](#), and at our company website: <https://www.safous.com/contact-us>. Connect with him to discuss forging new partnerships anchored by access management and risk mitigation at the frontier of cybersecurity.

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



Wielding AI As a Teammate in Cybersecurity

How to Optimize Human-AI Collaboration

By Dan Cole, VP of Product Marketing, ThreatConnect

Many discussions about artificial intelligence (AI) today trend to swing toward one extreme or the other: AI is either a revolutionary force or a harbinger of job displacement. It will either be really good for us or really bad, Terminator-style.

However, the reality is much more nuanced. There is no single, inevitable AI future. Rather, the impact of AI will depend less on its capabilities and more on how we choose to wield it.

This is especially true in the cybersecurity space. AI has great potential to make the threat landscape more manageable for security teams, so they can more effectively prevent and mitigate major cyber events. However, cybersecurity teams will need to take a thoughtful and strategic approach to integrating AI into cyber operations to maximize its impact.

At ThreatConnect, we believe that to effectively fight cyber threats moving forward, security teams will need to rethink their processes, workflows, and their own roles to find the right balance where AI enhances but doesn't replace human expertise.

Understanding AI's Strengths and Weaknesses in Cybersecurity

In general, AI's strengths lie in processing vast data volumes, pattern recognition, and automation. For cybersecurity teams, this might translate to machine learning models that can detect anomalies and patterns that humans might miss, AI-driven automation that reduces workloads for analysts, and more accurate, faster threat prioritization through AI-driven classification and scoring of threat indicators.

On the other hand, anyone who has experienced a hallucination knows that AI is not infallible. It can lack the necessary context to manage nuanced threats and it can miss novel threats due to training on historical data. AI models and data can also drift over time or be compromised by adversaries.

What this means is that AI is not a "silver bullet" tool that cybersecurity teams can simply set and forget. Without regular human intervention and oversight, AI is likely to misclassify threats and generally prove ineffective in the cybersecurity space.

Instead, cybersecurity teams should think of AI as a collaborator and find the best ways to use human expertise, intuition, and creativity to compensate for AI's weaknesses while leveraging its strengths.

Perfecting the Human-AI Collaboration Equation

Teams need to carefully rethink their existing work to identify the best way to integrate and make the most of AI. For example, at ThreatConnect, we design AI solutions and tools that work seamlessly into teams' existing threat intel lifecycles. In this way, teams aren't left to reinvent processes and procedures every time AI systems evolve. Instead, AI enhances existing, proven workflows in new ways.

When thinking about integrating AI at your own company, it can be helpful to think about AI as the world's fastest intern—incredibly helpful, but needing regular supervision and training.

For example, here are a few best practices to foster greater AI-human collaboration in your cybersecurity operations:

- **Establish human feedback loops:** AI models should regularly incorporate analyst input to improve over time.
- **Practice continuous monitoring:** AI insights require regular validation to maintain accuracy.
- **Deploy rigorous testing:** AI-driven threat intelligence must be vetted to avoid blind spots.
- **Commit to frequent model updates:** Environments, inputs, and expectations are always changing. Consider frequent model updates to ensure AI adapts to evolving threats.
- **Don't forget end-user input:** Sometimes people use tools differently than intended. Listen to end-user input to shape AI to meet real-world needs.
- **Build AI talent and expertise:** As AI proliferates, security teams must understand how AI systems work and where they pose risks.

How ThreatConnect Balances Man and Machine with Practical AI

At ThreatConnect, we believe that cybersecurity teams need AI solutions that enhance—not replace—their expertise so they can make faster, smarter, and more informed decisions. As a result, we take a dynamic, use case-driven approach to building AI solutions for security teams.

In practice, that looks like building solutions around three core AI capabilities and mapping those solutions into the threat intelligence lifecycle. Those AI capabilities include:

- **Correlation:** Uncover meaningful relationships across vast datasets and CTI frameworks to improve prioritization, context, and decision-making.
- **Classification:** Automatically tag, categorize, and contextualize threat intelligence to align with frameworks like MITRE ATT&CK.
- **Acceleration:** Reduce technical barriers to action through customizable automation and by distilling large volumes of intelligence, enabling teams to act faster

As a result, our AI technology is deeply integrated into the ThreatConnect ecosystem, supporting intelligence operations with automated decision support, classification, correlation, scoring, and summarization. To date, more than 250 enterprises worldwide trust our AI solutions to help them stay ahead of adversaries.

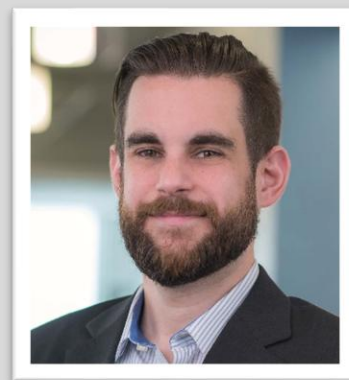
Choosing a Future of AI Collaboration

In many cybersecurity spheres, machine learning and AI are not necessarily new technologies. However, they're increasingly becoming must-have resources in today's threat landscape.

By thinking critically about the best ways to wield AI—to shore up its weaknesses with human intuition, context, and creativity while leveraging its strengths—cybersecurity teams can maximize the impact of AI now and in the future.

About the Author

Dan Cole is the VP of Product Marketing of ThreatConnect. He spent two decades as a product manager, developing a deep understanding of user and market needs. This expertise helps him evangelize the value of threat intelligence and ThreatConnect to cybersecurity teams across the globe, ensuring that our software resonates deeply with our users and that they can get the most out of our products. Outside of work, Dan is a Star Wars enthusiast, a wildlife (fox!) photographer, and an indulgent foodie. Dan can be reached online at dcole@threatconnect.com and at our company website <https://www.threatconnect.com/>





16th Advanced Forum on

DCAA & DCMA

COST, PRICING, COMPLIANCE & AUDITS

June 17 – 18, 2025 • Hyatt Centric Arlington, Washington, DC

Navigate Key Compliance
Challenges and Benchmark Best
Practices with Industry Leaders

Proud Partner



SAVE 10%!

MENTION CODE:
D10-999-CDM25



REGISTER TODAY!

www.AmericanConference.com/DCAA



The Art and Science of Being a CISO

By Ira Winkler, Vice President & Field CISO, CYE

Have you ever wondered why people are chosen to become [Chief Information Security Officers](#)? I started thinking about my peers and listening to their stories of how they obtained their positions. I then considered why I was chosen to be a CISO. At the end of the day, it really was a choice by the powers that be.

When CISOs hire people, many use some form of skills assessment. Sometimes there are sample assignments. We sometimes have people go through scenarios to see their problem-solving abilities. We apply some form of metrics to the process for many roles in cybersecurity.

With a CISO, everyone likes to believe that there are intangibles and soft skills that cannot be measured. People making CISO hiring decisions look to the applicant's past roles to predict their potential for success. While this may sound like an oversimplification, in essence the hiring team believes the CISO knows in their gut how to make appropriate decisions and will continue to do so for their organization.

For the most part, this is how CISOs function. We are brought information. We have situations that require our attention. We must determine how to balance limited resources. We must choose how we manage different people. We must choose how we structure our teams. We must prioritize different functions. To do so, we again gather data, take advice, and then make decisions. This is what a CISO does.

A CISO is also in the position where they have to [present information](#) to organization executives and boards. Their effectiveness in doing so is mostly believed to be tied to their communications skills, which go above and beyond a typical managerial function. It is largely for this reason why many CISOs tend to be external hires, and not as the result of an internal promotion.

Hiring teams want someone with executive presence and communications skills with a proven track record in working with executives. Even a Deputy CISO inside an organization is rarely looked at for promotion to the CISO role. The reason is that the Deputy CISO has not demonstrated the ability to work with the executives and the board, as an outsider has. They are looked at as probably a competent manager, but they have not proven themselves as a competent organizational officer.

Recently one of my friends made the leap after being a Deputy CISO of a large financial organization to that of a CISO. He did so by essentially putting together a business plan for the organization's cybersecurity department. Specifically, he analyzed the organization's security posture, as available from open-source information, highlighted how the organization was deficient compared to their peers, and created a plan as to how he would lead the organization to achieve parity. He also highlighted the cost of the organization's deficiencies.

Even though the organization might have initially preferred a proven CISO with a proven gut, my friend demonstrated the ability to apply tangible metrics to the role.

Put another way, the seasoned gut instinct of a CISO highlights their craft as something closer to art. They look at situations, look at the numbers, interact with people, and they make reasonable decisions based upon years of experience. And for the most part, their decisions are reasonable and the best to be made.

However, these decisions can be frequently wrong, or possibly not the optimal decisions. My friend, however, applied science. He applied data and analyzed the data to make a plan based upon that analysis. Even though my friend was not a proven artist, he demonstrated himself as a scientist—and executives and boards do like scientists.

Cybersecurity is one of the few corporate disciplines that has not embraced what I will broadly call data science. For example, if a COO wants to retool a factory, they use a variety of mathematical formulas to determine whether or not it makes sense, when there will be a break-even point, etc. They use mathematical models to calculate staffing. Likewise, a CFO will use a variety of mathematical models for just about any decision to be made.

[Cybersecurity programs](#) are just beginning to gather metrics to assist in gut-based decision making processes. The metrics can be straightforward, or they can be residual measurements of other activities. For example, I can look at a phishing simulation and the resulting click rates in the simulations, but does that indicate the results of click rates on actual phishing messages?

Instead, wouldn't it be ideal to be able to tie the impact of phishing simulations to reduced blocked actions by the web content filters? This would demonstrate the value of the phishing simulations. If I had the appropriate mathematical models, I could look, for example, at attack paths and determine which vulnerabilities in an attack path are worth mitigating and which aren't.

This is just one example of the application of data science to cybersecurity. In the ideal world, all aspects of a cybersecurity program can be modeled. For example, if you want to determine the best use of your budget, you should be able to put it through a system that optimizes a given budget. If you want to increase your budget, you can model the impact of the resources you want to add to the program and then calculate the return on investment. This would serve to justify your requests.

Likewise in times of budget cuts, when asked to cut your budget by a given amount, you can document the increased risk the company will incur with the budget cuts.

At the moment, when most CISOs are asked what they would do with a budget increase or decrease, they would reply to the best of their abilities, but they would not be able to accurately model the impact. Again, a CISO is usually hired for their proven ability to manage a program.

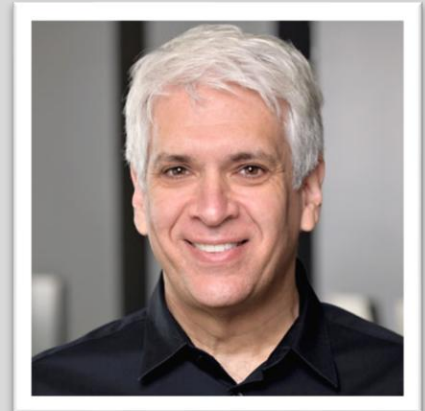
While this may all sound like science fiction, the reality is that the mathematics are available. I have [criticized](#) the broad use of the term AI. It is too vague to apply, and at its root, AI is essentially just mathematical algorithms, most of which have been around for decades. It is just now becoming more widely available, as AI algorithms require extensive processing capabilities that use big data sets. The processing power has become available, and we now have the required large data sets and ability to query and process it.

In cybersecurity, we have collected lots of data over the last few decades and it is available to CISOs to begin processing. There are now tools available, such as the CYE [Hyver](#) platform, that takes in data available to a cybersecurity, supplements it with proprietary and publicly available data, and applies a proven set of data models against the data to support decision making. Even if a CISO doesn't want to acquire tools that can simplify the process, they can create a data science team that examines the more pressing questions a CISO has to answer. The resulting models may or may not be better than the commercially available tools, but they can be tailored to specific needs.

The gut instincts of an experienced CISO produce defensible results; however, they might not be the best results. More importantly, gut instincts do not create defensible dollar values that a CISO can use to justify and rationalize their requests and defenses. Whether you choose to acquire commercial tools and/or implement your own data science program, it is critical you start. Again, you can be a true artist as a CISO, but you will be a better CISO when you become a scientist.

About the Author

Ira is the Executive Director of the Human Security Engineering Consortium, former Chief Security Architect at Walmart and author of *You Can Stop Stupid*. He is considered one of the world's most influential security professionals, and has been named a "Modern Day James Bond" by the media. He did this by performing espionage simulations, where he physically and technically "broke into" some of the largest companies in the World and investigated crimes against them, telling them how to cost-effectively protect their information and computer infrastructure. He continues to perform these espionage simulations, as well as assisting organizations in developing cost-effective security programs.





AFRICA FRAUD

SECURITY & COMPLIANCE SUMMIT 2025

25th–26th JUNE

NAIROBI, KENYA

"FORTIFYING FINANCIAL SECURITY-AI, COLLABORATION & FUTURE-READY FRAUD PREVENTION"

Get ready for East Africa's most important gathering of security minds and compliance leaders. The AFSC Summit 2025 brings together over 400+ executives, regulators, innovators, and global experts shaping the future of fraud prevention, cybersecurity, and regulatory compliance in Africa.

Whether you're defending digital infrastructure, driving policy, or delivering fintech solutions—this is where the region's critical conversations happen.



400+ top-tier attendees – banks, telcos, fintechs, regulators & enterprises



35+ expert speakers & panelists from across Africa & beyond



Real-world use cases on AML, KYC, data protection & fraud analytics



Tech showcases & innovation labs



Unparalleled networking with decision-makers & policy influencers

JOIN THE LEADERS SHAPING AFRICA'S DIGITAL DEFENSE FRONTIER

REGISTER OR BECOME A PARTNER AT:

<https://www.biaafsc.com/register/>





3 Reasons Onion Routing is Required for ‘Truly’ Secure Messaging

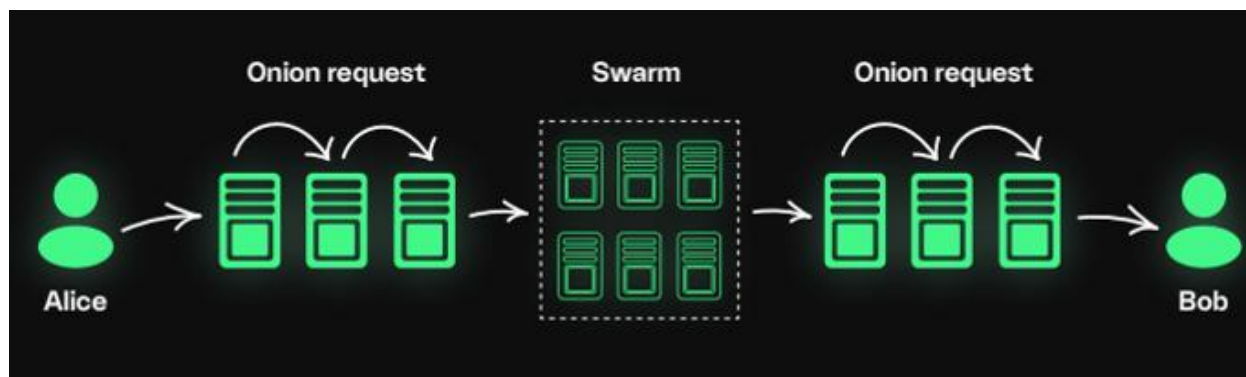
By Kee Jefferys, Co-Founder of Session

In an age where digital communication is ubiquitous, the demand for privacy has never been greater. While end-to-end encryption has become a standard feature in many messaging apps, it often falls short of providing complete protection. The reality is that when you send and receive encrypted messages you can still be revealing sensitive metadata, such as your IP addresses and communication patterns.

To truly safeguard user privacy, encrypted messaging apps should embrace onion routing or multi-hop routing technologies that obscure sender and receiver identities, adding a vital layer of anonymity.

The Limitations of Standard Encryption

End-to-end encryption ensures that only the sender and recipient in a conversation can read the contents of a message. However, it does not hide the metadata associated with the communication. This metadata can include IP addresses, phone numbers, and unique identifiers, and can be used to identify and track users. Centralized servers, common in many popular messaging platforms, further exacerbate this issue by creating single points of data collection, vulnerable to government requests, data breaches, and corporate misuse.



The Power of Onion Routing

Onion routing, or multi-hop routing, addresses these limitations by routing messages through multiple nodes in a decentralized network. Onion routing ensures that each node only knows the previous source and next destination in the chain, masking the sender and receiver's true identities from the content they are sending. This makes it very difficult and costly for any single entity, including node operators, to trace communications back to their origin.

In this era where privacy of our digital communications is increasingly under threat, here are 3 reasons why encrypted messaging apps should adopt onion routing technology:

3 Reasons Why Encrypted Messaging Apps Should Use Onion Routing:

1. Anonymity and Privacy Protection

Onion routing enhances user anonymity by preventing network operators from linking messages to a sender's or recipient's IP address. Messages are wrapped in multiple layers of encryption and relayed through decentralized nodes, making it nearly impossible to trace which IP address is sending or requesting specific messages. Additionally, by masking IP addresses, onion routing prevents the exposure of users' approximate locations, further strengthening privacy.

2. Resistance to Surveillance and Metadata Collection

By encrypting each message multiple times in an "onion" before being sent over the network, onion routing prevents metadata collection and analysis while a message is in transit. Unlike traditional services

that log metadata (e.g., phone numbers and IP addresses), each node in an onion-routed network only knows the previous and next hop for the message. They do not see the content or metadata of the message, making traffic analysis and surveillance significantly more challenging.

3. Decentralization and Censorship Resistance

Unlike centralized communication platforms, onion routing operates on decentralized networks, eliminating single points of failure in the routing process. This prevents governments and corporations from easily censoring or intercepting messages. Even if an individual node is compromised, it cannot expose the entire communication path, making onion routing a powerful tool for activists, journalists, and anyone facing surveillance threats.

In the modern digital age where privacy is increasingly under threat, encrypted messaging apps have become vital. However, traditional encryption methods alone are not enough. To truly obscure sender and receiver identities, messaging platforms that implement onion routing or multi-hop routing ensure an additional layer of protection. One that masks IP addresses and user locations, making tracking and surveillance exponentially more difficult. Implementing onion routing also demonstrates a commitment to user privacy, fostering trust and confidence in the messaging platform.

By leveraging onion routing and multi-hop encryption, privacy-focused apps can provide users with an unparalleled level of security. The Internet was once a place of free and anonymous communication—it's time to reclaim that right with nextgen technology built for privacy.

About the Author

Kee Jefferys is Co-Founder of Session—an end-to-end open-source, privacy-focused encrypted messaging app that prioritizes anonymity, security, and decentralization while maintaining the familiar features of mainstream messaging applications but prohibiting sensitive metadata collection that others allow. It's designed for people who want privacy and freedom from any forms of surveillance. He can be reached at <https://getsession.org>.





Building a Resilient Cyber Ecosystem

Cyber risk impacts operational safety *and* business continuity. Why the basic building blocks are still mission-critical.

By Blake Benson, Senior Director, Cybersecurity Practice Lead for ABS Consulting

The threats that digital-forward organizations are facing might have evolved from a technical perspective, but protection and risk mitigation activities do not need to shift priorities, says Blake Benson, senior director and cybersecurity practice lead for ABS Consulting Inc., an affiliate of the American Bureau of Shipping (ABS). According to Benson, CISOs at organizations who are responsible for critical assets should still focus on "right of boom" recovery and response, blocking and tackling on the programmatic basics before making capital investments in detection technologies.

As organizations build resilience by mitigating operational supply chain risks, adopting a holistic risk management approach and fostering a culture of cyber resilience, communication is a crucial key in managing evolving cyber risk. Strengthening public and private collaborations is important as organizations strive to align on cybersecurity regulations, standards and technical solutions to drive consistent and effective practices. Organizations must work to ensure that cyber risk management is a board-level priority, Benson underscores, with executives taking an active role in advancing resilience initiatives.

Cyber Defense Magazine sat down to review Benson's top considerations for building cyber resilience.

How do evolving regulatory frameworks influence how companies approach cyber resilience and business continuity?

Regulatory frameworks set a baseline and targets for where we need to go on the cybersecurity journey. Objective, third-party safety organizations add to that by bringing forward standards, guidance and compliance support with a critical mission: help protect life, property and the environment.

These safety and risk frameworks help us champion the security and sustainability of vital infrastructures worldwide, but evolving regulations can be difficult to navigate depending on where you are on the journey. Generally, our clients need help in prioritizing which cybersecurity activities required by regulation are going to contribute to their existing safety and security goals and what level of effort will be required to implement those activities.

What's your perspective on the role of government and private sector collaboration in improving cyber resilience?

Cross-collaboration is essential to build a resilient ecosystem for cybersecurity. Conversations need to happen between the sectors so that government and industry are in lock step with staying vigilant, improving systems and processes and applying best practices. Technology innovations and knowledge expertise from the private sector can support government agencies in improving their frontline defense. In many cases, industry should be leading the charge on collaboration because they have a higher concentration of expertise specific to each regulated industry.

How do technologies like AI and automation impact cyber resilience strategies?

We are in a rapidly evolving digital era where AI has the potential to transform everything in cybersecurity and management consulting, from regulation to operating procedures. This poses both challenges and opportunities to respond and reshape a new safety protection frontier.

AI's ability to generate real-time insights, risk assessments and behavior monitoring will improve hazard detection through visualization. For threat actors, the introduction of AI means that they can generate malware quicker and rapidly develop an understanding of previously isolated, cottage operations. The speed at which the industry needs to adopt automation implementations needs to at least match and preferably exceed the speed at which threat actors are iterating novel approaches. Technologies that provide predictive, actionable insights enable us to see beyond current limitations so we can find new ways and a new operating model that will fundamentally alter the nature of safety. What this means from a safety and risk perspective is that safety going forward will not be defined as just the absence of accidents. It will be a new way of thinking about performance as a predictive metric for reliability, leveraging datasets that were previously disparate and unrelated.

What trends do you predict will shape the future of cyber risk management and business continuity planning?

Industry stakeholders responsible for operating facilities and processes in critical infrastructure environments—such as energy and transportation—are increasingly grappling with the challenges of technology debt. Technology debt refers to the accumulation of systems, software and hardware that hinder operational efficiency, security and scalability. This issue is particularly acute in critical

infrastructure environments that have experienced significant corporate restructuring through acquisition activities.

Companies should be encouraged to evaluate the overlap of existing technologies (asset discovery/management platforms, network IDSs, network performance monitoring, etc.) and determine which functions are being performed by which tools. Tool rationalization studies to help better understand these overlapping functions are a great way to reduce technology debt.

These tools are often cited as the “mechanism” or centralized data collection point for determining compliance with security frameworks by providing evidence and artifacts. In some cases, tools are used as the primary system backup/recovery method—a foundational element of business continuity planning.

If you could give one critical piece of advice to CISOs about ensuring safe operations, what would it be?

Whether we are looking at this challenge through an operational or organisational safety lens, cyber risk is a critical business risk. An incident will impact everyone.

Communicating cybersecurity, and more specifically the different approaches to managing cyber risk, to a board is not an easy task for CISOs.

But we can speak to its ROI. Companies can enhance corporate value through improved performance by understanding their unique operational risks and managing these proactively. They can do this a number of ways by applying the right combination of actionable insights from digital tools, field techniques and expertise from engineering and data science. No singular solution exists because each company’s risk profile is unique.

There's more work and training to be done to fully integrate cybersecurity into organisational practices that reinforce operational readiness.

About the Expert

Blake Benson, Senior Director, Cybersecurity Practice Lead. Blake Benson leads the [industrial cybersecurity](#) practice at ABS Consulting, where he works closely with industry stakeholders, government leaders and senior executives across critical infrastructure sectors. His responsibilities include providing a strategic understanding of operational technology (OT) cybersecurity risks to the nation’s essential assets and operations. Blake has expertise in solving complex risk-based problems and specializes in developing tailored, environment-specific approaches to help both government and commercial clients develop and implement the security solutions and controls necessary to manage cyber risk.



Blake joined ABS Consulting in 2019 and is a Knoxville, Tennessee native and United States Air Force (USAF) veteran. While in the USAF, Blake was a founding member of one of the first operational cyber units.



All-Time High: Confronting The Escalating Threat of Medical Data Breaches

By Scott Speranza, CEO of HealthLock

The health care industry, a cornerstone of our society, is facing an unprecedented challenge when it comes to safeguarding the vast amounts of sensitive patient data it manages. What was once a concern has now become a crisis: medical data breaches are not isolated incidents but a relentless tide, impacting millions of individuals and placing immense strain on the health care ecosystem.

For IT and cybersecurity professionals, understanding the gravity of this situation, its underlying causes, and the shortcomings of current defenses is the first crucial step toward building a more secure future.

The statistics paint a sobering picture. According to the [2025 Breach Barometer published by Bluesight](#), the health care sector experienced an alarming surge in data breaches in 2024, with over 300 million patient records compromised— a 26% increase over 2023 numbers. This total includes the most extensive health care data breach on record, impacting approximately one out of every two individuals in

the United States.¹ This is unfortunately not surprising as statistics show that medical records are 50 times more valuable than traditional financial information – the risk/reward is worth it to the cyber criminals.

Even in the early months of 2025, the trend persists. In its [February 2025 Data Breach Report](#), the HIPAA Journal reported on 46 large health care data breaches (incidents involving 500 or more individuals), affecting 1.2 million individuals.² While this showed a month-over-month reduction, the high number of breaches throughout 2024 suggests this may be a temporary dip in an otherwise upward trajectory.

The causes behind this epidemic are multifaceted. According to the reported data, foremost among them are hacking and other IT incidents, which accounted for 74% of reported breaches in February 2025 and exposed the protected health information (PHI) of over 1.1 million individuals (89% of the total affected).

These incidents encompass a range of malicious activities, including data theft, ransomware attacks, and the compromise of email accounts through phishing campaigns. Health providers network servers remain the primary target, reflecting the wealth of sensitive information they often contain. The persistent success of email-related breaches, with 14 such incidents reported in February 2025, underscores the critical need for robust email security measures and user awareness training.

However, the threat landscape extends beyond external actors. Insider threats, both in the form of unintentional errors and deliberate malicious actions, also pose a significant risk. While perhaps less frequent than hacking, insider breaches can directly compromise patient privacy and erode trust in health care providers.¹

Furthermore, the interconnected nature of the health care industry introduces vulnerabilities through business associates – third-party entities that handle PHI on behalf of covered entities. In 2024, the 2025 Breach Barometer connected breaches involving business associates to a remarkable **77% of all breached records**.¹ This highlights the extended attack surface and the critical importance of ensuring robust security practices throughout the entire health care ecosystem.

Despite increasing awareness and regulatory mandates like HIPAA, many health care organizations continue to exhibit fundamental failings in their cybersecurity posture. A significant concern is the lack of comprehensive risk analysis and risk management processes. Without a thorough understanding of potential threats and vulnerabilities, organizations struggle to implement effective safeguards.

Inadequate access controls often grant unauthorized personnel access to sensitive electronic protected health information (ePHI). Moreover, a recent survey produced by the HIPAA Journal indicated that at least 43% of HIPAA-covered entities either rely on manual processes or may not track HIPAA compliance at all.³ This reliance on outdated methods can lead to inconsistent record-keeping, increased administrative burdens, and a higher risk of non-compliance and subsequent breaches.

Weaknesses in email security infrastructure, including the absence of advanced threat protection and multi-factor authentication, contribute significantly to the success of phishing attacks and email account compromises. Delayed patch management cycles leave critical systems vulnerable to known exploits, providing easy entry points for cybercriminals. Finally, insufficient oversight and due diligence regarding business associates can lead to breaches occurring within these third-party systems, with cascading effects.

For IT and cybersecurity professionals within the health care sector, the challenge is clear, and the responsibility is significant. Mitigating the risk of medical data breaches requires a multi-pronged approach encompassing technological solutions, robust processes, and a culture of security awareness. Here are crucial steps to take to shore up these gaps:

- **Prioritize advanced email security solutions**

Deploying sophisticated threat detection and prevention technologies, implementing multi-factor authentication for all email accounts, and conducting regular security awareness training focused on identifying and avoiding phishing and social engineering attacks are paramount.

- **Enforce stringent access controls**

Implement the principle of least privilege, ensuring that users only have access to the information and systems necessary for their job functions. Regularly audit access logs to identify and investigate any anomalous activity.

- **Establish and adhere to rigorous patch management processes**

Timely identification and application of security patches to all systems and applications are essential to close known vulnerabilities before they can be exploited by threat actors.

- **Develop and maintain comprehensive incident response plans:**

A well-defined and regularly tested incident response plan is crucial for effectively managing and mitigating the impact of a data breach, including procedures for investigation, containment, eradication, recovery, and notification.

- **Strengthen business associate agreements and oversight**

Conduct thorough due diligence on all business associates to ensure they have adequate security measures in place and regularly assess their compliance with these agreements and HIPAA regulations.

- **Invest in proactive monitoring and threat detection technologies**

Implement security information and event management (SIEM) systems and explore the use of artificial intelligence (AI) and machine learning (ML) powered tools to detect anomalous activity, identify potential threats in real-time, and accelerate incident response.

- **Consider implementing HIPAA compliance software**

For organizations still relying on manual processes, adopting dedicated HIPAA compliance software can significantly streamline compliance efforts, centralize documentation, automate tracking of essential tasks, and provide comprehensive reporting, thereby reducing the risk of non-compliance and potential breaches.

- **Foster a culture of security awareness**

Regularly educate and train all employees on patient privacy best practices, the importance of safeguarding PHI, and their role in preventing data breaches. This includes training on recognizing and reporting suspicious activity and understanding the organization's security policies.

The fight against medical data breaches is not a static battle but an ongoing evolution against increasingly sophisticated threats. By acknowledging the scale of the problem, understanding its root causes, addressing organizational failings, and proactively implementing robust IT and cybersecurity measures, professionals in this field can significantly strengthen the defenses of the health care industry and better protect the sensitive information entrusted to its care. The security and privacy of patient data must be a continuous priority, ensuring that the focus remains on delivering quality health care without compromising the fundamental right to privacy.

About the Author

Scott Speranza is the CEO of HealthLock, a company on a mission to restore privacy, control, and savings to health care consumers. With over 25 years of experience in software-as-a-service, health management solutions, and insurance claims auditing, Scott brings a deep passion for protecting patients from the growing issues of medical billing fraud, denied claims, and privacy violations.

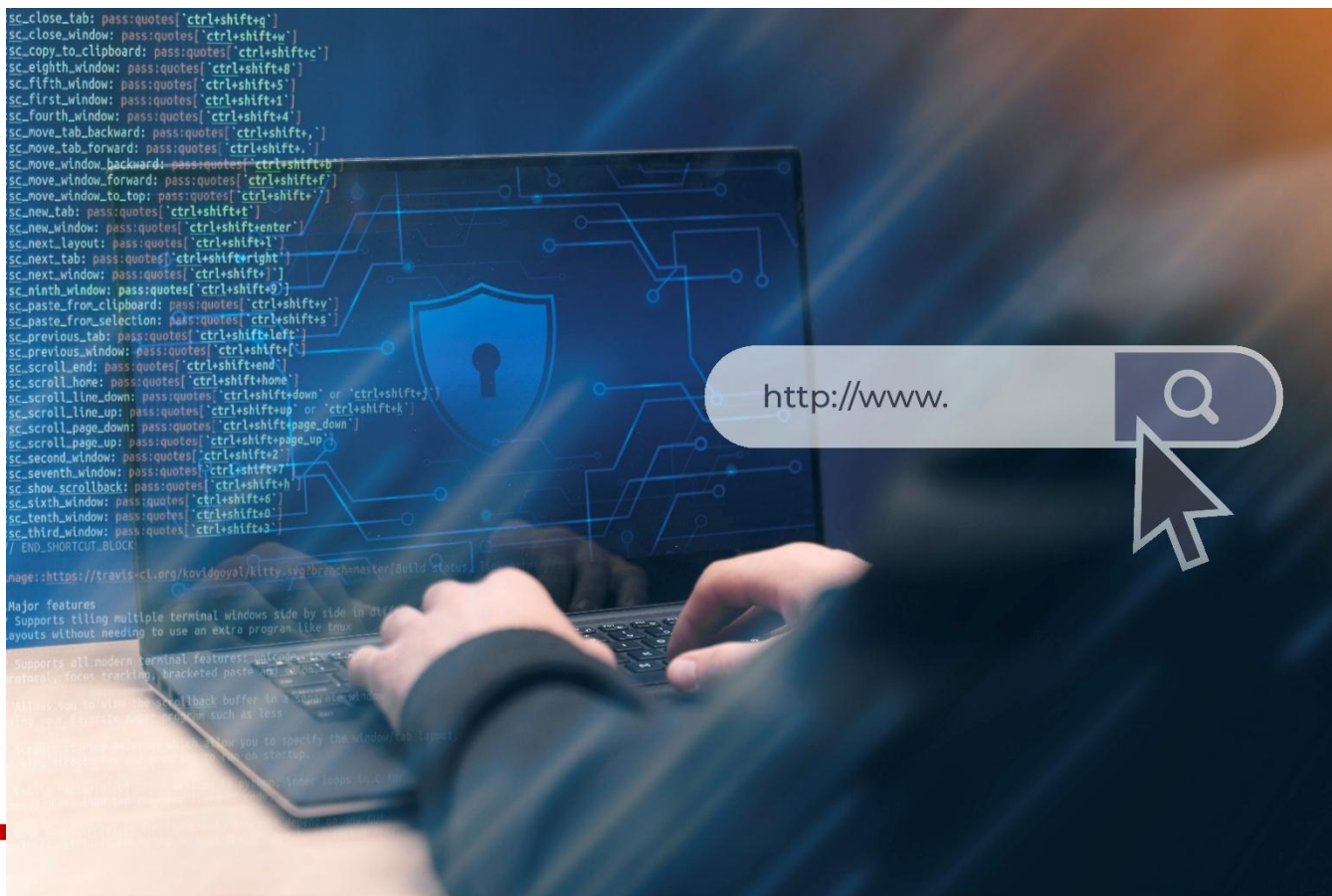
Scott's leadership spans roles at top firms including PricewaterhouseCoopers, SAP/BusinessObjects, RSA, and Fiberlink (where he helped grow MaaS360 Security to \$400M before its acquisition by IBM). He is also the founder of inAssist, HealthLock's parent company, and has overseen the audit of over half a billion dollars in medical claims—generating more than \$230 million in member savings.

A firm believer that the health care system should serve and protect patients—not profit from their confusion—Scott has championed HealthLock's innovative technology that detects billing errors, negotiates overcharges, and safeguards medical data. His vision has helped forge partnerships with major institutions like Mastercard, expanding HealthLock's impact to millions of Americans.

A graduate of Westmont College with a degree in economics, Scott balances his professional life with community involvement, including board service with Sharefest LA, and enjoys sports, politics, and time with family. His commitment to transforming the health care experience continues to shape HealthLock's role as a trusted advocate for every patient.

Scott can be reached online at sales@healthlock.com and at our company website <https://healthlock.com>





Beyond Zero Trust: How to Eliminate Backup Access and Elevate Your Cyber Security

Zero Access Fills the Gaps That Zero Trust Leaves Behind

By Robert Marett, Chief Technology Officer, Cobalt Iron

Astute data custodians use zero-trust methods to enhance infrastructure security. This model shifts the security perimeter from traditional network boundaries to individual resources, requiring continuous authentication and authorization for every single access request. However, a fundamental issue remains: the fact that access is granted in the first place. Once authenticated, a user could still do harm, even if by accident.

While zero trust significantly improves security, there is a more robust way to secure the backup environment, and that is not to grant access to it at all. The zero-access concept addresses the limitations of zero trust.

The Current Threat Landscape

Cybersecurity experts have seen a significant surge in cyber activities, primarily focused on obtaining credentials, gaining access, and manipulating or removing data. These activities often culminate in ransomware or other catastrophic attacks, forcing your business to recover and potentially even pay a ransom.

What's more, the threat landscape has evolved to a point where many attackers are now using AI to make their attacks easier. For instance, AI-generated phishing emails can now mimic trusted figures like CEOs, making the attack more convincing and harder to detect.

Backup operations are particularly attractive targets for these threats. Sophos' 2024 State of Ransomware report reveals that 94% of cyber attacks also attempt to compromise backup. Some ransomware gangs and variants like LockBit specifically target backup environments. A recent attack on UnitedHealthcare, a company that typically fends off an attack every 70 seconds, managed to freeze large portions of its IT infrastructure, including backup systems.

While the zero-trust approach is crucial in securing enterprise backup environments, it has limitations. On its own, zero trust is not enough to protect backup against these sophisticated threats.

Things Have Changed

In the past, once users passed initial security checks, they were trusted forever. They could access any resource in the network without ever being verified again. But the modern IT landscape — with its cloud computing, mobile workforces, and distributed systems — has rendered this approach obsolete. We can no longer rely on a single digital or physical barrier for protection. Because attackers can easily compromise user credentials and move laterally within the network, continuous verification is now a must.

Consequently, the access control methods that were effective a decade ago will no longer cut it.

The Concept of Zero Trust — Never Trust. Always Verify.

A zero-trust security model requires authentication for every single access request every time, no matter how many times the credentials have been verified before. The point of this “never trust; always verify” approach is to limit security exposure, minimize the number of attacks, and reduce the impact when they occur. That's why zero trust belongs in every IT and data protection strategy.

Special Considerations for the Backup Environment

The backup environment poses unique security challenges that make it ideal for the zero access-approach.

For one thing, backup contains copies of data from all other applications, making it a prime target for cyber attacks.

The backup environment is also incredibly complex. Even small backup environments have numerous components, and in larger organizations and enterprises, the number of software and hardware components and the interactions between them is staggering. Each component typically requires access, creating multiple potential vulnerabilities, even in security-hardened operations that use zero-trust methods like multifactor authentication.

Unfortunately, no organization is immune, as we saw in a recent attack against a large company with well-secured IT operations managed by an experienced provider. Even though the company did all the right things, it still lost its backup catalog, rendering data unrecoverable. This example highlights the difficulty in securing backup, especially since many backup products weren't designed to fend off cyber attacks.

Why Zero Trust Alone Can't Secure Backup

Zero trust is crucial for improving cyber protection and is widely recommended for securing infrastructure and data. Everyone should use it wherever applicable. But backup and recovery environments need more security than zero trust can provide. That's because zero trust has some limitations.

1. Access is access: While zero trust makes access more difficult, the goal is still to grant access, which can be exploited if credentials are compromised. This is an unacceptable risk for backup systems.
2. Multiple components = more vulnerability: The numerous components in a backup environment all act as potential attack vectors. Security is often managed separately for each component, thereby increasing the challenge.
3. Inconsistent vendor adoption: Not all technology vendors fully embrace zero-trust principles in their product design and management. Even backup vendors that offer advanced security features typically can't extend these protections to all components in a backup environment.
4. Framework flaws: Legacy code and architectures could contain hidden vulnerabilities that zero-trust methods might not recognize. For example:
 - SSH and OpenSSH, designed as secure replacements for remote login protocols, can serve as backdoor entries into some backup products.
 - Log4j, commonly used for monitoring and logging events, has been the target of attacks like Log4Shell, which exploits openings in the software. Patching these vulnerabilities across all systems remains a challenge.
5. Lack of cyber resilience for backup: Originally designed to counter hardware failures and human errors, backup now plays a crucial role in recovering from cyber attacks. To be truly cyber resilient, backup environments need advanced protection that is designed to withstand sophisticated attacks and maintain integrity when other systems are compromised. Zero-trust methods don't do that.

Because of these weaknesses, it's crucial to implement additional security measures tailored to the unique challenges of backup environments.

Enter the Zero-Access Model

Zero access is an advanced security approach for backup environments that surpasses traditional zero-trust methods. It prioritizes automation over access, significantly reducing the risk of human error and malicious intent in data breaches.

Key Features of Zero Access:

1. Automation-centric design: Zero access emphasizes automation as the cornerstone of its security strategy. By eliminating unnecessary human interaction with backup components and operations, it enhances security while improving system efficiency and effectiveness.
2. Comprehensive protection: This approach provides all-encompassing security for the entire backup infrastructure, safeguarding all components — including servers, software, databases, and storage systems — by removing access points for operational activities. In this way, zero access fills security gaps left by traditional zero-trust approaches.
3. Elimination of manual management: Zero access revolutionizes backup management by removing traditional login capabilities, preventing account takeovers and unauthorized access. It replaces manual management with automated systems, ensuring consistent and secure operations. [Perhaps replace the 2nd sentence with – Elimination of various component log-ins eliminates most of the attack vectors that bad actors typically exploit. I would like to eliminate automation here as it sounds like we are duplicating #1]

Zero access incorporates a specialized management interface that gives administrators visibility and control over the backup environment without direct access to the infrastructure. It implements robust zero-trust mechanisms, including multifactor authentication, to ensure only authorized personnel can interact with the system.

If there's ever a legitimate reason to delete a full backup, like when decommissioning a system, the zero-access approach would follow defensible data deletion protocols that require auditable, multifactor approval for any data removal, thereby preventing administrators from unilaterally deleting data. And in rare instances when an admin would need to access backup devices in a true emergency, it would require multiphase security approval from both company admins and the service provider. These stringent processes ensure that even in emergencies, security remains intact.

Zero Access in Action

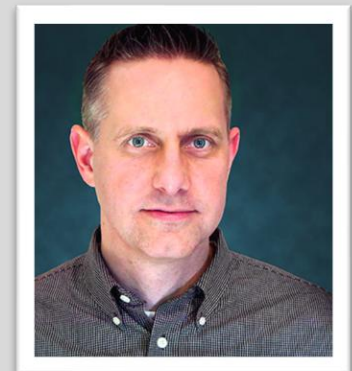
In a ransomware attack on a global company, hackers used stolen credentials to compromise more than 1,000 systems. Because the company's backup solution implemented the zero-access approach, its backups were completely protected. The company recovered without engaging with the hackers.

More attacks came weeks later and caused additional damage [maybe we add here "that was once again recovered with clean, untouched backups" or something to that effect]. The attackers threatened to target the company's backups, but because zero-access architecture eliminates the typical vulnerabilities found in backup environments, the hackers gave up and went away. This incident demonstrates the superior protection zero access offers compared to traditional zero-trust approaches.

Zero access represents a paradigm shift in backup security, offering a robust solution against cyber threats by redesigning how we manage and protect backup environments. By prioritizing automation, comprehensive protection, and stringent access controls, zero access is a new standard for securing critical backup data in an increasingly hostile digital landscape.

About the Author

By Robert Marett, Chief Technology Officer, Cobalt Iron. Robert can be reached online at <https://www.linkedin.com/in/robmarett/> and at our company website www.cobaltiron.com





Browser Security Must Anchor Your Defense Strategy

Lessons from the First Half of 2025

By Dakshitaa Babu, Security Researcher, SquareX

The security landscape of 2025 has crystallized around an undeniable truth: the web browser has become both your most critical application and your greatest vulnerability. Looking at recent major breaches, the pattern is clear - attackers have overwhelmingly shifted to browser-based attack vectors that bypass traditional security controls entirely.

This shift isn't coincidental. As organizations moved critical operations to cloud applications, the browser transformed from a simple website renderer into a complex application platform. It now functions as the primary workspace where employees access sensitive data, corporate systems, and authentication portals. Attackers have followed, developing sophisticated techniques that exploit the browser's complexity.

Recent high-profile attacks illustrate this evolution. OAuth consent phishing campaigns harvest access tokens through legitimate authentication flows. Browser-based cryptojacking and ransomware execute entirely in memory without triggering endpoint detection. Advanced brand impersonation pages use client-side assembly to evade server-side scanning. Malicious browser extensions with polymorphic code steal credentials and easily bypass all traditional security solutions. These threats share a common denominator: they execute within the browser environment where traditional security has limited or no visibility.

The most concerning aspect of this trend is that conventional security technologies - secure web gateways, cloud proxies, and even EDR solutions - fundamentally lack visibility into the browser's runtime environment. They can't see DOM manipulations, track JavaScript execution, or monitor real-time rendering that reveals malicious intent. This creates a critical blind spot exactly where organizations are most vulnerable.

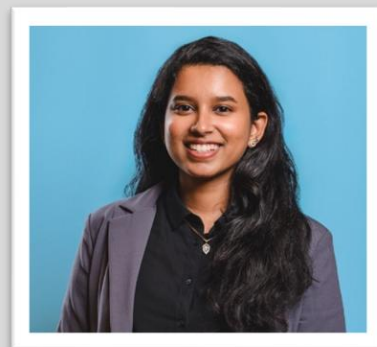
An effective 2025 security strategy must place browser security at its core. Browser Detection and Response (BDR) capabilities that monitor browser-level activities in real-time have become essential, not optional. These solutions provide visibility into the actual rendered content users see, detecting threats that assemble only at the last mile.

While a comprehensive security stack still requires identity protection, cloud security, and endpoint detection, these components must now integrate with and complement browser-centric security rather than operating in isolation. The browser has become the primary battlefield for modern attacks - making browser security the essential foundation upon which all other defenses must build.

Organizations that recognize this shift and prioritize browser security accordingly will be positioned to withstand the continued evolution of threats. Those that maintain outdated security paradigms centered on network perimeters or endpoint files will increasingly find themselves defending yesterday's attack vectors while remaining blind to today's most prevalent threats.

About the Author

Dakshita Babu is a Security Researcher and product evangelist at SquareX, where she leads the security research team. She has contributed to bleeding-edge browser security research presented at top conferences including DEF CON main stage. Her work on email security bypasses, breaking Secure Web Gateways, MV3 extension vulnerabilities, browser syncjacking and polymorphic extensions have been covered by leading media outlets, including Forbes Exclusive, TechRadar, Mashable, The Register, Bleeping Computer, and CyberNews. Dakshita can be reached online at <https://www.linkedin.com/in/dakshitaababu/> and at our company website <https://sgrx.com/>





How Critical Infrastructure Can Prepare for an Uptick in Cyberattacks in 2025

By Dr. Bill Anderson, Principal Product Manager, Mattermost

The discovery of Salt Typhoon and its deep penetration of privately run telecommunications networks last fall was alarming — but not unexpected. Since [at least 2019](#), hackers allegedly backed by the People's Republic of China have infiltrated water utilities, ports, and oil and gas facilities, periodically testing their foothold in these systems.

The attackers are persistent, patient, and increasingly sophisticated — and their activities will surge, according to the Department of Homeland Security's recently released [2025 Homeland Threat Assessment](#). Organizations that safeguard critical infrastructure and national security must focus on cyber resilience and adopt modern incident response strategies. In preparation, they need a centralized, secure platform that enables teams to respond efficiently, collaborate securely, and maintain compliance without relying on compromised systems.

The Core Elements of Effective Incident Response

Incident response involves a combination of predefined procedures, experienced and well-trained people, and integrations with a wide range of security tools and services. While team collaboration plays an essential role in mitigating potential security incidents, organizations must recognize that their security response teams can't rely on using the same systems that are under attack. Compromised infrastructure is not a place to manage a crisis. This is especially true for large organizations that juggle multiple incidents simultaneously.

For example, if a critical infrastructure operator relies on cloud-based tools for daily operations and security monitoring, an attack on that environment can severely limit the ability to respond effectively. Conventional communication tools also can pose security risks during an active breach. If these systems are compromised, attackers can intercept sensitive communications or disrupt coordination efforts. It's hard to bounce unwanted entities from your systems when they know your next move.

Secure, collaborative incident response platforms offer an alternative that is resilient to external threats and provides uninterrupted, high-trust communication. They provide an isolated, out-of-band environment safe from eavesdropping.

The Benefits of a Dedicated Incident Response Platform

Modern security operations use a variety of tools: firewalls, endpoint detection and response systems, intrusion detection software, and cloud security platforms. However, these tools often function in silos. Security teams must manually make sense of different tools' alerts and logs, which slows response times.

A dedicated incident response platform offers a unified, real-time view of cyber threats by integrating data from multiple sources. Analysts can identify abnormalities faster, triage incidents more effectively, and initiate containment procedures without delay in this consolidated view.

Speed counts when responding to an attack. A well-structured incident response strategy must incorporate automated workflows that enable organizations to react immediately to emerging threats. Pre-configured digital playbooks help teams follow reliable, approved, and compliant procedures when responding to different types of cyber incidents. Whether it's a data breach, ransomware attack, or insider threat, automated workflows ensure that every step — from detection to resolution — is systematically executed.

Beyond ensuring procedural integrity, playbooks address one of the biggest challenges in incident response: staffing turnover and training. Real-life incidents are documented and then become highly effective training tools, guiding new staff through best practices, expected standards, and necessary steps in handling incidents. By providing clear, step-by-step instructions, playbooks help new team members quickly adapt, reducing onboarding time and improving overall team readiness. As a result, organizations can maintain operational resilience and knowledge continuity even amid staffing changes.

Prepare for Post-Mortem Audits

After resolving an incident, a security team's work isn't finished. They must review what happened and assess the effectiveness of their response.

A centralized incident response platform should automatically log all activities, decisions, and communications so teams can generate detailed reports. These reports can help identify procedural gaps to strengthen future security strategies and identify threat patterns that can improve future security responses. These reports also meet regulatory requirements with comprehensive response documentation. For example, federal agencies require robust auditing to comply with Federal Information

Security Modernization Act requirements, the National Institute of Standards and Technology's incident tracking guidance, and other cybersecurity frameworks, while defense agencies must meet Cybersecurity Maturity Model Certification standards.

A Strategic Imperative for Cyber Resilience

Take heed of DHS' warning. Organizations can be prepared for the growing wave of cyber threats in 2025 and beyond by adopting a secure, collaborative, and highly efficient incident response platform. Investing in proactive defense measures today will enhance national security and ensure operational continuity in the face of evolving adversarial tactics.

Now is the time to rethink how your organization approaches cybersecurity. Is your incident response platform ready for tomorrow's threats?

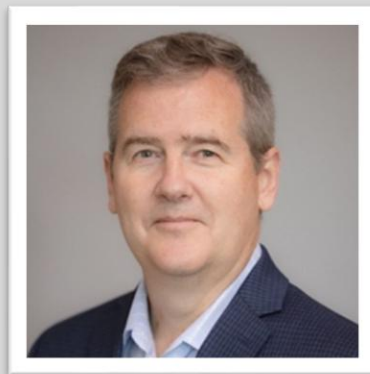
About the Author

Dr. Bill Anderson is the Principal Product Manager at Mattermost and an expert in the security industry, with a rich background in operating, founding, and funding high-growth security companies. He holds a Doctorate in Electrical Engineering from the University of Waterloo, where he specialized in cryptography.

Before joining Mattermost, Dr. Anderson served as the President of CIS Secure, where he successfully introduced a secure mobile platform solution for government defense and intelligence agencies in the U.S. and internationally. He is also recognized as the founder of Oculis Labs, an innovative data-in-use security company that catered to both the Department of Defense (DoD) and the Intelligence Community (IC), leading it through a successful acquisition by OptioLabs. At OptioLabs, he initially served as Chief Product Officer and later took on the role of CEO, where he launched groundbreaking security solutions for Android devices.

Dr. Anderson has also held executive positions at SafeNet Inc., Aether Systems, and Certicom, managing highly successful cryptography and communications product lines, including pioneering work in elliptic curve cryptography. Additionally, he serves as Vice Chairman of the board of directors for the Maryland Technology Development Corporation (TEDCO), where he supports early-stage technology investments.

He holds multiple patents, including innovations in computer display privacy and secure information systems. His patented technologies focus on physically securing information on computer monitors, using advanced facial recognition and privacy control mechanisms to ensure that sensitive data is visible only to authorized users.





Deep Learning-Based Solutions Help Enterprises Avoid Zero-day Attacks

By Dave Floyd, Vice President of Cybersecurity Sales and Service, Hughes Network Systems

Zero-day cyberattacks pose unique challenges for IT organizations, due in large part to their inherent novelty. Verizon's 2024 [Data Breach Investigations Report](#) (DBIR) found that attacks involving vulnerability exploits grew 180% from the previous year, and attackers' widespread use of AI tools makes it easier for them to carry out more exploits faster. But new solutions are available to help organizations fight back, with deep learning providing a foundation for a preemptive approach to data security that can finally get ahead of zero-day attacks.

Solving the challenges behind zero-day attacks

Because these attacks target vulnerabilities that aren't publicly known, zero-day exploits are often missed by signature-based threat detection platforms that rely on lists of recognized attack attributes. Once a zero-day attack enters the environment, IT has historically had few tools available to stop or defend against it. The best thing an enterprise can hope for is to receive some early-ish warning that something's wrong and then try to respond to it as quickly as possible.

Innovative platforms are turning the tables, empowering businesses to stop zero-day attacks with more advanced technology. For example, some solutions feature lightweight agents that can be installed on customer endpoints, so when a user downloads a file or when a file is in transit that could touch that endpoint, the file is quickly scanned for malicious content. If the agent spots anything malicious within the file, it's blocked before it can execute. The scanning happens so fast that an unsuspecting or inattentive end user doesn't even have a chance to click on or interact with the file. This switch to preemptive action is a meaningful step forward in blocking zero-day attacks before they can unleash their payloads.

Plugging the holes in patch releases

With traditional tools, providers push routine security patches to update the list of known threats, allowing the software to spot and, hopefully, stop them. However, despite the comprehensive nature of many vendors' lists, there are still gaps that can reduce the effectiveness of the company's defensive efforts. One problem is that zero-day exploits can take a long time to identify, and even after a vulnerability is known, there may still be a days- or weeks-long gap before it's included in a patch.

Patch release schedules often present their own challenges. Frequent patch releases may stress a cybersecurity vendor's quality assurance process, allowing errors to infiltrate customers' networks. Those mistakes can disrupt operations and potentially hop from the originating software to other systems in the environment. The more frequently an enterprise receives patches, the greater the chances that something will go wrong. If that little thing snowballs into a big thing, IT will have a new and urgent problem to fix.

Zero-day attacks and the AI difference

Solutions with deep-learning capabilities can address many of the drawbacks of traditional tools. For example, they can bridge the holes that may appear between patches. Rather than relying on frequently updated lists of attack vectors and attributes, which can become outdated almost as soon as they're released, platforms with advanced AI capabilities leverage alternative methods to stay ahead of zero-day attacks.

Working much like the human brain, these tools incorporate a neural network that can detect previously unknown attack patterns faster. In the case of zero-day attacks, this means the platform can make connections that didn't exist before, identifying novel cyberattacks or malicious software. Innovative

solutions with deep learning capabilities can see a threat it wasn't trained specifically to identify and, employing pattern recognition that's more advanced than traditional AI and machine learning, block the attack. Leading tools have an efficacy greater than 99%, giving IT teams more power to stop zero-day attacks than ever before.

Augment detection and response, reduce overall risk

Using advanced platforms alongside traditional tools, it's now possible to achieve two critical goals: stopping more zero-day attacks and reducing security operations center (SOC) stress. With advanced AI on the frontlines, detection and response solutions no longer need to wade through every potential threat in the search for genuinely malicious items. Existing platforms can be more efficient and accurate. In addition, as more incoming dangers are evaluated and managed automatically, the SOC team can focus on high-priority alerts elevated by the cybersecurity tools rather than wading through the entire flood of concerns.

New solutions with AI and deep learning at their core have a high success rate, but they aren't perfect. Companies should continue to employ a layered approach to cybersecurity, with deep-learning platforms and traditional detection and response tools working hand in hand to thwart zero-day, ransomware, and other attacks. Together, these layers can block threats at multiple levels, relieve the SOC team of unnecessary alerts, and drastically reduce the organization's overall risk.

About the Author

Dave Floyd is the Vice President of Cybersecurity Sales and Service for Hughes Network Systems. He works directly with organizations and enterprises across industries to provide tailored cybersecurity solutions that address pain points and build a comprehensive cybersecurity posture for their businesses. Dave can be reached online at [linkedin.com/in/davidefloyd/](https://www.linkedin.com/in/davidefloyd/) and at our company website <https://www.hughes.com/>





Securing Success in a Data-Driven World

By Yoav Regev, CEO and Co-Founder, Sentra

Sir Walter Raleigh once famously said, “For whosoever commands the sea commands the trade; whosoever commands the trade of the world commands the riches of the world, and consequently the world itself.”

If Raleigh was alive today, he might have expressed the same sentiment for data. Organizations controlling and harnessing data’s potential have a leg up against competitors. Yet, businesses find themselves often overwhelmed by the volume and complexity of their data and are struggling to keep pace with shifting security risks.

Data success isn’t defined by the volume of data, but rather the mindset of the organization. Data fuels growth, innovation, and smarter decision-making, yet many IT and security leaders still ask themselves the following questions:

- Are we making decisions based on reliable data insights?
- Is data guiding our long-term success?
- Are we in control of our data — or is it in control of us?

Mastering data isn't just a strategic advantage — it's essential in today's competitive market. To thrive in a data-driven world where speed, innovation, and security must work together, the right solutions can make all the difference.

Understanding and Securing Data

Data is used to improve customer interactions, create new solutions, and maintain that illustrious competitive edge. But simply collecting it isn't enough.

The secret to data success comes from securing it, understanding it, and putting it to work effectively. Unfortunately, for years, this was almost impossible. IT and security teams faced hurdles with complex, imprecise, expensive, and time-consuming data processes.

Today there are tools to transform data management from reactive to proactive, driving innovation, resilience, and a competitive advantage — but not every solution is created equally. There are three key pillars security leaders should look for in tools to secure and leverage data.

1. Uncover Your Data.

Visibility is the foundation of any data security strategy. It's critical to know where your data is stored, who has access to it, and what sensitive information it contains. Data sprawl, which refers to the uncontrolled growth and fragmentation of data across an ecosystem, is a challenge for many organizations.

To manage this, organizations should leverage tools that discover, classify, and map sensitive data across all environments. This visibility allows security and IT teams to monitor data flows, detect anomalies, and respond to risks before they escalate. A comprehensive view of data activity shifts security from *reactive* to *proactive*.

2. Control Your Data.

Once you understand your data estate, control is the next step. To protect sensitive information, it's critical to minimize risk. Organizations must identify overly broad permissions and ensure "least privilege." In other words, only give access to those who need it, for the shortest possible time.

However, this is easier said than done — having full control of data becomes challenging when it is copied and moved between environments, such as from a private to a public network, or when it is changed from encrypted to unencrypted. Doing so can create what is known as "similar data" — data that was initially secure but becomes exposed when moved into a different environment (ex. data moving from production to a lower environment).

The best data security strategies go beyond identifying these issues; they enforce access policies, automate corrective actions, and integrate with existing identity and access management systems to help maintain a strong security posture, even with changing business needs.

Data security tools should have access control measures that can help establish role-based access controls (RBAC) and attribute-based access control (ABAC) policies, ensuring the right users have the right data at the right time.

3. Update Your Data

Data security is not static. Effective solutions shouldn't just use real-time monitoring to detect risks and threats; they should anticipate them. Visibility into suspicious activities, with real-time alerts, *and* automated responses can enable security teams to act swiftly, ensuring businesses stay resilient and adaptive to emerging threats.

Scalability Starts with Continuous Data Security

As organizations grow and adopt new technologies, their data environments grow more complex. Securing data shouldn't be just a checkbox or a one-time effort — instead, it's an ongoing commitment. Organizations that use modern data security solutions to understand, control, and monitor their data continuously are set to fulfill Sir Walter Raleigh's prophecy — only this time, in 2025, navigating the sea of data.

About the Author

Yoav Regev is CEO and Co-Founder of Sentra. He has over two decades of experience in the world of cybersecurity, cloud, big data, and machine learning. He was the Head of Cyber Department (Colonel) in the Israeli Military Intelligence (Unit 8200) for nearly 25 years. Reflecting on this experience, it was clear to him that sensitive data had become the most important asset in the world. In the private sector, enterprises that were leveraging data to generate new insights, develop new products, and provide better experiences, were separating themselves from the competition. As data becomes more valuable, it becomes a bigger target, and as the amount of sensitive data grows, so does the importance of finding the most effective way to secure it. That's why he co-founded Sentra, together with accomplished co-founders, Asaf Kochan, Ron Reiter, and Yair Cohen. Yoav can be reached online at our company website www.sentra.io





Lights, Camera, Safety - The Video Surveillance Revolution

By Freddy Kuo, Chairman, Luminys

The last several years have been marked by a world-bending technological shift, powered by the advancements in AI. [McKinsey's 2024 Global Survey on AI](#) found that enterprise AI adoption spiked to 72%, up 50% from recent years. This technology has opened new windows of possibilities for companies across all industries. While there's been significant apprehension around AI, there's been a surge of new solutions, vendors, and applications that have integrated the technology and made significant strides in our workflows and personal lives.

Leaders in the security field, in particular, have started implementing AI-driven technology to protect their resources and employees in both the digital and physical worlds. As such, more companies are beginning to search for video surveillance solutions to protect their business' infrastructure, operations, and individuals' well-being.

As we move forward into future, AI's impact will continue to spread, and the ways we use the technology will keep evolving.

The Expanding Impact of AI on Security and Video Surveillance

In the security industry, AI has transformed the efficiency and effectiveness of security solutions that go well beyond ChatGPT and LLMs. In the world of software and cybersecurity, AI has accelerated and ramped up threat detection to a level that was incapable of humans before. This has allowed internal security teams to monitor, prioritize, and respond to credible threats and tackle the most pressing risks to their infrastructure and digital assets.

In addition, physical security solutions are also taking advantage of AI to enhance protection across physical resources or spaces and provide safety for individuals in their day-to-day lives. More and more, organizations are using AI to analyze user data and patterns, developing [user and entity behavior analytics](#) (UEBA). UEBA is a security strategy that uses AI and ML technologies to detect unusual patterns or behaviors from users and devices.

So, physical security devices that monitor crowds or spaces can connect to cloud-based platforms to identify suspicious activity with greater speed and accuracy. With wider adoption, this method could help keep organizations, individuals, and their assets safer by detecting abnormal behaviors or risks before they can become a significant threat.

It's also worth noting that legacy security systems are [increasingly targeted](#) by bad actors and are growing more vulnerable to those attackers' threats. These outdated solutions often fail to identify and block attacks or risks, and it does not take much for a criminal to exploit one of these systems. Organizations must modernize or implement innovative technologies that can ensure security measures are enacted – not just as a technical component, but also as a business strategy. Successful attacks can result in financial loss, damage to a company's reputation, or operational disruption, which can be quite devastating.

The Rise of Video Surveillance-as-a-Service (VSaaS)

As safety and protection become more vital in today's world, organizations are turning to video surveillance to monitor and manage their security. From large festival-style concerts to the outside of hotels to [Walmart employees with body cameras](#), companies are beginning to recognize and implement video surveillance measures into their operations for enhanced, comprehensive protection.

Video Surveillance-as-a-Service (VSaaS) is a cloud-based recording solution that gives organizations the ability to remotely store, manage, record, playback, and monitor video feeds through their protected platforms, eliminating the need for expensive onsite hardware and physical storage. Modern VSaaS providers have bolstered equipment to even the most demanding environments, which gives more peace of mind when considering the rapid effects of climate change and needing long-lasting security camera solutions.

Organizations should be on the lookout for solutions that have advanced self-learning capabilities and AI-ISP that can continually adjust to changing environments. This will enhance the VSaaS tech's threat detection capabilities and intelligence, helping businesses safeguard their properties with increased effectiveness and efficiency.

With advancements in video analytics, cutting-edge lighting technology, and robust monitoring systems, VSaaS is going to continue bringing preventative solutions that deter threats and risks by quickly identifying anomalies. Certain VSaaS technologies go even further with blue and red lights and alarms ringing from their equipment to prevent incidents. Business leaders can use highly advanced cameras to capture full-color images or videos, day or night, and also track targets from security footage through the use of AI and ML analytics. The best solutions will incorporate immediate response measures like deterrent flood lights, real-time alerts, and audio warnings to prevent threats from infiltrating a business.

Sustainability of Security Solutions

As we move forward, security organizations are going to be forced to reckon with accountability – not only in safety but also in sustainability. As mentioned above, climate change is creating more obstacles for businesses, and resources are becoming more expensive or more limited. Providers must confront their energy demands and figure out efficient, sustainable methods to run and scale their businesses.

For security vendors, it's not just about having state-of-the-art security solutions – it's also about the mark and impact they have on our planet and those around us. Solar-powered security systems are beginning to gain traction in the industry with visual intelligence and predictive capabilities. Renewable energy can deliver eco-friendly operations in addition to high-quality, top-tier performance, making them indispensable this year and beyond.

Newer solutions can use renewable solar panels and high-capacity batteries to provide high reliability and off-grid functionality for augmented versatility – some can even run up to seven to 10 days. These sustainable solutions can be taken anywhere to deter crime, secure a site, manage traffic, or monitor safety without being constricted to the grid.

The Future of AI and Business Security

It's clear that security is top of mind for all business leaders. UEBA and AI will have a definitive impact on business security as they continue to develop. Companies will prioritize safety solutions that deter threats in real-time and continuously monitor their assets. At the same time, they're going to have to rely on sustainable solutions that don't take up as many resources in order to continue protecting themselves.

In the new year, we'll start to see these conversations around video surveillance shift from the boardroom to the workplace and beyond to better protect and safeguard business, operations, and most importantly, people.

About the Author

Freddy Kuo is a seasoned technology executive with a robust track record in leading supply chain management, global manufacturing strategy, and strategic investments to drive market expansion for publicly listed companies.

Currently, Freddy serves as Executive Office Special Assistant at Foxlink, where he leverages over 20 years of experience in OEM and ODM manufacturing. Foxlink is renowned for designing and producing a diverse range of electronic components for major global brands. Additionally, he holds the position of Chairman of the Board of Luminys Systems Corp. (Luminys), a U.S.-based subsidiary of Foxlink that specializes in video security and smart building solutions. He also serves as Executive Director of Ubilink.AI, a joint venture between Foxlink, Shinfox Energy, and cloud provider Ubitus K.K.



At Foxlink, he spearheaded the development and execution of manufacturing and business strategies that fuel global growth as the company ventures into new sectors. He oversees all investment activities, including M&A and strategic investments, with a particular focus on the U.S. and North American markets.

In his role at Luminys, he successfully led the acquisition and integration of Dahua Technology USA. As Chairman, he is responsible for setting the strategic vision and roadmap, guiding the company's expansion in the U.S. to offer a comprehensive range of advanced security solutions. His extensive experience in managing Foxlink's global supply chain network is instrumental in transitioning Luminys manufacturing to Foxlink and its affiliates.

As Executive Director of Ubilink.AI, Freddy manages all aspects of the joint venture, from strategic planning to operational management, to enhance Taiwanese leadership at the intersection of generative AI and green energy.

Previously, he led Foxlink's accessories business group for six years, collaborating with top brands, including Fortune 500 companies, on an OEM and ODM basis. Under his leadership, the unit developed a wide array of innovative products, from cables and batteries to POS systems. He also drove the development and market expansion of PQI, Foxlink's in-house consumer electronics accessories brand.

Freddy's career began as a venture capitalist in the venture capital arm of Foxlink in San Francisco, where he honed his skills as a strategic investor.

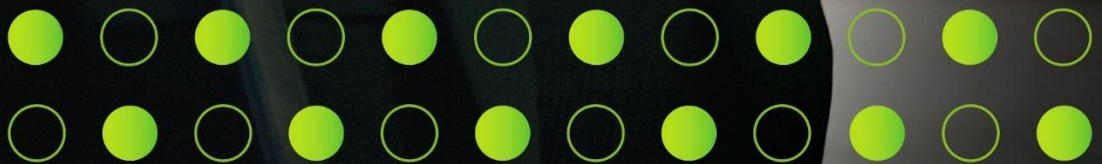
Born in Taiwan and raised on the U.S. West Coast, he completed his undergraduate education at Seattle University. His multicultural background, combining American education and Taiwanese roots, enables him to bring a unique and innovative approach to global business strategy.

Freddy Kuo can be reached online at <https://www.linkedin.com/in/freddykuo/> and at our company website <https://www.luminyscorp.com/>

Deloitte.



Ready to build
resiliency? Scan
to get started.



DELOITTE CYBER SERVICES

Do more than defend

In an increasingly open and connected world, cybersecurity is at the core of business success.

Because when you're secure, you can better navigate uncertainty.

When you're prepared, you can turn challenge into opportunity.

And when you're resilient, you can focus less on defending and more on driving forward.

Together, we'll make cybersecurity the core of your success, with the breadth and depth of cyber solutions you need, when you need them.

Ready to build resiliency? Go to Deloitte.com/us/DoMoreThanDefend

The Current: Trusted news & views
on cybersecurity

Scan to read the latest issue and subscribe >





Customer Trust Is a Business Imperative: It's Not Enough to Just Protect Customer Data, Businesses Must Show Proof of Their Efforts as Well.

By Sam Rehman, Chief Information Security Officer, SVP at EPAM Systems, Inc.

Customer trust is not a nebulous or abstract idea, but a real driver of business success, especially in today's digital-first world. In [a study on data privacy](#), 94% of surveyed organizations reported their customers would not buy from them if they did not protect data properly. Customer trust and cybersecurity are inseparable, and businesses must implement measures and strategies that help build customer trust and restore it should a breach occur.

However, customer trust encompasses more than data security. Pew Research Center reports that [81% of U.S. adults](#) believe companies will use their information in ways that make them uncomfortable. Such sentiment reflects the fear among consumers that companies collect their data without their permission. Security, privacy, transparency and collaboration are the bedrock of customer trust; these four elements are essential for increasing retention and revenue.

Cybersecurity Measures That Build Trust

Cybersecurity measures that build customer trust involve the key areas of technology, processes and people. Starting with technology, companies must ensure they are not using the same security solutions year-over-year. Cybercriminals are constantly adapting, re-engineering and refining their schemes—businesses should have the same mindset if they want to maintain customer trust.

Analytical solutions built on the latest technologies like artificial intelligence (AI) and machine learning (ML), for example, enable businesses to stay agile, helping them adapt to emerging threats quickly to ensure customer data remains protected. Brands can constantly enhance these AI- and ML-powered systems to combat new cyberattacks and identify emerging threats by inputting new data points.

Processes should also be secure, which will require regular threat assessments. These checks allow companies to find vulnerabilities within their everyday processes and procedures, followed by targeted security measures. Routine threat assessments also reveal if an enterprise complies with the latest industry regulations. Adherence to data protection regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) is crucial to mitigating financial and reputational risks while bolstering customer trust.

Last (but certainly not least) on the security checklist is people—specifically, employee training. As it stands, general employee security “training” involves watching awareness videos and completing quizzes. Businesses should use the same training methods to prepare general employees as they do cybersecurity teams—namely, role-relevant simulations and mockups. These methods will also help assess a workforce’s security fitness, enabling targeted training that adequately prepares the entire company and increases collaboration to improve security together.

The Importance of Transparency

Unfortunately, customers can’t see the behind-the-scenes work businesses put into protecting their data and minimizing data breaches. Companies should never assume customers know their data is safe—they must inform their customers and other stakeholders directly.

While enterprises can’t give away all their secrets (that would jeopardize security), greater transparency—when carefully managed properly and in close collaboration with partners—can boost customer confidence and build brand goodwill in the future. In the B2B space, this transparency should be bi-directional, meaning companies can learn from working with customers and their incident response exercises.

Businesses can boost customer awareness of data protection measures through campaigns and advertisements. Companies can also build customer trust by routinely publishing announcements or newsletters about their security credentials validated by accredited organizations. Likewise, posting on social media channels and other customer touchpoints about the latest company-wide security training or best practices for data security and fraud prevention will go a long way.

Businesses must remember to articulate how these measures not only minimize data breaches but also demonstrate a promise to consumer protection and privacy. Highlighting one's commitment to regulatory compliance regarding the GDPR and CCPA, for example, will strengthen brand reputation.

Persevering Trust Amid Breaches

When a data breach inevitably occurs, it is paramount that companies prioritize transparency with consumers by using communication channels to deliver important updates and advice throughout an incident. Proactive, open and honest dialogue with customers will help keep them in the know, reducing panic during the event while preventing trust from eroding in the immediate aftermath. Moreover, organizations can further bolster trust by sharing how they plan to minimize future breaches based on the most recent incident.

Despite companies' best efforts, the reality is that a cybersecurity breach is not a matter of if but when. Risk will always exist, and it's up to organizations to manage it accordingly, rather than hopelessly struggling to eliminate it completely. Educating customers on this reality will soften negative backlash toward organizations—especially if they successfully minimize the blast radius.

Companies can reduce the blast radius of a cybersecurity breach through methods like segmentation and isolation, which limit the lateral movement of bad actors once inside a system. Other practices, such as real-time and automated alerts, will help increase the time security teams have to react to a breach, enabling them to remediate it quickly. Businesses should likewise develop an incident response plan that outlines guidelines and responsibilities for if and when a breach occurs.

The Power of Strategic Partnerships

Cybersecurity is ultimately *not* a solo endeavor. As mentioned above, brands in the B2B space can increase their security posture by engaging in dialogues with their customers and their security teams. Portals that allow people to report suspicious emails and other fraudulent activity are great for those in the B2C space. Moreover, organizations should partner with trusted cybersecurity providers, ultimately transforming customer trust into tangible business gains through specialized expertise, advanced technologies and industry best practices.

About the Author

Sam Rehman is Chief Information Security Officer (CISO) and Head of Cybersecurity at EPAM Systems, where he is responsible for many aspects of information security. Mr. Rehman has more than 30 years of experience in software product engineering and security. Prior to becoming EPAM's CISO, Mr. Rehman held a number of leadership roles in the industry, including Cognizant's Head of Digital Engineering Business, CTO of Arxan, and several engineering executive roles at Oracle's Server Technology Group. His first tenure at EPAM was as Chief Technology Officer and Co-Head of Global Delivery.

Mr. Rehman is a serial entrepreneur, technology expert and evangelist with patented inventions in software security, cloud computing, storage systems and distributed computing. He has served as a strategic advisor to multiple security and cloud companies and is a regular contributor in a number of security industry publications.

Sam can be reached online at <https://www.linkedin.com/in/samrehman/> and at the EPAM website <https://www.epam.com/>.





Cyber Security Threats vs. Insider Threats

The Most Damaging Threats to Your Organization May Not Be from Cyber Criminals

By Jim Henderson, Founder / Chairman of the National Insider Threat Special Interest Group (NITSIG) CEO Insider Threat Defense Group, Inc. (ITDG)

For many years there has been much debate on who causes more damages (Insiders Vs. Outsiders). While network intrusions and ransomware attacks can be very costly and damaging, so can the actions of employees' who are negligent, malicious or opportunists. Another problem is that Insider Threats lives in the shadows of Cyber Threats, and does not get the attention that is needed to fully comprehend the extent of the Insider Threat problem.

The [NITSIG](#) in conjunction with the [ITDG](#) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **6,100+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud, embezzlement, shell company - fake invoicing schemes, contracting fraud, bribery, kickbacks and more. This is very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

To grasp the magnitude of the Insider Threat problem, one must look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to significant underreporting on the Insider Threat problem.

Surveys and reports that simply cite percentages of Insider Threats increasing, do not give the reader a comprehensive view of the actual malicious actions employees' are taking against their employers. Some employees' may not be disgruntled / malicious, but have other opportunist motives such as financial gain, to live a better lifestyle or supporting their gambling addictions, etc.

The severe damages from employees' can be into the MILLIONS and BILLIONS, as referenced in the reports on the link below. Companies have also had large layoffs or gone out of business because of the malicious actions of employees. The damages caused by employees can happen in an organization, from big to small, from U.S. Government to private sector businesses.

These Insider Threat incidents are not just caused by JUST 1 EMPLOYEE. In some case multiple employees may be involved, or employees may be in collusion with external cyber criminals or conspirators.

Some organizations invest thousands of dollars in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem. If you read any of these monthly reports, you might have a different perspective on Insider Threats.

Could your organization rebound / recover from the severe impacts that an Insider Threat incident can cause?

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational, guidance and support tool to: **1)** Gain support from CEO's, C-Suite, key stakeholders and supervisors for developing or enhancing an Insider Risk Management (IRM) Program. These reports provide the justification, return on investment and the funding that is needed for an IRM Program. **2)** Provide Insider Threat Awareness Training to the workforce on the importance of reporting employees' who may pose a risk or threat to the organization. **3)** Review and enhance security controls (Non-Technical, Technical) to protect the organization from the many different types of Insider Threats.

Download Reports / No Registration Required

www.insiderthreatincidents.com

If you would like to receive the monthly Insider Threat Incidents Reports via email, please send your request to: jimhenderson@nationalinsiderthreatsig.org to be added to the distribution list.

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The NITSIG
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org

About the Author

Mr. Henderson is the Founder and Chairman of National Insider Threat Special Interest Group (NITSIG). The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The NITSIG Membership is the largest network (1000+) of Insider Risk Management (IRM) professionals in the U.S. and globally.

Mr. Henderson has 20+ years of experience protecting sensitive and classified information up to the Top Secret SCI Level, with hands-on experience in the development, implementation and management of; IRM Programs, Cyber Security - Information Systems Security Programs, Information Assurance Programs, for U.S. Government Agencies, Department of Defense, Intelligence Community Agencies, Defense Contractors, State Governments, large and small businesses.

Mr. Henderson developed and instructs the highly sought after IRM Program Evaluation & Optimization Training Course, and also provides IRM consulting services to [clients](#).

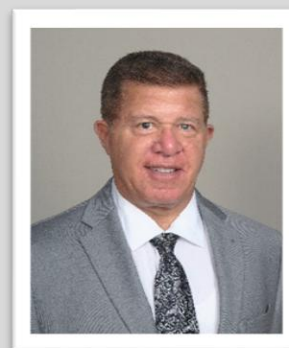
<https://www.insiderthreatdefense.us/wp-content/uploads/2024/05/insider-threat-defense-group-client-listing.pdf>

Mr. Henderson developed and taught an Information System Security Program Management Training Course to 100 NSA Information Systems Security Managers.

Additional information on Mr. Henderson's background can be found on [this link](#).

<https://www.insiderthreatdefense.us/wp-content/uploads/2024/05/Insider-Threat-Defense-Group-Overview-Insider-Risk-Management-Program-Training-Consulting-Services.pdf>

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Risk Management Program (IRMP) Training Course Instructor / Consultant
<https://www.insiderthreatdefensegroup.com/>
james.henderson@insiderthreatdefense.us
Phone: 561-809-6800
Follow Us On Twitter / X: @InsiderThreatDG





Cybersecurity Due Diligence in Mergers and Acquisitions: Essential Focus Areas

By Tom Cockriel, co-leader of Trenam Law's Business Transactions practice group, Trenam Law

Introduction

Many companies view mergers and acquisitions (M&A) as opportunities for growth, market expansion, talent acquisition and enhanced operational efficiencies. However, they also include potential cybersecurity risks that, if not properly assessed and addressed, could result in financial losses, reputational damage and legal liabilities for the acquirer.

Cybersecurity due diligence should be a core part of any M&A strategy so that acquirers are fully aware of potential risks before finalizing the acquisition. Diligence should include members of the acquirer along with third-party advisers such as technical IT and cybersecurity advisers and legal counsel. This article explores essential areas, largely from a legal perspective, that acquirers must examine when conducting cybersecurity due diligence during M&A transactions. It should be noted that data protection and privacy regimes and industry practices are fast-evolving, and cybersecurity diligence does and will continue to evolve as well. Acquirers should work with knowledgeable internal and third-party advisers and take into account any industry-specific and geographic-specific concerns related to the target company.

1. Assessments of Security Framework

The first step in cybersecurity due diligence is evaluating the target company's security framework to determine its overall cybersecurity practices. This assessment should cover:

- **Compliance Standards:** Assess whether the company adheres to specific regulatory requirements such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS) and National Institute of Standards and Technology (NIST) frameworks. The applicable requirements will vary based on the company's industry, products, services, and data collection and usage practices, among other factors.
- **Incident Response Plans:** Review the company's incident response capabilities, including documented processes, and response teams, as well as how those capabilities were implemented during (and updated since) past breach history.
- **Security Infrastructure:** Evaluate existing security controls, including firewalls, intrusion detection systems (IDS), encryption protocols and endpoint protection mechanisms. The infrastructure will likely include functionality controlled by the company and products and services provided by third parties.
- **Vulnerability Management:** Analyze the company's approach to patch management, software updates and vulnerability assessments to determine whether it follows best practices.
- **Third-Party Risk Management:** Determine how the company manages cybersecurity risks posed by vendors, suppliers and partners with access to its systems.
- **Penetration Testing and Audits:** Review the company's history of penetration testing and security audits to gauge the robustness of its defenses. These tests and audits will include recommendations from the auditors; however, companies frequently do not implement all recommendations. Additionally, tests that were conducted several years prior to the acquisition may not adequately address the current state of cybersecurity needs and concerns and may not offer much valuable to the acquirer's review.
- **Cyber Insurance Coverage:** Determine whether the company has cyber insurance and assess the terms, limitations and coverage of potential cyber-related incidents. The acquirer likely will not be able to assume the coverage after closing of the acquisition; however, the target company might be able to extend its preclosing coverage by utilizing a tail policy.

2. Reviews of Data Management Policies

Data is a very valuable asset in many organizations, regardless of industry, and the acquirer should include it as a focus in M&A due diligence. A thorough review of data management policies should focus on:

- **Data Collection, Use and Transfer:** Examine how data is collected, stored, used and transmitted within the company.

- **Data Classification and Handling:** Examine how sensitive data is categorized, stored and transmitted within the organization.
- **Access Controls:** Assess whether data access is based on the principle of least privilege (PoLP), ensuring that employees can only access information necessary for their roles.
- **Data Retention and Deletion Policies:** Determine how long data is retained and whether the company follows best practices for securely deleting obsolete information. The company may have legal and contractual obligations related to its retention and deletion practices.
- **Encryption Standards:** Review whether sensitive data is encrypted at rest and in transit.
- **Data Breach History:** Investigate whether the company has suffered data breaches, how they were handled, and whether vulnerabilities were adequately remediated and proper notice procedures were followed.
- **Data Backup and Recovery Plans:** Review the robustness of data backup policies and disaster recovery plans to understand the company's business continuity in case of security incidents.
- **Cloud Security:** Examine security controls in place for cloud-based infrastructure, including vendor management, access controls and encryption protocols.

3. The Role of Emerging Technology Within the Company

As emerging technologies such as artificial intelligence (AI) and machine learning (ML) become more prevalent in business operations, cybersecurity due diligence must evaluate the security implications related to those technologies. Key considerations include:

- **AI/ML-Driven Security Measures:** Determine whether AI and ML are being used for threat detection, anomaly detection and automated incident response.
- **Potential AI-Related Risks:** Assess whether AI systems are susceptible to adversarial attacks, model or data poisoning, or data manipulation.
- **Third-Party AI Vendors:** Evaluate the security posture of AI service providers and the potential risks associated with outsourcing AI-driven tasks.
- **Automated Decision-Making Risks:** Review the company's AI governance policies to ensure that automated decisions do not introduce security blind spots or biases.
- **Regulatory Compliance:** Confirm that AI-driven data processing aligns with relevant data protection regulations and ethical AI standards.
- **Integration with Legacy Systems:** Examine how AI solutions integrate with existing infrastructure and assess potential security gaps in interoperability.
- **AI Model Transparency and Accountability:** Ensure that AI models used in the organization maintain transparency and auditability to prevent biased or erroneous decisions that could compromise security.

4. Assessments of Employee Access to Secure Information

Human factors remain one of the most significant cybersecurity risks. Evaluating employee access to and handling of sensitive information is critical to preventing insider threats and unauthorized disclosures. Key areas of assessment include:

- **Identity and Access Management (IAM):** Determine whether the company implements multifactor authentication (MFA), role-based access controls (RBAC) and single sign-on (SSO) mechanisms.
- **User Privilege Audits:** Conduct audits of accounts to identify excessive permissions and ensure proper access governance.
- **Security Training and Policies:** Evaluate the company's cybersecurity training programs, phishing simulations and employee adherence to security policies.
- **Employee Exits:** Analyze processes to ensure that departing employees no longer have access to sensitive systems and data.
- **Third-Party Contractor Access:** Assess security policies for contractors and vendors who may have temporary access to the company's infrastructure and ensure that third parties are subject to written contracts that include proper acknowledgements and indemnities.
- **Remote Work Security Measures:** Assess how the company secures remote access, including VPN usage, endpoint security controls and mobile device management.

Conclusion

Cybersecurity due diligence in M&A transactions is no longer optional or limited to target companies engaged in specific industries. It is now a critical part of the deal process across deal sizes, industries and geographic locations. By conducting assessments of security frameworks, data management policies, emerging technologies and employee access controls, organizations can mitigate cybersecurity risks before finalizing an acquisition. A proactive approach to cybersecurity due diligence minimizes exposure to known and unknown cyber threats and data practices noncompliance.

Furthermore, organizations should consider post-merger integration strategies to maintain cybersecurity continuity. Establishing a unified security framework, harmonizing policies and continuously monitoring for new threats will help ensure long-term protection and operational stability. By prioritizing cybersecurity due diligence, M&A stakeholders can transform cybersecurity risks into strategic advantages, better positioning themselves for a more secure target company and successful acquisition while minimizing potential post-closing issues.

About the Author

Tom Cockriel is the co-leader of the Business Transactions practice group of Trenam Law. He focuses on corporate and business transactions, including mergers, acquisitions and sale transactions; capital raising transactions; intellectual property and technology agreements; trademark and copyright protection; commercial contracts; and other general business matters. Tom may be reached online at tcockriel@trenam.com and at our company website <https://www.trenam.com/people-list/thomas-j-cockriel/>





Dark Web Threats: How Your Data Is Compromised and Monetized by Cybercriminals

By Ankit Sharma, Senior Director and Head - Solutions Engineering, Cyble

In the vast expanse of the internet lies a concealed realm known as the dark web—a hidden network where anonymity reigns supreme. While it serves legitimate purposes for privacy-conscious users such as whistleblowers, journalists, and dissidents, it has also become a hotbed for illicit activities. One of its most lucrative markets is the buying and selling of stolen personal and corporate data. Understanding how cybercriminals compromise and monetize this data is crucial in safeguarding individuals and organizations alike from becoming victims.

How Your Data Ends Up on the Dark Web

Most users never visit the dark web, but that doesn't mean their data isn't there. Every online transaction, sign-up form, or social media profile leaves behind digital breadcrumbs. When those breadcrumbs land in the wrong hands, they often become part of massive data sets marketed and sold on dark web forums.

The journey begins with compromise. Cybercriminals use a blend of tactics to harvest personal and corporate data:

- **Data Breaches** remain the most prolific source. In 2024, India witnessed an alarming rise in targeted attacks against financial institutions, insurance firms, and healthcare providers. A single breach at a medical diagnostics firm led to the exposure of over 5 million patient records, which quickly surfaced on dark web marketplaces.
- **Phishing Scams** continue to be weaponized at scale. Fake emails, SMS messages, and even job offers are designed to lure victims into handing over credentials or downloading malware.
- **Malware Attacks** are often embedded in pirated apps, infected websites, or unsecured Wi-Fi networks. Once installed, they silently capture keystrokes, login credentials, and financial data.
- **Credential Stuffing** thrives on weak or reused passwords. Hackers simply automate login attempts using data leaked from previous breaches—often with shockingly high success rates.
- **Insider Threats** also play a role. Employees, either disgruntled or incentivized, may leak or sell sensitive databases directly to cybercriminals.

The Business of Stolen Data

Once harvested, the data is cleaned, categorized, and auctioned like inventory in a wholesale warehouse. A full identity—known as “fullz”—can fetch between \$10 and \$100 depending on its quality. A hacked bank account with a clean transaction history? That can go for hundreds.

Here's how the monetization lifecycle works:

1. **Bundling and Valuation:** Cybercriminals compile stolen data into categories like login credentials, medical records, tax IDs, or passport scans. Each bundle is priced based on its utility and rarity.
2. **Dark Web Marketplaces:** Platforms like Genesis, BlackForums, and Hydra function like eBay—complete with user reviews, refund policies, and customer service. Sellers build reputations over time, and the most reliable vendors command premium prices.
3. **Crypto-Powered Transactions:** Payments are made via cryptocurrencies such as Bitcoin and Monero to maintain anonymity. Smart contracts and escrow services often protect both parties.
4. **Exploitation and Resale:** Buyers may directly use the data to commit fraud—applying for loans, stealing medical benefits, or launching phishing campaigns—or they may resell the information to other actors.

A Case in Point: The AT&T Breach

In March 2024, a massive breach involving [AT&T](#) made headlines after data from over 70 million current and former customers was discovered on a dark web forum. Unlike ransomware attacks where data is held hostage, this breach was purely transactional. The attackers didn't demand a ransom; they directly monetized the data, selling it to the highest bidder. Among the exposed data were Social Security

numbers, email addresses, and phone records—each piece a potential ticket to identity fraud or SIM-swapping scams.

What Happens with Your Data?

Once in the hands of a cybercriminal, your data becomes a multi-use asset:

- **Identity Theft:** Fraudsters open bank accounts, apply for credit cards, or file tax returns using stolen personal details.
- **Account Takeover:** If your Netflix login is sold, it's a nuisance. But if your banking or PayPal credentials are reused across services, the financial fallout can be immediate.
- **Synthetic Identities:** By blending real and fake information, cybercriminals create “new” individuals, enabling them to access credit or healthcare fraudulently.
- **Corporate Espionage:** Leaked corporate credentials often lead to business email compromise (BEC) attacks, where executives are impersonated to authorize wire transfers.

The Human and Business Cost

The fallout is far more than financial.

- **Individuals** suffer damaged credit scores, emotional stress, and years of recovery from identity theft.
- **Companies** face regulatory scrutiny, reputational damage, and operational disruptions. One Indian fintech startup in early 2024 suffered a major trust crisis when 20 million user records were leaked, resulting in investor pullout and app uninstalls.
- **Healthcare providers** risk patient safety and compliance violations when medical records are exposed.

Building Resilience Against Dark Web Threats

Preventing your data from ending up on the dark web is an ongoing process—not a one-time fix. A mix of proactive habits and organizational practices can significantly reduce risk:

- **Use Complex, Unique Passwords** and update them regularly. A password manager can help keep track.
- **Turn on Multi-Factor Authentication (MFA)** wherever possible. It's a simple barrier that stops most credential attacks.
- **Limit Data Sharing:** Think twice before filling out online quizzes or sharing sensitive details with third-party apps.
- **Invest in Dark Web Monitoring:** Businesses should scan the dark web for leaked credentials or mentions of their brand in illicit contexts.

- **Educate Employees:** Regular training on phishing and secure practices is essential to building a resilient workforce.
- **Patch Vulnerabilities Quickly:** Outdated systems are soft targets. Automated patching can drastically reduce exploitability.

The Bottom Line

The dark web isn't science fiction—it's the backroom of the internet where your identity, passwords, and personal history can be sold in minutes if not seconds. In this high-stakes black market, data is currency and ignorance is costly. The best defense is staying ahead of cybercriminals through awareness, proactive protection, and a culture of cybersecurity at every level.

About the Author

Ankit Sharma, Senior Director and Head - Solutions Engineering, Cyble, is a Seasoned Techno-commercial professional, having refined skill set & relevant experience in driving both Topline & Bottomline growth. Domain expertise in the field of Program Delivery Management, Technical Sales & Key Account Management. Highly skilled Data security & Privacy professional, specializes in Data Privacy (Global Privacy law/regulations/standards & Privacy Information management Systems), Data Governance, Compliance Management & Cloud Security. Currently Heading Solution Engineering for Cyble Inc., managing the global team of some brilliant solutions engineers and architects, which also act as a bridge between the Clients and back-end teams. Responsible to drive business growth across the globe & support Cyble Sales.

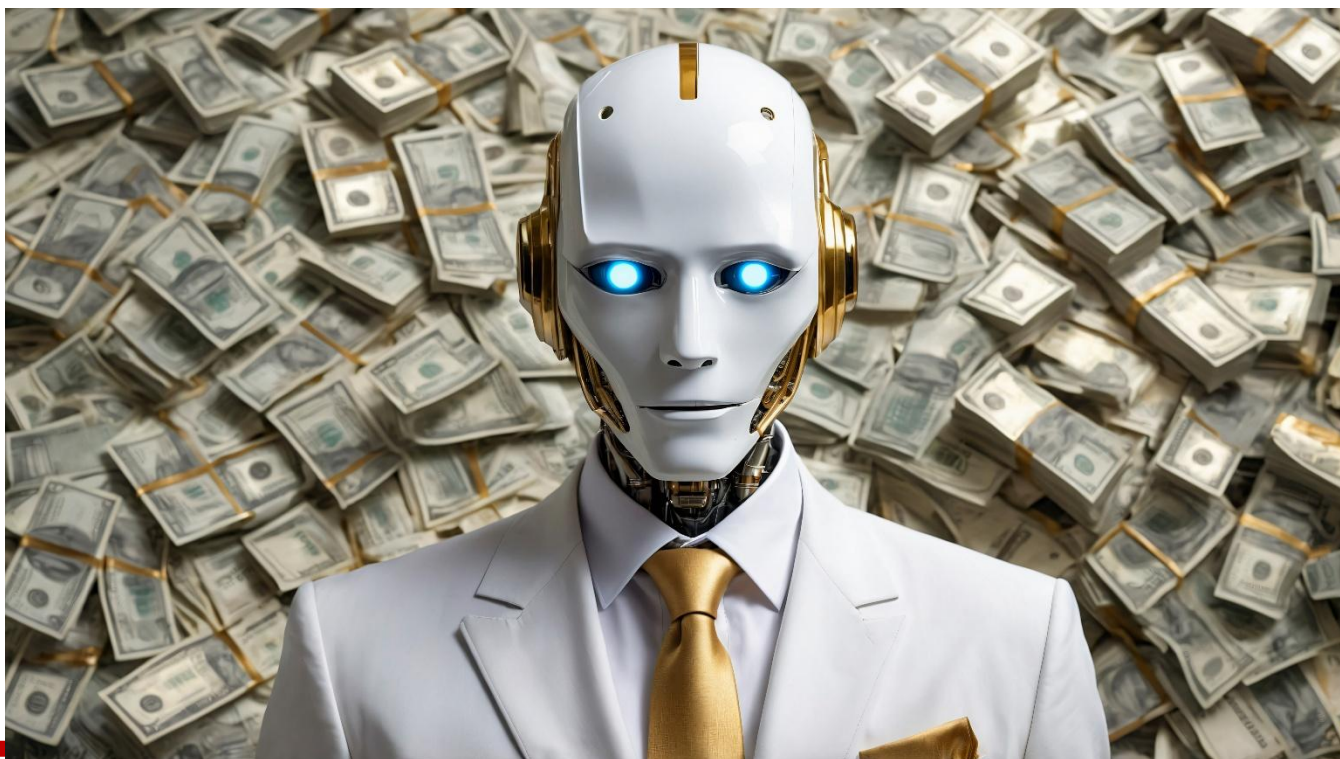


He previously worked as a Lead- Global Service delivery & Lead Consultant- Data Governance & Privacy at Provise Consulting (Baker Tilly GCE).

- Delivered 100+ big ticket projects for diverse businesses ranging from Telecom to Real Estate, predominantly in Middle East, India, South East Asia & Europe region

Before joining Provise, he was associated with Aditya Birla Group (ABG), where he was Leading- Risk & Data Privacy function for BMCSL HR Shared Service. He also worked in the Corporate Information Security team of ABG as an IS & Privacy Project Manager, where he was involved in - Information Security, Data Privacy, Business Continuity, Risk Management & Compliance for the entire ABG conglomerate at the central level with help of the team of 140 ABG CISOs. This includes the challenging task of defining the information security and privacy requirements for a global and sector diverse businesses (such as manufacturing, telecom, finance and retail)

Ankit Sharma can be reached at ankit.sharma@cyble.com and our company website <https://cyble.com/>



DeepSeek's AI Revolution: Cost Efficiency Meets Security Concerns

By Alix Melchy, VP of AI at Jumio

Artificial intelligence continues to reshape industries, and DeepSeek has emerged as a major player in the AI race. The model's rapid rise to fame — becoming the most-downloaded free app on the U.S. iOS App Store and surpassing competitors like ChatGPT — is a testament to its appeal. By achieving advanced AI capabilities at a fraction of the cost of its competitors, DeepSeek has captured the interest of enterprises and startups alike.

However, DeepSeek's success has also sparked concerns. U.S. lawmakers have raised national security and data privacy issues, leading to the introduction of the No DeepSeek on Government Devices Act to ban the app from federal devices. The controversy surrounding DeepSeek highlights a growing tension: how can enterprises take advantage of cost-efficient AI while ensuring data security and compliance with evolving global regulations?

DeepSeek's Appeal

DeepSeek's biggest draw is its cost-efficient, open-weight model, which significantly reduces AI deployment expenses. Unlike proprietary AI models, DeepSeek allows businesses to train and fine-tune models at a much lower cost. The company trained its model for just under \$6 million—a stark contrast to the billions spent by U.S. tech giants.

This affordability has made DeepSeek attractive for certain enterprise use cases, particularly in coding assistants, internal knowledge exploration, and processing sensitive data in airtight environments (where no data exits company premises). Startups and academia are also leveraging the technology due to its accessibility and flexibility.

The Security Risks of DeepSeek

While DeepSeek presents similar security risks as other generative AI models, such as biases, hallucinations, and potential copyright infringements, it introduces unique concerns tied to its Chinese data centers. A few prominent risks include:

Data transparency and compliance risks: DeepSeek does not disclose its training data, making it difficult to assess potential biases or data rights issues. U.S. and European enterprises must consider regulatory compliance risks when handling sensitive data with an AI model hosted in China.

Code and security vulnerabilities: All AI-generated code must be tested for security, suitability, and IP protection, ensuring it does not include open-source components with restrictive licenses that could compromise proprietary rights. For DeepSeek specifically, its undisclosed training data raises concerns that it may replicate coding patterns with inherent security vulnerabilities.

Data storage and government access risks: DeepSeek stores user data in China, raising concerns about government intervention. Chinese data center providers must comply with local laws, which could allow authorities to access stored information. This concern has fueled calls for tighter AI regulations and influenced the decision to ban DeepSeek from U.S. government devices.

Mitigating Risks: AI Governance and Compliance Best Practices

Enterprises looking to integrate DeepSeek, or any AI model, must implement a responsible AI framework to ensure security, privacy, and compliance. Elements of this framework include:

Self-hosting AI models: Running DeepSeek in a closed environment to prevent external data access.

Using synthetic data or strong anonymization protocol: Deploying advanced synthetic data generation tools to simulate real datasets without exposing sensitive information or anonymizing data.

Implementing strict AI governance: Establishing internal policies to oversee AI model use, security testing, and compliance with international regulations.

Should Enterprises Build Their Own AI Models Instead?

One alternative to using DeepSeek's API is for enterprises to develop their own AI models based on DeepSeek's techniques. Given its open-weight nature, companies with the expertise to fine-tune AI models may opt for a self-hosted approach that eliminates risks tied to third-party data storage. By taking control of the AI development process, organizations can reduce their dependence on external providers and mitigate concerns related to data privacy and security.

This approach may also help enterprises increase compliance, as it allows businesses to fully control the AI training and inference process, ensuring that sensitive data remains within their own infrastructure. Additionally, developing an in-house model enables organizations to tailor AI capabilities to their specific needs, optimizing performance while maintaining strict security protocols.

Seeking Alternatives to Safehouse Data

AI innovation must not come at the expense of security. DeepSeek's rise reflects the demand for affordable, high-performance AI, but enterprises must carefully weigh the risks. The model's China-based data storage, undisclosed training data, and potential security vulnerabilities introduce compliance challenges that businesses cannot ignore.

In 2024 alone, the use of generative AI among enterprises increased by 71%. As the adoption of this technology accelerates, companies must prioritize cybersecurity strategies that include robust security frameworks, regulatory alignment, and ethical AI practices to harness the benefits of AI while mitigating risks.

Businesses that proactively address these risks will be best positioned to leverage AI safely and effectively in a rapidly evolving technology and regulatory landscape.

About the Author

Alix Melchy is the VP of AI at Jumio, where he leads teams of machine learning engineers across the globe with a focus on computer vision, natural language processing and statistical modeling. An experienced AI leader, Melchy has a passion for turning AI-innovation into enterprise-grade AI systems, fostering the responsible practice of AI and shaping a secure digital landscape.

Alix can be reached on [LinkedIn](#) and at his company's website <https://www.jumio.com/>





Fake REAL Ids Have Already Arrived, Here's How to Protect Your Business

By Jillian Kossman, Vice President of Marketing & Policy, IDScan.net

When the REAL ID Act of 2005 was introduced, it promised to strengthen national security by setting higher standards for state-issued IDs, especially when it came to air travel, access to federal buildings, and more. Since then, the roll-out of the REAL ID program has faced delays, but with an impending enforcement deadline, many are questioning if REAL IDs deliver the level of security intended.

IDScan.net's latest testing of REAL IDs revealed overconfidence in ID security could be a tragic misstep. Running proprietary, AI-powered [ID verification](#) technology on over 170 million IDs scanned, we found that REAL IDs were actually **36% more likely to be flagged as fraudulent**. This means that while the process for obtaining a legitimate REAL ID is more rigorous, fraudsters are having no trouble fake identity documents claiming to be REAL ID compliant.

What is a Real ID?

Originally slated to take full effect in 2008, the REAL ID deadline has been pushed back multiple times, with the latest being May 7, 2025. In December 2020, Congress passed legislation allowing mobile driver's licenses (mDLs) to comply with REAL ID requirements. Since then, the TSA has taken over management of the initiative.

While the original aim was to prevent another 9/11-style attack, over 20 years later, the focus has shifted to protecting against identity theft and illegal immigration. The final deadline to get your REAL ID is now May 7th, 2025, owing in part to differing opinions and adoption rates state-by-state which has dragged enforcement on for two decades.

While there aren't any features of REAL IDs that are particularly radical in terms of identity documentation technology, they still bear the hallmarks of government-issued state IDs, such as holograms, UV images, and additional barcode security features that help verify the ID form's legitimacy.

Delayed rollout sparks security concerns

The delayed timelines of REAL ID adoption and enforcement have created a window of opportunity for fraudsters and criminals.

According to the Department of Homeland Security, as of January 2024, just over half (56%) of all IDs in circulation in the U.S. are REAL ID-compliant. While all states, territories, and the District of Columbia are now compliant with REAL ID standards, the percentage of REAL ID-compliant IDs varies greatly from state to state. In fact, in 34 states, less than 60% of IDs are REAL ID-compliant, and in 22 states, that number drops below 40%.

To put it into perspective, there are approximately 162 million REAL IDs in circulation, while around 110 million noncompliant IDs and 14 million legacy IDs (those issued before a state's REAL ID compliance determination) are also in circulation. The national adoption rate of REAL IDs is currently 0.56% per month, meaning by the enforcement deadline in May 2025, only around 61.2% of IDs will be REAL ID-compliant.

The delays and staggered adoption has given bad actors the chance to create templates for fraudulent REAL IDs. Businesses may incorrectly assume that an ID bearing a REAL ID star symbol are more likely to be legitimate, but as our data proves, this is not the case. REAL IDs can be faked just as easily as any other identity document, putting the onus on businesses to implement robust ID verification methods to ensure they don't fall victim to ID fraud.

The vast differences in ID documents, which vary state-by-state and are updated regularly, make verifying without an ID verification solution impossible. According to [IDScan.net research](#) from 2024 on the state of fraudulent identities, 26% of all fake ID catches were from out-of-state IDs. Unfamiliarity with various forms introduces additional risk, particularly when attempting to verify without technology.

A staggered approach to REAL ID rollout, or at least faltering adoption, also has a more dangerous effect on businesses' ability to prevent ID fraud: we've enabled fraudsters to get ahead of the game in the production of REAL ID fakes.

This throws the security 'benefits' of a REAL ID into serious debate, how secure is an identity form, if fraudulent copies are so prevalent?

Steps to combatting REAL ID fraud

The deadline for REAL ID enforcement is quickly approaching, whether individuals and businesses are prepared or not. There is a greater degree of risk in assuming a REAL ID is more secure than other forms. However, with the right outlook, operational set-up, and identity verification technology, businesses can still stay ahead of bad actors.

Cover all touchpoints with ID scanners

The best way to protect your business from rising identity fraud is to make sure all potential touchpoints are covered. Fraudsters are tech-savvy and deliberate, and have the know-how to identify the weakest link in your security. For physical spaces, such as stadiums, hotels, retail stores, and warehouses, ensuring ID scanners are present at all relevant locations and entrances is a must; failing to cover just one entrance is the same as failing to cover all of them.

Identity verification providers have worked hard to provide affordable verification solutions to all manner of businesses, from the world's largest hotel and automotive chains to independently run retail stores.

While the best identity verification solutions can catch the majority of fake IDs - IDScan.net's proprietary ID authentication solution averages [95%](#), and for emerging forms, such as AI-generated IDs, catch rates increase to 99.6% - there is always a chance the very best fake document may slip through. Businesses using ID verification solutions remain exponentially safer from the repercussions of ID fraud.

When looking for the right provider, consider the following features:

Document authentication efficacy

Authentication ID scanners use a series of light checks, typically UV, IR, and white light, and when paired with other identity verification software, such as VeriScan Authentication, businesses can reference these security features against each state's template. VeriScan Authentication can also crossmatch the data embedded in the barcodes with the ID's text-based information.

Diversified verification

Many identity verification companies only offer two or three hardware options compatible with their software, which takes a one-size-fits-all approach that doesn't account for each organization's unique threat landscape and operational standards.

Businesses should utilize ID scanners that are flexible and capable of processing across both computer and smartphone devices. While the objective is the same, portability can be a crucial factor in ensuring all customers are verified to be who they say they are.

Future-proof solutions

As ID fraud becomes more sophisticated and accessible, it is essential to choose an ID verification solution that is looking ahead to spot trends or security weaknesses before criminals can strike.

AI-powered identity verification is one of the only ways to combat the increasing use of AI-powered criminal tools. VeriScan uses machine learning algorithms to analyze high volumes of data and identify patterns associated with synthetic identity fraud. AI-powered systems can detect imperfections and indicators commonly seen on fraudulent identity documents to instantly flag fraudulent identity documents.

The use of [third-party database](#) checks can further strengthen identity verification processes. Integrated third-party checks, such as DMV database checks, can significantly increase the chances of catching fake IDs by verifying the data presented on the identity document against trustworthy databases.

POS integrations

Existing POS processes are crucial in making your business tick, so verification solutions need to complement existing workflows. When researching identity verification solutions, it is also important to consider existing workflows and point of sale (POS) systems. Utilizing an age verification API or SDK integrated into existing workflows means you're not sacrificing efficiency for security.

The best providers acknowledge the need for seamless verification, and solutions such as ParseLink quickly scan, parse data, and auto-populate to the right location of your respective POS. These technologies work the same for REAL ID as they do with other forms.

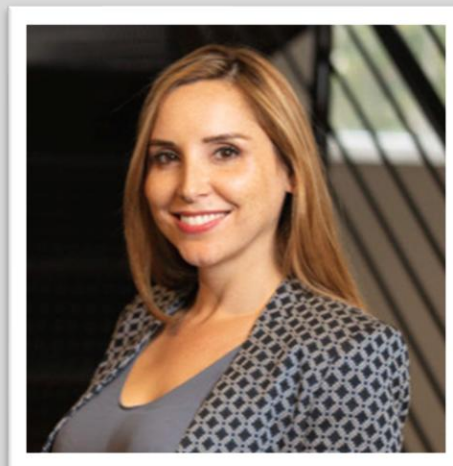
While the threat of a fake REAL ID carries no larger weight than traditional fakes for the majority of businesses, we recommend a proactive approach to educating staff that REAL ID fakes are out there in droves. Businesses need to ensure their verification provider is innovating to combat new fraud types and ensure that the way they integrate catalyzes stronger protection and customer experience, not detract from it.

With the right solution provider onboard, all forms of ID fraud, including REAL ID fraud, can be mitigated.

About the Author

Jillian Kossman currently serves as Vice President of Marketing & Policy at IDScan.net, where tenure began in March 2022. Previously, Jillian held various marketing leadership roles, including Director of Marketing at DNSFilter and iSeatz, contributing significantly to the marketing strategies of notable clients such as American Express and Visa. Experience also includes directing marketing efforts at Furlane, Inc., and leading digital initiatives for the Travis County Democratic Party. Jillian's marketing expertise was further honed at LookFar, managing comprehensive strategies across marketing channels, and as Account Director at Keating Magee, focusing on healthcare-related clients. Early career involvement as Marketing & Community Relations Manager at War Era Veterans Alliance underscored a commitment to community outreach. Educational background includes a Bachelor's degree in Literature from the University of California, Santa Cruz. Additionally, Jillian is an active Committee Member on the State Regulatory Committee for the National Cannabis Industry Association since July 2023.

<https://idscan.net/>





Five Crucial Insights to Combat Today's Deepfake Phenomenon

By Dominic Forrest, Chief Technology Officer, iProov

In today's rapidly evolving cybersecurity landscape, distinguishing fact from fiction has become increasingly challenging due to the rising threat of deepfakes. These sophisticated AI-generated impersonations have emerged as a formidable danger, catching even the most vigilant organizations off guard. The recent [\\$25 million deepfake scam](#) against global engineering firm Arup serves as a stark reminder of the financial and reputational risks posed by deepfake technology.

Deepfakes present a significant problem in our increasingly interconnected digital world, where the ability to trust the identity of individuals within digital ecosystems is paramount. In fact, a recent [study](#) of global technology leaders by iProov showed deepfakes rank equal with phishing/social engineering attacks as the third most prevalent security concern, after password breaches and ransomware.

This article explores five crucial insights into the deepfake phenomenon, shedding light on why many organizations underestimate the risk, the effectiveness of biometric defenses, the necessity of multi-

layered security approaches, and the critical role of leadership in combating this sophisticated form of cyber deception.

1. Deepfakes Are a Real and Present Danger

The Arup scam spotlights the tangible financial and reputational risks deepfakes present. In this instance, an Arup employee transferred unauthorized funds to the tune of \$25 million after being duped by AI-generated deepfakes of senior company officials during a video call. This incident proves that even the most security-conscious organizations are vulnerable to sophisticated identity-centric cyberattacks.

As deepfake technology becomes more accessible and advanced, the potential for its malicious use in various sectors, including business, finance, politics, and social media, continues to grow.

2. Too Many Organizations Underestimate the Risk

According to the [iProov data](#), 70% of technology leaders believe AI-generated attacks will significantly impact their organizations. However, the [same study](#) found over two-thirds (62%) worry their organizations aren't taking the threat seriously enough. This disconnect highlights the need for more proactive and robust measures to mitigate the risks posed by deepfake technology. Organizational complacency can be traced to several factors, including lack of awareness, where decision-makers may not fully understand the capabilities of deepfake technology nor its potential impact on their organization. Another issue is a false sense of security: organizations may believe their existing security measures are sufficient to protect against such attacks. Lastly, some organizations may view deepfake attacks as unlikely or too sophisticated to target their specific industry or company. Unfortunately, for many, this assessment will turn out to be incorrect.

However, deepfakes threaten any situation where remote identity verification is needed, making them a powerful tool for launching cyberattacks, particularly financial fraud where the potential reward for threat actors is high. As remote work and digital communications continue to dominate the business landscape, the attack surface for deepfake-enabled deception expands.

3. Biometrics with Liveness Detection is the Most Effective Defense

Biometric face verification with strong liveness detection offers the most reliable method of remote identity verification. This is backed up in the study, with a resounding 75% of organizations turning to facial biometric solutions as their primary defense against deepfakes. This reflects a growing recognition of facial biometrics' ability to provide more secure and reliable identity verification compared to traditional methods like passwords, which are easily shared, lost or stolen.

Liveness detection prevents criminals or impostors from spoofing the system using photographs, videos, masks, or other non-living artifacts. The ability to establish 'liveness' - confirming the presence of a real, live person during authentication - significantly mitigates the risk of scalable, low-cost spoofing attacks

like deepfakes. This technology provides a crucial layer of security that traditional methods like passwords or other biometrics lack.

By combining these techniques with advanced machine learning algorithms, organizations can create a robust defense against even the most sophisticated deepfake attempts.

4. A Multi-Layered Approach is Necessary

To combat the deepfake threat effectively, organizations should implement a proactive, multi-layered strategy. This includes:

- **Advanced Authentication:** Utilizing biometrics and strong liveness detection technologies as the first line of defense.
- **AI-Powered Detection Tools:** Implementing solutions that can analyze and detect subtle inconsistencies in video and audio content.
- **Continuous Monitoring:** Adopting systems that can identify atypical patterns or behaviors indicating a potential deepfake attack.
- **Incident Response Plans:** Developing clear procedures for containing and mitigating damage in case of a breach.
- **Employee Training:** Building awareness among staff about the risks of deepfakes and their risks, and how to identify potential threats.

5. Leadership Must Set the Tone for Battling Deepfakes

Organizational leaders play a crucial role in preparing for deepfake threats and setting the tone for the entire company. This means prioritizing cybersecurity investments so there are sufficient resources to implement and maintain advanced security measures. Fostering a culture of awareness and promoting ongoing education and vigilance among all employees regarding cybersecurity risks creates an internal army ready to fight back against deepfake threats. It's also essential for companies to embrace emerging technologies in the war on deepfakes. This includes leveraging advanced AI-based solutions with the sophistication to stay a step ahead of AI-generated deepfakes.

Conclusion

The threat of deepfakes is real and growing, with the potential to cause significant financial and reputational damage to organizations across all sectors. As the line between reality and digital fabrication continues to blur, understanding and addressing this risk is essential for any organization seeking to protect its assets and reputation in the digital age.

By acknowledging the reality of the deepfake threat, implementing robust biometric defenses, adopting a multi-layered security approach, and ensuring leadership commitment to cybersecurity, organizations can significantly enhance their resilience against deepfake attacks. As deepfake technology evolves, so

must the strategies for combating these sophisticated forms of deception, ensuring a safer and more secure digital future for all.

About the Author

Dominic Forrest is Chief Technology Officer at iProov, a leading provider of science-based solutions for biometric identity verification.

Dominic can be reached at our company website <https://www.iproov.com/>





From Factory Floor to Second Life: Why Platform Security Must Be Managed Throughout the Lifecycle of a Device

By Boris Balacheff, Chief Technologist for Security Research and Innovation at HP Inc.

Laptops, PCs and printers are the workhorses of the modern enterprise. Given their multi-year lifespan, and the growing importance of device security down to the hardware and firmware level, the choice of endpoints is foundational for securing enterprise infrastructure. Just like software, device security should be assessed, managed and monitored proactively through its lifetime – from manufacturing to onboarding, ongoing management, remediation, and even second life or decommissioning.

[New research from HP Wolf Security](#) reveals that despite the growing awareness of the importance of device security – securing the hardware and firmware of PCs, laptops printers, or other devices – it is often overlooked. Part of this stems from a lack of maturity, with 79% of IT and Security Decision Makers (ITSDMs) saying their understanding of hardware and firmware security lags behind their knowledge of software security. But part of it is down to the recent evolution of the device technology landscape, where not all vendors prioritize this area of technology, and many don't provide tools and capabilities to simplify ongoing management of hardware and firmware security.

There are security challenges at every stage of the device lifecycle that can only be solved with an end-to-end approach to securing and managing hardware and firmware configuration.

Why platform security?

Hardware and firmware attacks are difficult to detect and expensive to fix, providing a stealthy and persistent foothold into IT infrastructure and networks. This has been driving investments and interest on the attack side and makes device security an increasingly important layer of the IT stack to achieve resiliency.

A core challenge with device security at the hardware and firmware level is that it is very hard, if even possible, to address with software alone. This is why it is key for manufacturers to invest in security by design from the hardware-up, including building the necessary manageability capabilities for a modern hybrid workforce.

Device security should be considered from the procurement stage, but it is usually ignored in favor of short-term gains, such as reduced costs. In fact, 68% of ITSDMs say hardware and firmware security is often overlooked in the evaluation of the total cost of ownership (TCO) for managing device security through its lifecycle. It is important to remember that purchasing a device is a security decision, with the wrong choice having far-reaching implications that can weaken security posture or increase infrastructure security management costs for years to come.

Organizations need to develop the capability to set requirements for device hardware and firmware, as well as the necessary lifecycle management processes to ensure that devices can be trusted to operate as expected throughout their lifetime. This requires an end-to-end approach, considering platform security across the entire device lifecycle.

1. It starts with suppliers

Taking control of device security starts with supplier selection. Too often, procurement teams work alone to source devices, without the expertise of security and IT teams to evaluate vendors and guide security requirements that may have long term security and manageability implications across the fleet. In fact, more than half (52%) of ITSDMs say procurement rarely collaborates with IT and security to verify suppliers' hardware and firmware security claims.

Collaboration between IT, security, and procurement is key to ensuring that procurement requirements appropriately serve the long-term security posture and digital strategy of an organization. This includes setting procurement requirements for device hardware and firmware security capabilities, and articulating standards to audit supplier security governance. The latter is not broadly practiced, but our findings show that 34% of organizations that do audit suppliers have had a PC, laptop, or printer supplier fail a cybersecurity audit in the past five years. Almost a fifth claim the failure was so serious that they terminated their contract.

2. Onboarding and configuration go off track

The risk of hardware or firmware tampering exists at every stage of a device's lifecycle. While a device is in transit, or simply unattended, it could be tampered with to insert malware or malicious hardware

components. This is compounded by poor BIOS administration security practices. More than half (53%) of ITSDMs admit to using BIOS passwords that are shared, used too broadly, or are not strong enough. The same number say they rarely change these passwords over the lifespan of a device.

Without strong BIOS passwords, threat actors could gain unauthorized access to firmware settings, significantly weakening devices by turning off security features. Over half of ITSDMs (55%) would like to set BIOS passwords to protect firmware settings but say they can't because it is too complicated or costly.

3. Ongoing management woes

More than three quarters (78%) say they need to continuously validate the integrity of devices across the lifecycle. This is because the security of the device infrastructure depends on low-level firmware security and configurations.

However, poor firmware update practices are widespread, and make ongoing integrity monitoring a significant challenge. Over 60% of ITSDMs do not make firmware updates as soon as they're available for laptops or printers, while 57% say they hesitate to deploy updates because of risks of disruptions to their users and applications. This hesitancy is concerning as 80% of respondents fear the rise of AI could mean attackers can develop exploits much faster.

4. Remediation struggles

Establishing and maintaining a strong device security posture involves managing threats that target hardware and firmware across device fleets. This means IT and security teams must be able to continuously monitor and remediate security issues quickly. However, organizations report being ill-equipped to tackle hardware and firmware level platform threats, with 60% of ITSDMs saying that detection and mitigation of such attacks is impossible, viewing post-breach remediation as the only path.

For laptops, monitoring and remediation must also extend to lost or stolen devices. Work-from-anywhere employee behavior is a key factor behind thefts and losses, with one in five remote workers having lost a device or having one stolen. The study also revealed that, on average, there was a 25-hour delay in notifying IT when an employee device was lost or stolen. This gap gives threat actors a dangerous head start. To address these monitoring and remediation gaps, organizations need to look beyond detection, focusing on built-in capabilities to prevent, contain and recover against hardware and firmware attacks.

5. A risky second life

The end of the device lifecycle is fraught with risk. As a result, many organizations often destroy devices over security concerns because they find it too difficult to give them a second life, compounding e-waste and running counter to sustainability goals. In fact, some 69% of ITSDMs say they have many devices that could be repurposed or donated if they could be securely decommissioned.

What's more, employees may hold onto old laptops and PCs, creating further visibility and security gaps if these machines still carry sensitive corporate data.

If organizations do not have a secure way to erase sensitive hardware and firmware data and enable safe decommissioning, they are missing out on quick and easy Environmental, Social, and Governance (ESG) wins. They are also unable to redeploy devices securely, and reduce the Total Cost of Ownership (TCO) of machines.

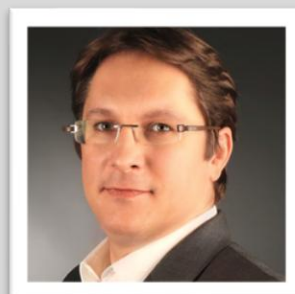
The pathway to device security

To address these challenges, organizations should first bring IT, security and procurement teams together to ensure they bring security requirements into purchasing decisions that consider the entire device lifecycle. Next, investigate solutions that flag when devices have been tampered with, and that enable zero-touch onboarding, as well as stronger alternatives to BIOS passwords. Organizations then need to prioritize devices and tools that allow hardware, firmware configurations, and security updates to be managed proactively and remotely across the fleet.

Finally, organizations should look for devices that can securely and verifiably erase sensitive hardware and firmware data even when the devices are powered down – solutions that already exist on the market. This will streamline decommissioning and help organizations meet sustainability goals. Securing PCs, laptops and printers is often overlooked or taken for granted. But since they are critical entry points into corporate IT infrastructure, they must be judiciously procured, so that teams have the tools and device capabilities to enable them to closely manage, monitor, and securely decommission their fleets.

About the Author

Boris Balacheff is Chief Technologist for System Security Research and Innovation at HP. He leads HP's Security Lab's research strategy, from analyzing and reporting on trends in the threat landscape, to designing security from the hardware and firmware up. Boris shapes security technology strategy at HP in partnership with HP business units and customers. He and his team drive academic, industry and government collaborations to improve on the state of the art and progress standards, from supply chain security to migration to post-quantum cryptography. Named on over 40 US patents, Boris is an inventor of modern approaches to hardware design for firmware and software resilience, and an early contributor to Trusted Computing standards and technologies. Boris is a Director of the Trusted Computing Group (TCG) where he chairs the Certification Program Committee.



Boris can be reached online at LinkedIn <https://www.linkedin.com/in/boris-balacheff-26381> and at our company website <https://www.hp.com>.



The Future of Automotive Cybersecurity Safeguarding the Next Generation of Mobility

By Bhushan Dhumal

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.

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.

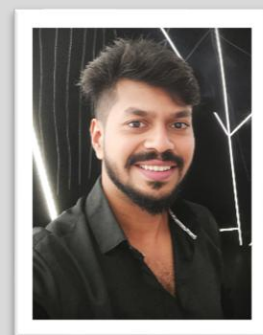
Future Outlook

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.





How to Adopt Advanced Edge Cybersecurity to Protect Smart Buildings

By Fabio Zaniboni, Founder & Chief Executive Officer at BubblyNet

The increasing digitization of smart buildings presents both unprecedented convenience and significant cybersecurity challenges. With the number of [IoT devices globally projected to reach 40 billion by 2030](#)—up from 16.6 billion in 2023, and interconnected systems managing critical functions such as access control, HVAC, and lighting, the potential attack surface for cybercriminals continues to expand. A comprehensive approach to security by leveraging edge computing, hardware-based solutions, air gapped systems, and secured wireless protocols such as Bluetooth® Mesh technology, is essential to mitigate these risks and safeguard sensitive data.

Top Biggest Security Flaws in Existing Smart Building Frameworks

Cyberattacks on IoT devices have been increasing rapidly, [growing by 400% year-over-year \(YoY\)](#). Traditional cybersecurity frameworks for smart buildings often rely on centralized cloud-based architectures, creating several vulnerabilities. One of the most critical flaws lies in the dependency on internet-connected systems to control building operations. These frameworks inherently introduce risks such as remote exploitation, unauthorized access, and the potential for widespread system failures in the event of a Cyberattack.

Additionally, many smart building solutions lack robust encryption standards, leaving transmitted data susceptible to interception. Weak authentication protocols further exacerbate these risks, enabling cybercriminals to gain entry to building networks and manipulate critical infrastructure.

Cloud-Based Operation and Increased Cyber Threat Vulnerability

Cloud dependency remains a major weak point in smart building security. While cloud solutions offer scalability and remote accessibility; they also create multiple vulnerabilities. Any system that transmits data over the internet inherently exposes itself to interception, hacking, or service disruptions. Cloud-based architectures are often targeted by distributed denial-of-service (DDoS) attacks, which can bring down critical systems and disrupt building operations.

Another issue is data privacy. Cloud-reliant systems collect, process, and store vast amounts of occupant data, including access credentials and behavioral patterns. This concentration of sensitive information makes cloud-based platforms attractive targets for cybercriminals. Moreover, misconfigurations in cloud security settings or inadequate encryption measures can expose user data, leading to potential breaches with severe financial and reputational consequences.

Keys to Transform Cybersecurity in Smart Buildings: Edge Computing, Air Gapped Networks, and Hardware-First Security

A shift toward a decentralized approach by eliminating external access points can address these vulnerabilities effectively.

- **Edge Computing for Real-Time Security:** Processing data at the edge— closer to its source— significantly reduces the risk of cyberattacks by minimizing data transmission to external networks. By keeping critical information within the local environment, organizations can limit exposure to remote threats while ensuring faster response times for threat detection and mitigation.
- **Air-Gapped Networks for Enhanced Isolation:** Air-gapped systems physically separate critical networks from the internet and other external access points, preventing cyber intrusions. This approach ensures that even if one system is compromised, it does not serve as a gateway to the entire infrastructure. With air-gapped networks, malicious actors are unable to exploit remote entry points, reducing the likelihood of ransomware attacks and unauthorized system manipulations.
- **Hardware-First Security for Data Privacy:** Implementing security at the hardware level ensures that only essential data is collected, minimizing exposure to potential breaches. For instance, instead of recording and transmitting full audio feeds, security solutions can be designed to analyze data in real-time and transmit only essential signals, such as identifying abnormal sound patterns without recording conversations. Similarly, motion sensors can differentiate human presence, eliminating the need for invasive surveillance.

Bluetooth® Mesh Security: Encryption, Authentication, and Privacy

Bluetooth® Mesh has emerged as a powerful networking open standard for smart buildings, industrial automation, and connected lighting systems. With its ability to support thousands of devices in a decentralized network, security is a top concern. Cyberattacks such as eavesdropping, replay attacks, unauthorized access, and denial-of-service (DoS) attacks pose serious threats to IoT systems.

Fortunately, Bluetooth® Mesh incorporates multiple layers of encryption, authentication, and privacy protection to safeguard networks from cyber threats.

1. Strong Encryption & Authentication

Bluetooth® Mesh ensures that all communication is encrypted to prevent unauthorized access. It uses AES-128 encryption with Counter with CBC-MAC (CCM) to protect data transmitted across the network. Even if an attacker intercepts a message, they cannot read or modify it without the correct encryption keys.

Each message also contains a message integrity check (MIC) to verify its authenticity. This prevents attackers from injecting fake messages or altering commands sent between devices. Additionally, Bluetooth® Mesh protects against replay attacks by using sequence numbers—ensuring that older messages cannot be resent by an attacker to manipulate devices.

2. Secure Device Provisioning

Before a device can join a Bluetooth® Mesh network, it must go through a secure provisioning process to prove its authenticity. This process includes:

- Out-of-Band (OOB) authentication, such as QR codes or NFC, to verify legitimate devices.
- Elliptic Curve Diffie-Hellman (ECDH) encryption, ensuring that device provisioning is secure against man-in-the-middle (MITM) attacks.

Unlike some IoT systems that rely on default passwords or pre-configured security credentials, Bluetooth® Mesh ensures that all devices establish secure keys during provisioning, preventing attackers from exploiting weak authentication.

3. Network-Level Security

Bluetooth® Mesh networks use a three-tiered key system to provide strong security at different levels:

- Network Key (NetKey): Encrypts messages at the network level, ensuring all devices in the mesh are authenticated.
- Application Key (AppKey): Used for specific applications, preventing unauthorized devices from accessing sensitive functions (e.g., lighting control vs. security systems).
- Device Key (DevKey): Assigned to each device during provisioning, preventing rogue devices from impersonating others.

If a device is compromised, Bluetooth® Mesh supports a key refresh mechanism, allowing administrators to generate new encryption keys and remove unauthorized devices from the network.

4. Privacy Protection

To prevent tracking and data theft, Bluetooth® Mesh devices use randomized source addresses that change periodically. This prevents attackers from identifying or tracking specific devices based on their network activity.

Additionally, message relays in the mesh network do not decrypt forwarded messages. This means that even if an attacker gains control of a relay node, they cannot read the message contents or identify the sender, enhancing overall network privacy.

5. Defense Against Denial-of-Service (DoS) Attacks

Bluetooth® Mesh has built-in mechanisms to prevent message flooding attacks, where an attacker attempts to overwhelm the network by sending a large number of requests. Rate-limiting ensures that devices cannot overload the network with excessive messages.

Suspicious devices can also be blacklisted or temporarily blocked, preventing malicious nodes from disrupting operations. Additionally, because Bluetooth® Mesh devices do not connect directly to the internet, they are less vulnerable to remote cyber threats compared to traditional Wi-Fi-based IoT systems.

A cyber-secure approach to Smart Buildings

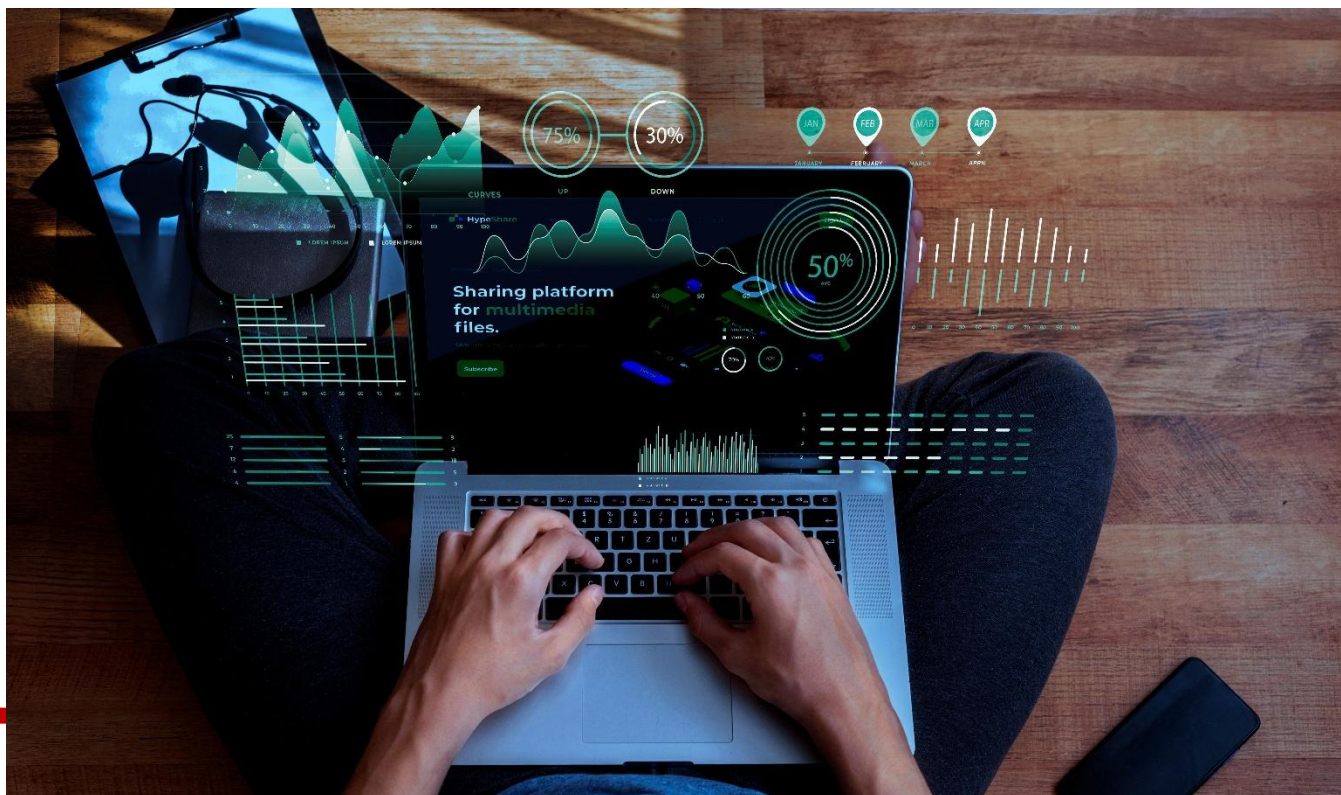
As cyber threats evolve, so too must the security strategies used to protect smart buildings. A holistic approach that integrates edge computing, air-gapped networks, and hardware-first security measures provides a stronger defense against emerging threats. By decentralizing data processing and minimizing cloud exposure, smart building operators can significantly enhance security while maintaining user privacy. The adoption of Bluetooth® Mesh further strengthens authentication protocols, ensuring robust protection against unauthorized access.

With the growing need for resilient cybersecurity frameworks, organizations must rethink their reliance on traditional, cloud-based security models. Prioritizing hardware-based security and decentralized network architectures is key to safeguarding the future of smart buildings from cyber threats.

About the Author

Fabio Zaniboni, Founder and CEO of [BubblyNet](https://bubblynet.com/), is a technology leader with over two decades of experience in the Internet of Things (IoT), digital transformation, and sustainable innovation, particularly in the lighting industry. His career, including roles at Emerson Electric and Comau Robotics, has given him a global perspective and market insights. Leading an R&D team, Fabio integrates advanced technologies to enhance building efficiency, sustainability, and user experience. His research on how factors like light, sound, and air affect well-being is driving smarter, more sustainable building solutions. Known for transforming complex technologies into scalable applications, Fabio partners with global organizations to foster digital innovation and sustainability in the built environment. For more about BubblyNet visit <https://bubblynet.com/>.





How To Leverage Cloud Analytics to Detect and Prevent Cybersecurity Threats in Real-Time

By Laurence Dale, CISO, Surveil

Today, cloud environments are more complex than ever. Organizations are navigating multicloud, multi-tenant, multi-national, and multi-business unit landscapes. On top of this, the speed of fluctuation in usage and cloud consumption adds another layer of complexity. This increases an organization's attack surface, leaving it more vulnerable to cyber-attacks and data breaches that can cost business millions of dollars.

Microsoft Azure gave some interesting insights at the start of 2025. The cloud computing platform reported that towards the end of 2024, [it was mitigating up to 3,800 attacks daily, and 20% of those were large-scale attacks comprising more than one million packets per second \(pps\)](#). It's therefore more important than ever to utilize cloud analytics tools to mitigate risk. These tools help CISOs and their teams to gain real-time insights and comprehensive visibility to proactively detect threats before they can cause harm.

Here are five tips to ensure best practice when leveraging cloud analytics to detect and prevent cybersecurity threats:

1. **Implement Continuous Security Monitoring (CSM) and Real-Time Alerts:** CSM tools are essential for early detection and swift response to potential threats. Cloud analytics play a crucial role in this process by continuously monitoring your environment and setting up real-time alerts for any suspicious activities or anomalies. This is especially important in complex cloud environments where workloads are constantly being moved, and user licenses are frequently added or removed.

Real-time alerts enable security teams to respond immediately to potential threats, minimizing the impact of cyber-attacks. For example, if an unusual login attempt is detected, an alert can be triggered, allowing the security team to investigate and take appropriate action. This proactive approach helps prevent security breaches before they occur.

2. **Utilize Machine Learning and Behavioral Analysis:** Machine learning and behavioral analysis are powerful tools for predicting and preventing cybersecurity incidents. These technologies use algorithms to analyze massive data sets in real-time, identifying patterns and detecting anomalies that may indicate security threats.

Cloud analytics enhances these capabilities by providing the data needed for machine learning models to learn and improve. For instance, behavioral analysis can track user behavior over time, identifying deviations from normal patterns that could signal a potential threat. By leveraging cloud analytics, organizations can gain deeper insights into user behavior and detect threats more accurately.

3. **Maintain Comprehensive Activity Logs:** Activity logs provide detailed information about system operations, making troubleshooting faster and more efficient. Cloud log management tools can analyze logs from various sources, correlate events, and provide an overall view of system operations.

Maintaining comprehensive activity logs is crucial for forensic analysis and auditing. Cloud analytics can help by aggregating and analyzing log data, providing insights into who did what and when. This level of detail is essential for identifying the root cause of security incidents and ensuring accountability.

To maximize the effectiveness of activity logs, organizations should ensure notifications are switched on within their log management platform. This way, they can be alerted to any suspicious or unusual activity in real-time. Additionally, it's important to retain activity logs for the recommended length of time for the log type, to ensure that historical data is available for analysis.

4. **Enforce Strong Identity and Access Management (IAM):** IAM is a critical component of cloud security, and can help protect organizations from up to [600 million identity attacks per day](#). Implementing robust IAM policies helps control access to cloud resources and reduces the risk of intrusion, data loss, or ransomware attacks.

Cloud analytics enhance IAM by providing visibility into access patterns and identifying potential security risks. For example, analytics can track login attempts, flagging any unusual activity that may indicate unauthorized access. By using a zero-trust model, including multi-factor authentication (MFA) and least privilege principles, organizations can minimize the risk of unauthorized access.

5. Establish Comprehensive Cybersecurity Training and Upskilling with Advanced Analytics

Tools: Back in 2019, Gartner claimed that [99% of all cloud security failures would be the customer's fault by 2025](#), primarily due to a lack of full visibility and understanding of their complex cloud environments. Businesses must gain a deep understanding of their data and have speed to insights to effectively secure and control their cloud infrastructure. This feat cannot be achieved alone or with sole reliance on native security tooling.

By combining comprehensive visibility with advanced analytics tools, organizations can upskill their workforce, reduce the risk of customer error, and maintain a secure cloud environment. This proactive approach not only enhances the ability to detect and respond to threats in real-time but also fosters a culture of continuous improvement and security excellence.

Through continuous monitoring, machine learning, and strong identity management, IT security teams can ensure a secure and compliant cloud environment that reduces the chance of customer error. Cloud analytics provide real-time insights and proactive threat detection – essential for preventing cybersecurity threats and protecting cloud infrastructure.

By following these best practices, organizations can leverage cloud analytics to enhance their cybersecurity measures, ensuring that they stay ahead of potential threats and maintain a secure cloud environment.

About the Author

Laurence Dale is CISO at Surveil – an analytics and insights engine – which can help optimize IT spending to reduce waste and unlock funds for investment in crucial cyber defenses. Throughout his 25-year technology career, Laurence has gained invaluable global experience through several senior IT leadership roles. Laurence has been responsible for driving the digital, security, and commercial capabilities of multi-national organizations across the FMCG, technology, and manufacturing industries, as well as the UK public sector. In 2017, Laurence took the position of Chief Information Security Officer (CISO) at Essentra PLC., where he led the cyber-risk and privacy management transformation programs. This was followed by a promotion to Group IT Director (interim CIO), leading the global IT team through two major divisional divestments.



Laurence's LinkedIn page can be found here <https://www.linkedin.com/in/laurencedale/>. Our company website is here: <https://surveil.co/>



How to Stop Infostealers and Next-Gen Ransomware with an Identity-Centric Security Approach

By Trevor Hilligoss, SVP of Security Research, SpyCloud Labs at SpyCloud

Ransomware is the leading cybersecurity threat across every industry and a top priority for every Security Operations Center (SOC) team according to the [SpyCloud 2024 Malware and Ransomware Defense Report](#). When focusing on mitigating ransomware risk, it's important not to overlook the growing threat of infostealer malware (“infostealers”) – an often quiet precursor to ransomware attacks.

Our research has revealed that one-third of companies who fall victim to ransomware have experienced at least one infostealer infection within 16 weeks before the attack – a crucial warning sign.

What is Infostealer Malware?

Threat actors use infostealer malware to infiltrate devices and steal any and all information that can be of value – login credentials, session cookies, personally identifiable information (PII), authentication data,

and much more. Bad actors can then sell or trade the most critical access to specialized brokers, or use it themselves, to gain unauthorized access to systems and networks to facilitate follow-on attacks, including ransomware.

The Infostealer Challenge

Unfortunately, infostealers can be challenging to identify and often leave little evidence – going unnoticed for days or weeks before the initial infection and stolen information has been detected. Even after an infection is detected and remediation has begun, stolen information may be difficult or impossible to fully invalidate; resulting in an elevated risk for months or even years.

Despite the growing concern about infostealers and high-profile incidents (like the previous [Medibank](#) breach), organizations still have significant gaps in their ability to address malware exposures. Typical machine-centric malware response processes emphasize a three-step approach of 1) detection and analysis, 2) containment, and 3) eradication and recovery. However, a “brute force” reset and wipe doesn’t solve the larger issue of stolen data, and thus access, in the wrong hands.

Addressing the Infostealer Threat

To combat the risks associated from data siphoned from malware-infected devices, a more identity-centric approach is required to prevent cybercriminals from gaining credentials to successfully carry out attacks and profit from stolen data. Here are three things SOC leaders can do to gain the upper hand:

1. Act on Compromised Data

As every SOC team member knows, remediating a malware infection can feel a bit like playing darts in a heavy fog. Having better visibility of malware-exfiltrated data (such as exposed credentials and session cookies and other tokens) can simplify the process of remediation and significantly improve an organization’s resistance to ransomware attacks.

The approach – known as Post-Infection Remediation (PIR) – works like this. Once an infected device is identified, security teams must respond swiftly. The first step is to clear the infected device. However, as soon as the immediate risk of an ongoing infection event is mitigated, teams must begin the work of identifying what identity data may have been exposed. In many cases, this involves going to where the criminal communities are trading data: the dark web, criminal forums, and messaging platforms.

With access to the data criminals have in hand from the dark web, organizations have better visibility into the overall exposure and cyber risk to their business. Knowing what data is in the hands of criminal actors, the SOC can remediate all compromised credentials and systems impacted by an attack by resetting application credentials and invalidating session cookies exfiltrated by malware. If all exposed data is reset, a follow-on ransomware attack has a low probability of occurring.

2. Mitigate the Risk from Third-Party Exposure

Threat actors leverage a range of strategies to gain the upper hand in the ransomware landscape. Still, nothing presents as ample an opportunity as malware-infected third-party and unmanaged devices used to access corporate applications.

Whether these devices belong to employees or third parties, a single device infected with infostealer malware can open the doors for threat actors to move laterally beyond the initial endpoint, gaining access to potentially hundreds of applications and stealing thousands of third-party credentials. This can quickly escalate to a ransomware attack, especially if persistent access credentials like API keys, long-lived authentication cookies, or administrative credentials are compromised.

Security researchers found that as many as 90% of security compromises [originate from unmanaged devices](#), and third-party access is only second to phishing as a common entry point for ransomware. Many exposures result from enterprise data siphoned out of a managed network as a result of ease-of-access systems that sync credentials and other information between connected devices.

Outside of traditional IT control and without visibility into these exposures, it's difficult for an organization to fully understand its risk and properly defend itself.

To negate the opportunities for third-party exposure, security teams need to work proactively to illuminate the full attack surface. This includes continuously monitoring for exposed identities on the dark web so they can identify compromised accounts before they are exploited. By improving visibility into malware-exfiltrated data, they can quickly discover exposed applications and execute a rapid response, such as remediating credentials associated with third-party applications like Single Sign-On (SSO), code repositories, payroll systems, VPNs, or remote access portals.

Educating employees about the risks associated with using personal devices for work can also help reduce the likelihood of infections occurring.

3. Use Automation to Speed Up Detection and Mitigation

We know cybercriminals leverage automation, but as they get faster, so can we. By leveraging automated remediation from alerts and incident notifications for new breaches and malware infections, SOC teams can more quickly operationalize data and feed it into automated remediation workflows to negate its impact.

Enterprises should consider the following strategies:

- Set up automated alerts for when the organization's credentials appear in data leaks and integrate findings with a SIEM for proactive monitoring, ticket generation, and resets.
- Create automated workflows to notify users when their credentials are compromised and guide them through remediation actions.
- Schedule automated scans of the dark web to compare user credentials against compromised accounts.
- Develop automated playbooks for incident response, including a more robust post-infection remediation that outlines the comprehensive steps needed to take when credentials are found.

- Set up a centralized dashboard to track metrics related to compromised credentials so SOC teams can quickly assess the situation and respond effectively.

The Identity-Centric Approach

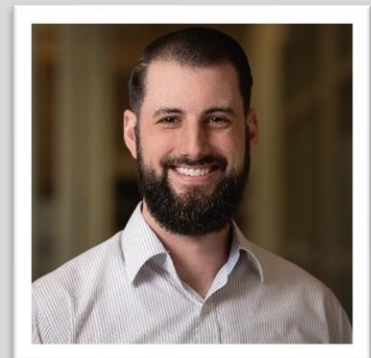
As ransomware attacks evolve and cybercriminals increasingly rely on next-generation tactics, organizations must shift to next-generation defense.

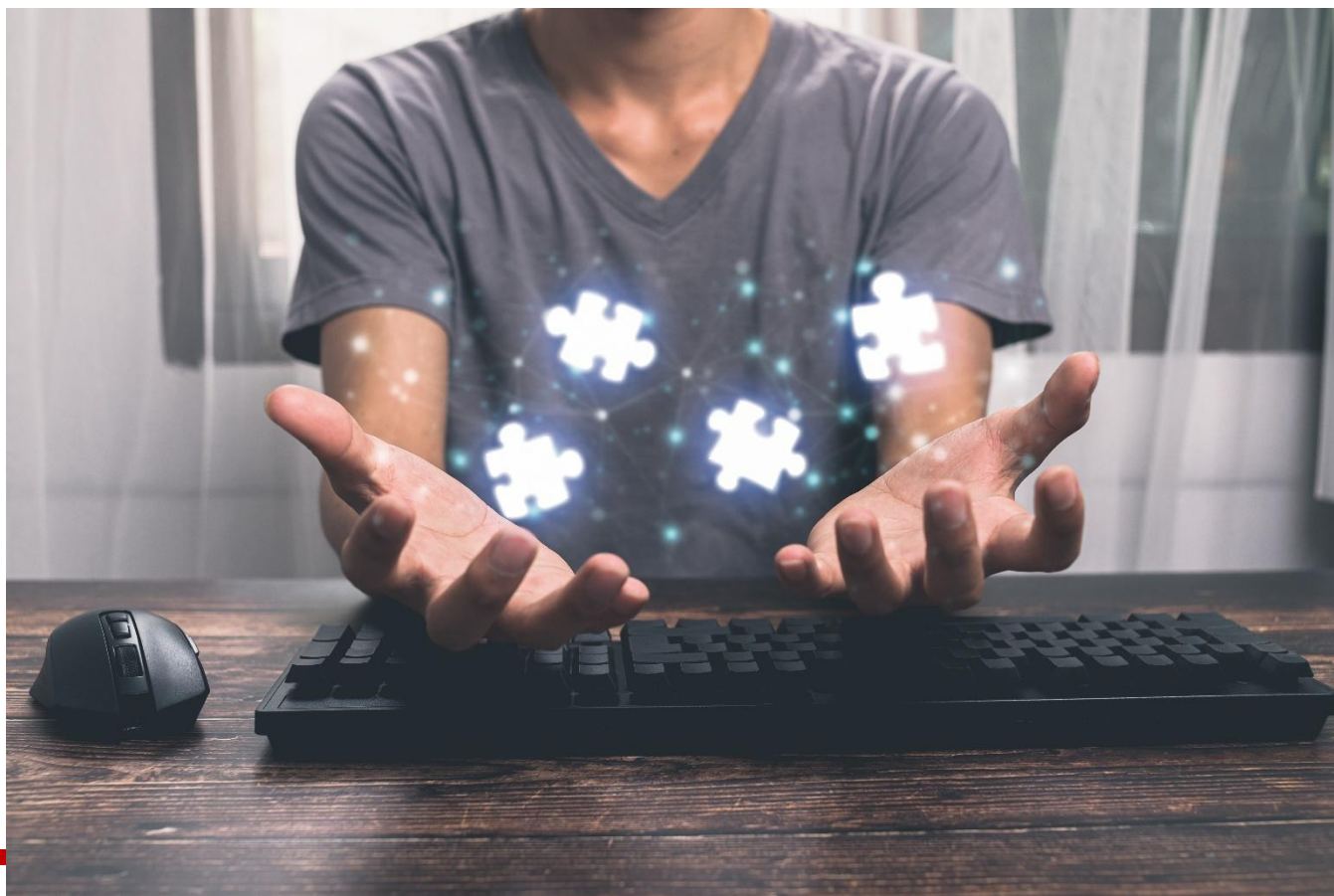
Traditional methods of dealing with malware are not enough to stop cybercriminals from using exfiltrated data, leaving organizations vulnerable to prolonged risks. To effectively disrupt ransomware attacks, security teams and fraud prevention counterparts must adopt an identity-centric approach. By doing so, they can better mitigate the impact of ransomware and protect valuable data from falling into the wrong hands.

About the Author

Trevor Hilligoss is the Senior Vice President of [SpyCloud Labs](#), SpyCloud's in-house security research team. He served nine years in the U.S. Army and has an extensive background in federal law enforcement, tracking threat actors for both the DoD and FBI. He serves in an advisory capacity for multiple cybersecurity-focused non-profits. He has spoken at numerous US and international cyber conferences, holds multiple federal and industry certifications in the field of cybersecurity, and is a recipient of the President's Volunteer Service Award for volunteer service aimed at countering cyber threats.

Trevor can be reached online at trevor.hilligoss@spycloud.com.





How To Strengthen the Security of Your Symfony-Based Solution

By Roman Davydov, Technology Observer, Itransition

Like all web-based solutions, applications built with Symfony are exposed to various cyber threats, and you should be ready to address them to make your website or app secure. After all, if hackers are able to gain access to your corporate and user data through your Symfony solution, you risk losing business reputation, which is extremely challenging to recover.

In this article, [Symfony experts](#) from Itransition highlight the common security threats for Symfony-based solutions and provide three tips to help you mitigate them.

What threats pose a risk for your Symfony solution?

The cyber risk landscape constantly expands, with new threats emerging almost daily. Here are the main types of threats that Symfony solutions are exposed to:

- **Cross-site scripting (XSS)**

XSS attacks enable hackers to inject malicious scripts into the pages of Symfony websites or apps. When a user visits such an infected webpage, he or she becomes exposed to malicious code, which enables attackers to steal their login credentials or get access to a user's device. In [its 2024 report](#), Edgescan rated XSS a critical security threat and revealed that an average XSS attack requires 100 man-days for remediation.

- **Cross-site request forgery (CSRF)**

During a CSRF attack, an attacker tricks a user into submitting a malicious web request to a Symfony website or app in order to perform some unwanted action unintentionally, such as changing a password, making a purchase, or altering other users' permissions. In 2023, MITRE Corporation [had ranked](#) CSRF as the 9th most dangerous software security risk, but just a year later it moved CSRF up to the 4th position.

- **SQL injections**

SQL injection is another hacker attack technique, which can be used by a malefactor to penetrate a website or app database. According to MONITORAPP, SQL injection is one of the most common types of hacker attacks – the company [has detected](#) over 3,800,000 attacks in December 2024 alone.

Obviously, you should not consider this list as ultimate, as there are other types of threats, with server-side template injections and host header attacks among the examples. To learn more about the risks that can compromise the security of your particular web solution, consider consulting with Symfony experts.

How can you protect a Symfony solution from cyber threats?

There is no one-size-fits-all approach to securing Symfony solutions, which means you should implement a set of practices to minimize the risk of a successful attack.

- **Leveraging Symfony's in-built security solutions**

The Symfony framework offers several components and tools that your team members can use to ensure the security of your solution. Symfony's Security Component, for instance, can be used to establish a full-fledged security system for your company's web software. The Security Component is divided into several smaller subcomponents, each serving a specific purpose.

Some of these subcomponents allow teams to quickly implement common security mechanisms in the solution, from authentication and authorization to password encoding. Others can be used to secure different parts of the app via firewalls and build a "line of defense" against XSS attacks. There are also subcomponents enabling teams to implement anti-CSRF tokens to prevent CSRF attacks.

While teams can use these and other Symfony's in-built security components and tools separately, we recommend implementing them in conjunction. This way, your team can quickly ensure all-round robust security for your Symfony-based solution and prevent the majority of cyber attacks.

- **Complementing your Symfony stack with third-party tools**

Although Symfony provides a robust security toolset by default, teams can complement it with third-party tooling resources to get access to additional security functionalities and further strengthen the defense mechanisms of their websites and apps. All your team has to do is to install one of the publicly available Symfony security bundles (no fees required, they are distributed free of charge), install the bundle, and configure it.

Some of these bundles, such as `SchebTwoFactorBundle`, can provide two-factor authentication for your Symfony websites and apps, which can help you establish an additional layer of protection against unauthorized access. Others, such as `Symfony Health Check Bundle`, can assist teams with identifying performance issues across their systems and detecting security vulnerabilities timely.

There are also bundles, such as `SpecShaper Encrypt Bundle` or `DoctrineEncryptBundle`, enabling teams to implement data encryption in their Symfony applications to protect sensitive user data (names, addresses, etc.) from malicious use in case hackers gain access to it. In the event of a successful attack, these free bundles can save you millions of dollars in costs, as, according to IBM's [report](#), the average cost of a data breach has grown up to \$4.88 million in 2024.

- **Conducting security audits regularly**

Among other things, you should remember that maintaining Symfony app security is a continuous process rather than a one-time event. Thus, you should constantly evaluate your solution in terms of cyber risks and threats to ensure that it can withstand both known and new types of threats. In this context, conducting comprehensive security audits at least twice a year is critical.

Before conducting such an audit, your team should study with the current landscape of web cyber threats specific to your industry and business niche. Then, they need to conduct comprehensive security testing, including the review of the solution's architecture, underlying code, software dependencies, etc. to determine whether it can withstand these threats. If the audit reveals any software bugs or vulnerabilities, your team should implement specific measures to mitigate them.

Final thoughts

If you are planning to follow the examples of Spotify, Google, and other companies and develop your own Symfony solution, make sure to protect it from various cyber threats. Otherwise, you risk compromising corporate and user data, which can cause business disruption, reputational losses, and other severe consequences. By following the practices listed in this article, you can significantly strengthen the security of your Symfony-based solution.

Nonetheless, we recommend additionally consulting Symfony experts about app security enablement, especially if your in-house team is not experienced enough. Third-party experts can share more specific, valuable practices to help you maximize your solution's security. If needed, they can also help you build a secure Symfony solution by assisting your team with software design, coding, testing, and other tasks.

About the Author

Roman Davydov is the Technology Observer at Itransition. He has over five years of experience in the IT industry. Roman monitors and analyzes the latest technology trends, helping businesses make informed software decisions that align with their strategic goals. Roman can be reached online at r.davydov@ittransition.com, LinkedIn, and at our company website <https://www.ittransition.com/>





How to Use Risk Management to Strengthen Business Cybersecurity

By Taylor McKnight, Digital PR Specialist for CLDigital

Cybersecurity is a massive point of emphasis for most businesses in the modern age. You must work diligently to protect your company from hackers, scams, phishing emails, and data loss. However, it can be difficult to know where to start, what to do, and how to help your team stay abreast of the current landscape.

Using these pointers, you can create a [risk management](#) plan that focuses entirely on cybersecurity. While you may not know the outcome, starting with a company-wide plan is always a best practice.

How Does Risk Management Dovetail with Cybersecurity?

Any business should have a corporate risk management plan that goes beyond cybersecurity. You must address insurance, profits and losses, workplace injuries, vehicle management, financial security, and online security all at once.

Therefore, your cybersecurity structure should have already been addressed as you built that risk management plan. However, it can be simple to hire an accountant, set up emails that filter junk mail, and prevent unauthorized persons from entering the facility. Plus, you can easily purchase insurance policies that back up your business in a number of areas.

You can even purchase cyber insurance that will pay out claims on a variety of losses, but how do you prevent those losses from occurring?

You must generate a complete cybersecurity plan that takes into account every device and employee. Take a look at how these plans are set up and what should be done to support the mission

How Does Cyber Security Work?

Because risk management and cybersecurity operate in the same arena, you should be just as aggressive with cybersecurity as you would be with workplace safety or financial security. You can take several steps, including:

- Purchase the aforementioned cyber insurance to protect your business
- Hire an outside firm to manage simple cybersecurity training modules
- Set up security alerts that go to all stakeholders
- Remind your staff to avoid all suspicious persons on the premises and report them to security
- Regularly audit your systems to ensure that they have not been breached
- Hire a full-time CIO or information specialist who can support this cause

With each step in this process, you are educating your team and locking down your facility for the betterment of everyone. Remember, hackers can even sit in the lobby and use your public wifi to hack your systems, which is something many business owners simply do not realize. Therefore, diligence is key.

Cybersecurity Awareness

Cybersecurity awareness is a major point of contention for businesses and their employees. Your staff doesn't want to be told time and again that they could be hacked, but you know that everyone gets complacent if they are not reminded on a routine basis.

Therefore, you should routinely cover three major items:

- Report all suspicious emails, do not open them, and move them to the trash folder
- Never let anyone without an ID into the building
- Never leave your workstation open if you are not present

With these simple tips, you can help your staff do most of the loss prevention on their own. Plus, empowering your team with these simple tips will help them remain safe when they leave the office.

Enhance Your Cybersecurity Measures Today

Your business is always under attack—even when you cannot see it. Using the information listed above, you can prepare your staff for the assault of information and scams that will come their way. Plus, you can rest easy knowing that training and cybersecurity tools are available for business owners such as yourself. This small investment of time and energy will help protect your private information, website, customers, and bottom line.

About the Author

Taylor McKnight is a Digital PR Specialist representing CLDigital. When not working I enjoy learning of social media trends and current events. Taylor McKnight can be reached at his LinkedIn profile: <https://www.linkedin.com/in/taylor-mcknight/>.





Implementing Effective AI Guardrails: A Cybersecurity Framework

Securing AI Systems Without Sacrificing User Experience or Innovation

By [Sourabh Satish](#), Co-Founder & CTO of [Pangea](#)

As organizations race to implement AI solutions, security leaders face the challenge of enabling progress while protecting sensitive data. [Grand Canyon Education \(GCE\)](#), which serves 22 university partners, recently confronted this exact dilemma when deploying an AI chatbot platform for thousands of students and staff.

We spoke with Sourabh Satish, a cybersecurity veteran with over 25 years of experience and more than 260 issued patents, about the lessons learned from this implementation and how similar approaches can benefit organizations across sectors. [Drawing from GCE's experience](#) and his extensive background in security architecture, Sourabh shares a framework for securing AI without stifling growth.

What are the unique challenges organizations face when implementing AI?

Organizations, especially those in education, healthcare and finance face a fundamental security paradox. They need to be open enough to foster innovation while simultaneously protecting highly sensitive data, including records protected by FERPA, HIPAA and others.

When organizations implement AI solutions, they're essentially creating new data pathways that weren't accounted for in traditional security models. GCE encountered this firsthand when implementing their AI chatbot platform for university students and faculty. Their security team recognized early on that users might inadvertently share personally identifiable information or sensitive health data that could potentially be stored in backend systems or used to train future models.

The challenge becomes even more complex because these institutions often operate with limited security resources but face sophisticated threats. They need security solutions that can scale across thousands of users without hindering the user experience or technological advancement.

What security risks should CISOs in education and other sensitive industries be most concerned about when deploying AI?

The primary concern is what I call "unintentional data leakage" – when users share sensitive information with an AI system without realizing the downstream implications. Unlike traditional applications where data pathways are well-defined, AI systems can be black boxes that ingest, process and potentially store information in ways that aren't immediately transparent.

There's also the risk of prompt injection attacks, where malicious actors might try to trick AI systems into revealing information they shouldn't have access to. And we can't forget about the possibility of AI systems generating harmful or misleading content if not properly secured.

Organizations need to think about securing both the input to these AI systems – what users are sharing – and the output – what the AI is generating in response.

How can institutions balance security with the need for technology adoption and accessibility?

A reflexive security response might be to lock everything down, but that approach simply doesn't work. If security becomes too restrictive, users will find workarounds – they'll use unsanctioned consumer AI tools instead, creating an even bigger shadow IT problem.

The key is implementing what I call "frictionless security" – protection mechanisms that work in the background without users even knowing they're there. Think of it as an invisible safety net that catches sensitive data before it reaches external AI models but doesn't impede legitimate uses.

API-driven security approaches work particularly well here. Rather than restricting AI adoption, organizations can implement security solutions that automatically redact sensitive information from user prompts and uploaded files in real-time before they reach external AI models. As Mike Manrod, CISO at GCE explains: "What Pangea has allowed us to do is to intercept and apply logic to those prompts. If the

prompt violates a data rule for something we don't want going to an API like OpenAI or Anthropic, we apply redaction at machine speed, without any user impact or user experience change."

It's also crucial to adopt a risk-based approach. Not all AI interactions carry the same level of risk. A student asking about cafeteria hours doesn't need the same security controls as a faculty member uploading research data.

What technical capabilities should security teams look for when securing AI implementations?

Security teams need several key capabilities when implementing AI security guardrails.

Content redaction in real-time is foundational – technology must identify and remove sensitive information from prompts before they reach external AI models. An effective solution should recognize various data types like student IDs, health information, financial details and other PII without introducing noticeable delays.

Further, file sanitization capabilities become essential as more AI systems accept document uploads. The security layer needs to scan and clean documents of sensitive metadata and content before processing, preventing data leakage through attached files. GCE built their security approach around this principle, seeking guardrails that could handle both conversational text and document uploads to their AI platform.

Customizable policy controls allow security teams to define what constitutes sensitive information in their specific context. This is crucial because organizations often have unique identifiers and data structures that generic solutions might miss.

Performance cannot be compromised – any security layer should add minimal latency to maintain a seamless user experience. When security introduces noticeable delays, user adoption inevitably suffers and creates incentives for workarounds. For GCE, this performance requirement was essential as they needed to deploy quickly without introducing latency that could affect student and faculty experiences.

Comprehensive logging and visibility round out these requirements, providing the audit trails needed for compliance. Security teams need clear insights into what types of sensitive information are being caught and redacted, without necessarily exposing the sensitive data itself.

What are the basics of a secure AI framework?

I recommend a four-phase approach:

Assessment: Begin by cataloging what AI systems are already in use, including shadow IT. Understand what data flows through these systems and where the sensitive information resides.

Policy Development: Create clear policies about what types of information should never be shared with AI systems and what safeguards need to be in place. Get buy-in from academic, administrative and executive stakeholders.

Technical Implementation: Deploy appropriate security controls based on risk. This might include API-based redaction services, authentication mechanisms and monitoring tools. The GCE security team initially considered building their own redaction solution but quickly realized this would significantly delay their AI initiative. Instead, they identified an API-based solution that could be implemented quickly while meeting their security requirements.

Education and Awareness: Perhaps most importantly, educate users about AI security. Help them understand what information is appropriate to share and how to use AI systems safely.

Start with high-risk use cases – perhaps those handling sensitive records or research data – and expand from there. Remember that this is an iterative process; as AI capabilities evolve, so too must security measures. The most successful implementations come from close collaboration between security teams, developers and stakeholders who can work together to achieve the desired outcomes.

Looking ahead, what emerging AI security challenges should organizations prepare for?

We're entering a fascinating period where AI is becoming increasingly embedded in nearly every process. Several challenges are emerging:

First, the line between generative AI and traditional applications is blurring. AI features are being integrated into everything from information systems to learning management platforms. This means security can't be bolted on as an afterthought – it needs to be woven into the fabric of these applications.

Second, multimodal AI that processes images, audio and video creates new security dimensions. Organizations will need to think about how to protect sensitive information in these formats as well.

Third, the regulatory landscape around AI is rapidly evolving. Organizations should prepare for new compliance requirements specifically addressing AI usage and data protection.

Finally, there's the challenge of AI alignment – ensuring that AI systems act in accordance with organizational values and objectives. This goes beyond traditional security but is equally important for maintaining trust.

GCE's implementation shows how API-driven, SaaS microservice architecture provides the flexibility to adapt security policies over time as AI platforms evolve. Their team appreciated that with this approach, making redaction policy changes doesn't require developer sprint cycles – security teams can update policies directly through a management console, significantly reducing the time needed to implement security changes.

The organizations that will thrive in this new landscape are those that view AI security not as a barrier to advancement but as an enabler – a foundation that allows them to deploy AI confidently and responsibly.

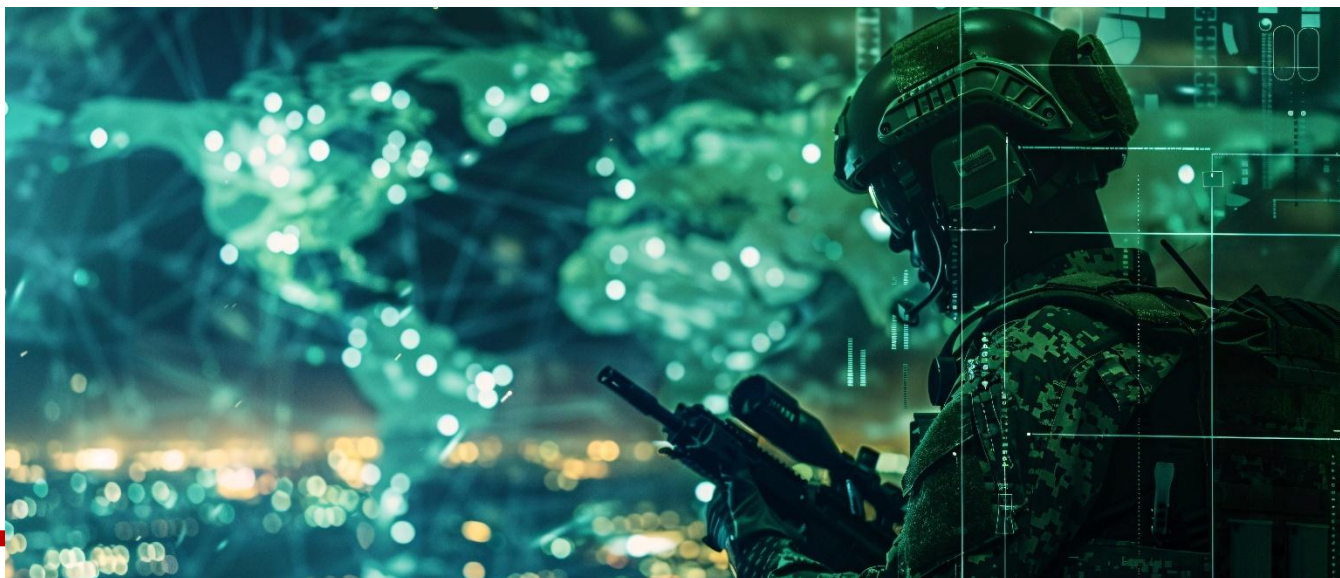
About the Author

Sourabh Satish is CTO and Co-Founder of Pangea and a serial entrepreneur with a 25+ year track record of designing and building ground-breaking security products and technologies, with more than 260 issued patents and additional patents pending. Sourabh most recently founded and served as CTO of Phantom Cyber, which was acquired by Splunk in 2018 and he previously served as a Distinguished Engineer at Symantec.

Read the full case study with Grand Canyon Education here: <https://pangea.cloud/case-studies/grand-canyon-education/>

Sourabh can be reached on [LinkedIn](#) and at <https://pangea.cloud/>





Scaling Smart: Federal Leaders Prioritize AI Security and Resilience

By MeriTalk Staff

The biggest threat to artificial intelligence (AI) in government isn't hype – it's inertia. As Federal agencies explore opportunities to integrate AI into mission operations and citizen service functions (alongside efforts to improve efficiency and reduce costs), they face roadblocks: leadership gaps, legacy infrastructure, and cybersecurity risk management bottlenecks.

A new study from MeriTalk, [Tech Tonic: 2025 Federal CAIO Outlook](#), highlights a widening gap between ambition and execution. While AI use cases across government have doubled in the past year, many agencies are still stuck in pilot mode – hamstrung by limited authority, underfunded initiatives, and a narrow focus on governance. For cybersecurity leaders, that gap represents more than a missed opportunity. It's a growing risk vector that demands increased attention as AI initiatives move forward.

“AI presents a transformative opportunity for government to lead with resilience and innovation by incorporating security at every stage. For effective adoption of AI in cyber operations, we must stay ahead of increasingly sophisticated cyber threats. Thus, it is imperative that pilots move to production so that challenges with operationalizing AI are addressed swiftly and proactively. Meanwhile, by empowering CAIOs, investing in powerful infrastructure, and taking a security-first approach, agencies can scale responsibly and deliver real mission impact.” - Dean Koester, Public Sector Vice President, NVIDIA

AI Cyber Risk – and Responsibility – Are Mounting

Federal Chief AI Officers (CAIOs) overwhelmingly agree on the transformative potential of AI – 85% say it will transform agency operations by 2030. But cybersecurity and risk management have become central to the AI conversation: 57% of CAIOs rank implementing security, privacy, and risk management as a top-three priority for 2025.

Additionally, just 29% of CAIOs say they currently have the authority needed to advocate for meaningful change. And 66% report their agency lacks the infrastructure, talent, and funding to meet AI goals.

These shortfalls can significantly impact cyber posture. Unsecured models, unvetted tools, and fragmented governance all increase the surface area for attack. With more AI tools in play, the risk isn't abstract – it's operational.

Growing Governance Alongside Execution

CAIOs report strong internal backing for AI governance and compliance – currently their most supported initiative area. But support drops off sharply for more strategic needs. Scaling infrastructure and computing, expanding AI talent, and strengthening interagency collaboration all rank as some of the lowest on the leadership support scale – even though they're critical for secure implementation.

The takeaway is clear: governance isn't just red tape – it's the roadmap. But without infrastructure and talent to execute, that roadmap leads nowhere.

Security Starts with Authority

The report highlights a leadership paradox: while 88% of CAIOs hold multiple titles, 100% say the CAIO role should be full-time and stand-alone. Lack of structural authority is slowing progress – and cybersecurity is caught in the fallout.

Agencies operating in compliance-first mode may appear risk-aware, but there are blind spots – pilot tools that aren't hardened, AI services without defined ownership, and models that operate outside enterprise visibility. As AI use grows, so does the risk of unmanaged endpoints and shadow AI.

Scaling AI Without Breaking Trust

Agencies that have started scaling AI are seeing results. But these scaling efforts should include foundational cybersecurity planning, from the onset – and as use cases increase in complexity.

Integration with legacy systems remains a major challenge, with 50% of CAIOs citing it as a top barrier. That's a critical inflection point: every legacy interface added to an AI implementation increases the likelihood of vulnerability. And as data quality and accessibility issues persist – identified by 67% of CAIOs – AI tools may be built on shaky ground, further compounding cybersecurity concerns.

"Embedding security into AI from the beginning isn't optional; it's the foundation for resilient and transformational outcomes. For federal agencies to scale AI responsibly, robust, scalable infrastructure and proactive security measures must go hand in hand. At Dell, we've witnessed how public-private collaboration can bridge the gap between AI's promise and secure implementation, unlocking value while mitigating risk. By prioritizing data quality and protection, accessibility, and integrated safeguards, we can build resilient AI systems that empower governments to lead with confidence, trust, and a commitment to delivering meaningful impact." – Bobbie Stempfley, Vice President and Business Unit Security Officer, Dell Technologies

Action Items for Cyber Leaders

The road to secure, scalable AI isn't just a technology problem, it's an organizational one. To move forward safely, cybersecurity and IT leaders can take steps including:

- **Assert joint ownership of AI security architecture.** Integrate CAIO efforts with enterprise security teams from day one – not after a tool is deployed
- **Advance zero trust principles into AI deployments.** AI tools must meet the same access control, segmentation, and continuous verification standards as other digital assets
- **Push for infrastructure modernization as a security imperative.** Cyber risk multiplies when outdated systems are forced to host next-gen tools. Modernizing backend environments isn't just about performance – it's about protection
- **Invest in AI-specific workforce training.** Threat modeling, red teaming, and AI system auditing require specialized skills that most cyber teams don't yet have
- **Close governance gaps with transparent workflows.** Use standardized pipelines and approval gates for AI tool development, deployment, and updates

The AI opportunity is real. Hardened infrastructure and security-first execution will deliver against this once-in-a-generation opportunity and deliver real mission impact.

Read MeriTalk's full [2025 Tech Tonic: Federal CAIO Forecast](#)

About the Author

The voice of tomorrow's government today, MeriTalk is government IT's top digital platform. Our award-winning editorial team and world-class events and research staff produce unmatched news, analysis, and insight. The goal: more efficient, responsive, and citizen-centric government. MeriTalk connects with an audience of 160,000 Federal community contacts. For more information, visit www.meritalk.com or follow us on X, @MeriTalk. MeriTalk is a [300Brand](#) organization.





Modernizing Critical Infrastructure Security to Meet Today's Threats

By John Kindervag, Chief Evangelist and Creator of Zero Trust, Illumio

Ransomware attacks are no longer just a cybersecurity concern – they are a direct threat to national security. A [recent study](#) found that among organizations hit by ransomware in the past 12 months, an average of 25 percent of critical systems were affected, with downtime lasting an average of 12 hours. The Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the Multi-State Information Sharing and Analysis Center have sounded this alarm and recently issued a [joint cybersecurity advisory](#), warning that ransomware groups are exploiting vulnerabilities in aging systems, including in the critical infrastructure sector.

Such attacks don't just threaten individual agencies – they pose a serious national security risk by targeting essential services used by everyday citizens, including energy grids, healthcare systems, water treatment facilities, and transportation networks.

As Rear Adm. Mark Montgomery (Ret.) a retired navy admiral [recently said](#), “the state and local cybersecurity officials are the front line – they ought to be treated like the front line. [...] Cybersecurity soldiers are on the front line defending our water power utilities, our state and local databases, judicial information.” This means acknowledging the potential for cyber warfare and putting a proactive and modern security strategy in place that effectively defends critical infrastructure.

Traditional cybersecurity approaches fall short against modern and sophisticated threats because legacy systems often lack fundamental security controls. Many were not designed with today's cyber risks in mind, leaving agencies and critical infrastructure owners with limited visibility, weak access controls, and flat network architectures that allow attackers to move laterally with ease. Without segmentation, containment, and advanced threat detection, agencies struggle to identify and mitigate attacks before they disrupt operations or compromise sensitive data. To defend against evolving threats, agencies must shift to a model that enforces continuous verification and least-privilege access to limit an attack's impact.

Moving Away from Outdated Security Practices

Traditional models lack the visibility needed for effective risk detection and response, creating dangerous blind spots. While internet-connected systems enhance defense and stability, they also give nation state actors new attack opportunities, putting sensitive data and critical services at risk.

The security approach Zero Trust addresses modern cyber threats by preventing attackers from gaining access they need to succeed. No matter how advanced their tools are, cybercriminals can't breach what they're not allowed to reach. Operating on the principle of "never trust, always verify," Zero Trust eliminates blind spots by enforcing continuous verification and least-privilege access, ensuring that even if attackers find a way in, they can't move laterally or cause widespread damage.

Securing critical infrastructure through Zero Trust requires placing essential computational controls – such as programmable logic controllers (PLCs) and human-machine interfaces (HMI) – within a defined Protect Surface. By building out protections with a five-step Zero Trust model, agencies can effectively secure these high-value assets. First, they must identify the data, applications, assets, and services that require protection. Mapping transaction flows then reveals how these components interact, informing the architecture's design to ensure controls are placed as close as possible to the Protect Surface. Establishing Zero Trust policies then further restricts access to only those who truly need it. Finally, continuous monitoring and telemetry analysis enable real-time threat detection and adaptive security improvements, ensuring that critical infrastructure remains resilient against evolving cyber threats.

Another key component of Zero Trust, Zero Trust Segmentation (ZTS), prevents attackers from moving laterally across networks and reaching high-value assets. By automatically isolating critical systems and containing threats at the source, ZTS not only minimizes the impact of breaches but also accelerates incident response. With ZTS in place, agencies and critical infrastructure owners can quickly contain threats without widespread operational disruptions – enabling mission continuity and operational efficiency even in the face of attacks.

Integrating Advanced Security Measures to Enhance Resilience

Beyond ZTS, agencies and critical infrastructure owners must leverage continuous monitoring and threat intelligence sharing to detect and respond to emerging threats in real time. The integration of artificial intelligence (AI) and automation plays a crucial role in cybersecurity, enabling faster threat detection, predictive analytics, and automated response mechanisms. Within the Zero Trust framework, AI

accelerates key processes such as labeling environments and implementing day-one policies, making security measures more efficient and adaptive. By leveraging AI-driven automation alongside solutions like ZTS, agencies and owners can proactively isolate threats while maintaining seamless operations, strengthening their overall security posture.

Strengthening collaboration efforts is also essential. Critical infrastructure owners and agencies must work closely with the federal government to share intelligence, enhance threat visibility, and develop coordinated defense strategies. By integrating these advanced security measures, agencies can build adaptive, resilient defenses that protect vital assets and maintain national security.

By modernizing security strategies and adopting proactive measures, critical infrastructure owners can reduce operational risk, limit the impact of cyber intrusions, and strengthen national security.

Balancing Security with Operational Continuity

Striking the right balance requires a security strategy that enhances protection without introducing inefficiencies or disrupting mission-critical functions. This means adopting solutions, like ZTS, that integrate with existing infrastructure to help isolate threats while allowing normal operations to continue. Agencies must also take a phased approach to modernization, testing and implementing security upgrades incrementally to minimize operational disruptions and ensure efficiency. Additionally, cybersecurity measures should be tailored to specific operational needs – rather than applying one-size-fits-all solutions.

Meeting Today's Threats and Charging Forward

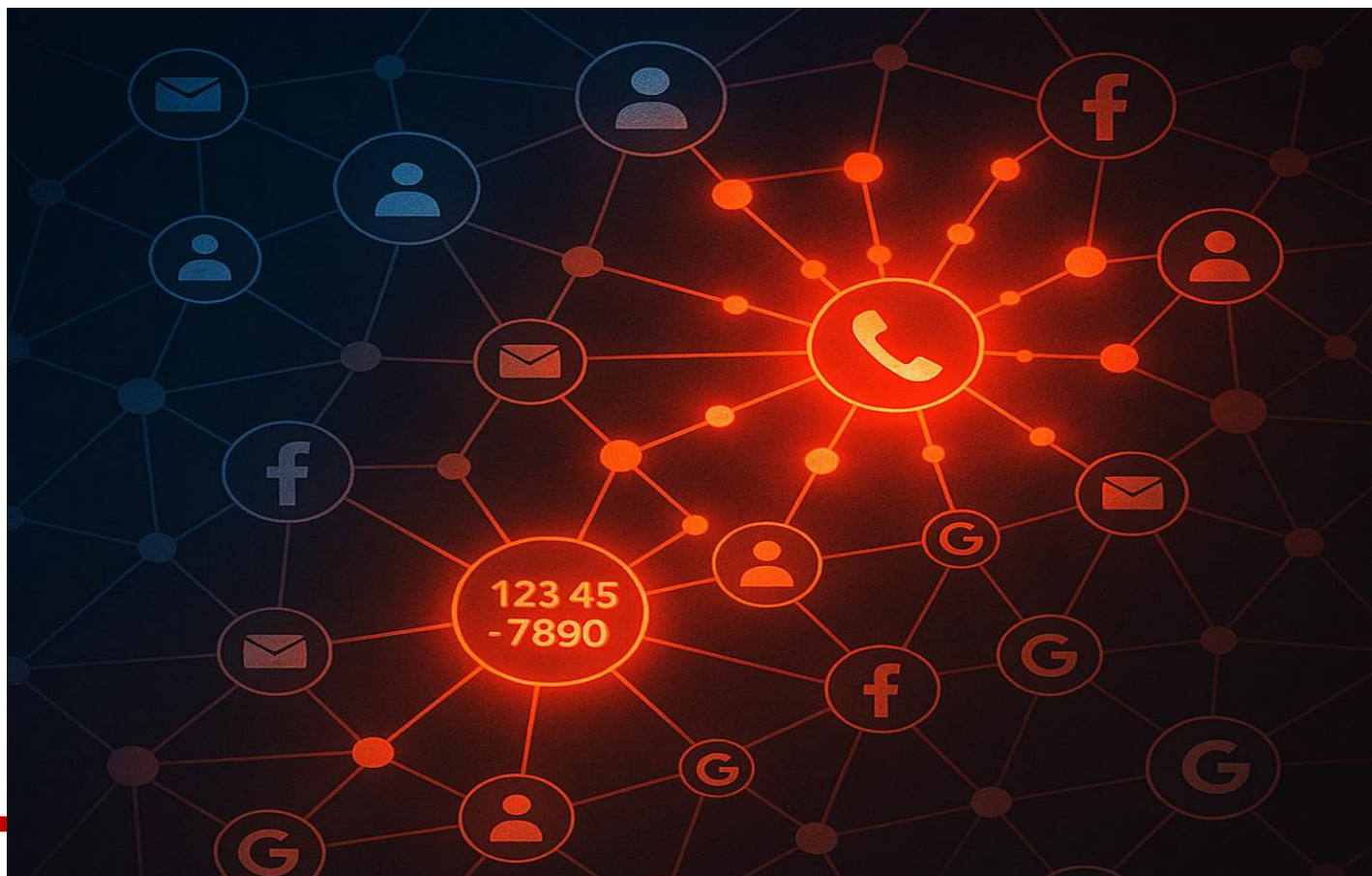
As cyber threats continue to evolve, securing critical infrastructure demands a proactive and modernized approach. Critical infrastructure owners can no longer rely on outdated security models that leave vital systems vulnerable to ransomware and other attacks and ultimately create an environment that stalls efficiency.

By adopting Zero Trust principles and implementing ZTS, agencies and critical infrastructure owners can significantly reduce risks and strengthen national security. Balancing these measures with operational continuity ensures that security enhancements do not compromise essential services. Through strategic modernization, agencies can build resilient defenses that safeguard the nation's most essential assets.

About the Author

John Kindervag is considered one of the world's foremost cybersecurity experts. With over 25 years of experience as a practitioner and industry analyst, he is best known for creating the revolutionary Zero Trust Model of Cybersecurity. As Chief Evangelist at Illumio, John Kindervag is responsible for accelerating awareness and adoption of Zero Trust Segmentation. Most recently, John led cybersecurity strategy as a Senior Vice President at On2IT. He previously served as Field CTO at Palo Alto Networks and, before that, spent over eight years as a Vice President and Principal Analyst on the security and risk team at Forrester Research. In 2021, John was named to the President's National Security Telecommunications Advisory Committee (NSTAC) Zero Trust Sub-Committee and was a primary author of the NSATC Zero Trust report that was delivered to the President. That same year, he was also named CISO Magazine's Cybersecurity Person of the Year. John serves as an advisor to several organizations, including the Cloud Security Alliance and Venture Capital firm NightDragon.





One Piece of the Puzzle: How a Single Digital Identifier Can Unravel Your Entire Online Life

The Hidden Risks of Reusing Emails and Phone Numbers—and How They Become Gateways to Your Entire Digital Identity

By Raphael Marchand, CEO, ChatOdyssey

One Piece of the Puzzle: How a Single Digital Identifier Can Unravel Your Entire Online Life

In an era where our lives are increasingly lived online, our digital identities are sprawling networks of accounts and personal data. A simple email address or phone number—often considered a secondary identifier—can serve as the key to this entire web of information. Privacy advocates warn that if an attacker or unauthorized person discovers just one of these identifiers, it could trigger a chain reaction, exposing a trove of connected accounts and sensitive details. This article explores how a single digital identity marker (like your phone number) can unravel your whole online presence, the cybersecurity implications of this vulnerability, and what can be done to mitigate the risks.

Secondary Identifiers: The Overlooked Keys to Your Digital Identity

Modern online services commonly use email addresses and phone numbers as unique identifiers for user accounts. They function as convenient usernames or verification tools—but this convenience comes at a cost. Because people tend to reuse the same email and phone number across many platforms, these identifiers become an interlinking thread tying all their accounts together. In fact, the average internet user today has roughly 240 online accounts that require a password, yet often only a couple of email addresses (or just one) to manage them. This means one email inbox is the gateway to hundreds of services. If that email or a linked phone number is exposed, it essentially provides half the puzzle to an attacker for every other account (it reveals the username for those accounts).

Phone numbers play a similar role. Many apps and platforms request your phone number for account creation, two-factor authentication, or social connectivity. Over time, your primary number may be associated with banking apps, messaging services, social networks, and more. It's an open secret that phone numbers are widely used as a lookup key: if someone knows your number, they can often find your profile on social media or messaging apps (unless you've adjusted privacy settings). By default, some platforms even allow this kind of discoverability. For example, until recently, services like Twitter let anyone find an account by phone or email by default (except in jurisdictions like the EU that require opt-in). The result is that a single phone number or email address can unlock access to a wealth of information about an individual.

Fact: Investigators and malicious actors alike use OSINT (Open Source Intelligence) tools to leverage these secondary identifiers. A phone number can serve as a gateway to an individual's online activities, revealing linked social media profiles, associated usernames, and even data breaches tied to that number.

Most users underestimate how much of their digital footprint is tied to just one or two identifiers. A recent security analysis found that only about 0.03% of breached accounts in circulation used any form of email alias – indicating that almost everyone relies on the same real email for multiple services. Likewise, few people use secondary or “burner” phone numbers for everyday accounts. This consolidation means our secondary identifiers have effectively become master keys to our digital identities.

One Exposed Identifier Can Unravel the Whole Web

It only takes one exposed node in the network of your digital identity for a determined party to start pulling on the thread. If a hacker, scammer, or even a curious researcher learns just one of your identifiers (say your primary email or cell number), they can begin mapping out your entire online presence. This chain reaction often unfolds in a few ways:

- **Data Breaches & Leaks:** If your email or phone number appears in a data breach, it often comes bundled with other personal info. The 2021 leak of 533 million Facebook users' data is a prime example: attackers exploited a flaw and scraped phone numbers linked to profiles, exposing names, locations, and more. Similarly, an API vulnerability in Twitter allowed malicious actors to submit an email or phone number and learn the associated account name, affecting 5.4 million users. In both cases, a single piece of contact info became the index to a larger profile.

- **Social Media and OSINT Lookup:** Many social platforms and apps let users find friends by phone or email. Attackers can abuse these features (or their APIs) to discover your accounts. In fact, Twitter disclosed that bots were uploading huge lists of phone numbers just to see which ones hit a match, effectively building a reverse lookup database of users. A phone number plugged into people-search tools or even Google can surface LinkedIn profiles, WhatsApp statuses, Skype IDs, or forum posts. From one account, others often follow—your Instagram might reveal your full name, which leads to a search that uncovers your other profiles, and so on. The web of connected accounts starts to light up one by one.

- **Password Reset and Account Recovery Routes:** An exposed email address opens doors via the password reset function on countless sites. A malicious actor who has your email can attempt to reset passwords on popular services; even if they don't succeed without access to your email inbox or phone, they might learn which sites you use (some services inadvertently disclose whether an email is registered). If they do have your email account (or convince an email provider or phone carrier to help via social engineering), they can snowball into many other accounts by triggering password resets. This domino effect is precisely how a compromised email led attackers to multiple connected accounts in one incident.

- **Cross-Service Identity Linking:** Our digital identifiers are often used beyond login. For example, if you use the same email for an e-commerce account, a social media profile, and a health app, and one of those leaks it, criminals can correlate that email across different dumps or platforms to assemble a richer picture (perhaps linking your email to a real name, physical address, or medical info from separate breaches). They know people recycle personal information across platforms, so finding one identifier in one place can validate that it's the same person elsewhere.

From a privacy advocate's perspective, this interconnectedness is alarming. It means that despite all the passwords and security measures on individual accounts, your online life has a single point of failure: the exposure of a secondary identifier. An opportunistic attacker doesn't need to "hack" 20 different sites to learn about you; they can simply pivot from one exposed ID. In practical terms, this could mean a stalker starting with your cell number and ending up with your home address and family photos, or a scammer starting with your email and discovering where you bank and shop. It's a chain reaction of vulnerability—one link weakens, and the whole chain can come undone.

The Cybersecurity Implications of Linked Identities

The fallout from a single identifier leak can extend far beyond embarrassment or nuisance; it raises serious cybersecurity threats for individuals and organizations alike:

- **Targeted Phishing and Scams:** Once attackers know which services you use (because they discovered your linked accounts), they can craft convincing phishing emails or texts. For instance, if they uncover that you have an account at a particular bank or an online store, they can send you tailor-made fake alerts appearing to come from those businesses. The success rate of phishing climbs when the attacker has personal context. A trove of leaked phone numbers has already led to surges in SMS phishing ("smishing") attacks impersonating companies that users trust.

- **Credential Stuffing and Account Takeovers:** If an email address is found in a breach, often accompanying it are hashed or even plaintext passwords used on one site. Attackers will try those email/password pairs elsewhere. Even if the passwords are different, knowing your primary email gives them a username to target. Many people reuse passwords or slight variations, making the attacker's job easier. And if they get into one account, they will quickly check your email or profile info for clues to access others, snowballing their access. When threat actors seize one account, they often pivot to more valuable accounts via notifications or contacts found inside.

- **Social Engineering and Impersonation:** With bits of your personal data pieced together (from profiles, signatures in email leaks, etc.), attackers can impersonate you or someone you know. They might call your mobile provider pretending to be you (armed with your name, number, maybe address) and convince them to issue a new SIM card (a SIM swap), hijacking your phone number to intercept verification codes. Or they could impersonate a service rep to you, citing some info as "verification." The more connected data points they have, the more credible they seem. This is how a single clue can bypass security questions or trick support desks into resetting credentials.

- **Privacy Erosion and Doxxing:** Beyond immediate financial harm, there is a personal privacy impact. A determined individual could use one identifier to doxx someone—aggregating public and private info to expose their identity or location. We've seen cases where something as simple as a leaked phone number of a journalist or activist led to their entire online history being dug up and publicized. The psychological toll and safety risk can be severe, especially for those who assumed their various online personas were separate or anonymous until the dots got connected.

It is clear that interlinked digital identities have broadened the attack surface. Security professionals note that users often reuse and recycle personal information across sites, which attackers count on. Even years-old leaked data can be re-purposed in new attacks; nothing truly "expires" once it's public. This is why protecting secondary identifiers is now as crucial as protecting passwords. They are the weakest link in many cases. As one security researcher wryly observed, an email address today is like an index to a person's entire digital file cabinet. If you wouldn't hand a stranger your entire file cabinet, you should be just as wary about that one email or number that unlocks it.

Mitigations: Masking and Managing Your Digital Footprint

The good news is that both individuals and organizations can take steps to break the chain and protect these critical identifiers. A growing movement in cybersecurity and privacy circles advocates for masking or aliasing our digital identifiers to limit exposure. Here are some strategies and best practices to consider:

- **Use Multiple Email Addresses or Aliases:** Don't use one email address for everything. Instead, segregate your identity by purpose (e.g. one email for banking and important accounts, another for social media, another for online shopping). This way, a breach of one won't automatically link to all your other services. You can also use email aliases or forwarding addresses – unique addresses that all deliver to your main inbox. For example, creating an address just for a specific service (like `yourname+someservice@example.com`) can help contain and identify exposure. Privacy experts note that relying on different addresses greatly limits how much of your profile a single leak can expose. In

practice, very few users do this yet (only ~0.03% of breached accounts contained a custom alias, according to one analysis), but it's a highly effective shield.

- [Employ Secondary Phone Numbers](#): Just as you might use multiple emails, consider getting a secondary phone number for less critical uses. This could be a prepaid SIM, a VoIP number, or a number provided through an app or privacy service. Use your primary personal number only for things that truly need it (family, secure accounts, work), and give out a secondary number for everything else (online forms, app signups, etc.). This way, if that secondary number gets spammed, leaked, or compromised, your main phone remains unaffected. Keeping your primary number private is a strong deterrent to mass scraping or random attacks.

- **Limit Discoverability**: Review privacy settings on social networks and other platforms. Turn off the option that lets people find you by your email or phone number, if available. This simple step prevents casual lookup of your accounts by unknown parties. For instance, ensuring the “let others find me by phone/email” setting is off on platforms like Facebook, Twitter, and others puts a roadblock in the way of opportunistic data harvesters. While it won't stop a determined hacker using stolen data, it will stop your neighbor or a stranger with your number from easily pulling up your profile.

- **Practice Data Minimization**: The less you share each identifier, the safer it is. Avoid posting your email or phone in public forums or social media bios. Be cautious when asked for personal contact info—provide it only when necessary and to trusted parties. If a website or app demands a phone number and you're not comfortable, see if you can opt out or use an alternative (like an email or an alias number). Every time you withhold your primary identifiers from yet another database, you shrink the attack surface. As one industry saying goes, what isn't collected can't be leaked.

- **Enhance Account Security**: Since some sharing of identifiers is unavoidable, mitigate the impact of a leak by securing the accounts themselves. Use strong, unique passwords for each account (a password manager can help) so that even if your email is known, an attacker can't guess their way into your accounts. Enable two-factor authentication (2FA) wherever possible — and opt for app-based or hardware 2FA over SMS-based 2FA when you can (to reduce reliance on your phone number for security). This ensures that knowing your email or number isn't enough to breach an account. Also, monitor your accounts for unusual activity and consider using breach notification services (like haveibeenpwned) to get alerts if your email or phone appears in a new data dump.

On a broader level, companies and service providers are starting to acknowledge this problem. Some are implementing features like “Sign in with Apple” or other federated identity systems that hide your email from third-party services by using an email relay. Others offer one-time codes or app-based verification in lieu of always using your phone number. As users, showing that we value these privacy-respecting options (by using them when available) sends a clear message to the industry.

Lastly, if you suspect that one of your identifiers has been exposed or is being misused, take action quickly: change associated passwords, consider retiring that email address or number if feasible, and notify your contacts or relevant institutions if needed. Early containment can prevent an initial exposure from snowballing further.

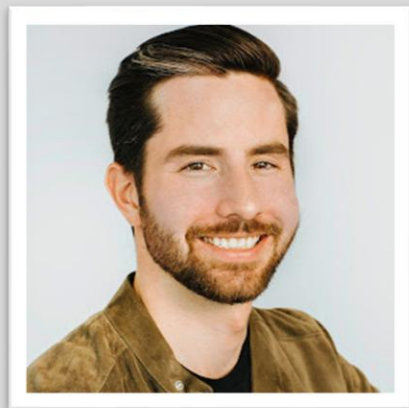
Conclusion: Strengthening the Weak Links

Our digital identities will only continue to expand as we integrate more of our work, finance, and social lives with online services. This makes it ever more important to safeguard the linchpins of those identities—our emails, phone numbers, and other secondary identifiers. What might seem like just a harmless bit of contact info can be the thread that, when pulled, unravels the tapestry of someone's private life. From a cybersecurity standpoint, recognizing this fact is half the battle. The other half is acting on it: employing the tools and best practices that add layers of protection around these identifiers.

In the spirit of a privacy advocate, the message is clear: Don't let a single email address or phone number be your undoing. By fragmenting your digital identity where it makes sense, keeping your personal identifiers close to your chest, and demanding platforms do more to protect these details, you can enjoy the convenience of our connected world without laying out the welcome mat for attackers. In an age of ever-more connected accounts, true security and privacy come from disconnecting the dots that others would so eagerly connect. Stay safe by staying one step ahead – treat your secondary identifiers as seriously as you do your passwords, and you'll drastically reduce the risk of a chain reaction compromise.

About the Author

Raph Marchand is the Founder and CEO of ChatOdyssey, a privacy-focused communication platform offering end-to-end encrypted messaging, email and phone relay masking, and domain-free custom email identity solutions. With over a decade of experience at the intersection of cybersecurity, encrypted communication protocols, and product development, Raph is passionate about building tools that give users control over their digital footprint. His work spans secure app architecture, anti-surveillance systems, and privacy-first user experience design. At ChatOdyssey, his mission is to simplify privacy for everyone by making secure, anonymous communication intuitive and accessible. He can be reached at raph@origins.io Learn more at <https://www.chatodyssey.com>





On Constant Community Improvements

By Maxime Lamothe-Brassard, Founder and CEO, LimaCharlie

The theme of this year's RSAC is "*Many Voices. One Community.*" While our field can rightly claim "many voices", portraying it as a "community" is a bit of a stretch. By this, I mean countless cybersecurity vendors hawking proprietary solutions will be attending RSAC, but they are competitors, not players on a common team. Each vendor wants to capture as much of the cybersecurity market as they can and this economic reality hinders true community building.

To be clear, there is no hard and fast definition of what constitutes a community. The Cambridge dictionary defines community as: *the people living in one particular area or people who are considered as a unit because of their common interests, social group, or nationality*. In its broadest sense, one could argue our *community* has a common interest in cybersecurity. By this same definition, we all belong to the *pro-breathing*, *pro-hydration*, and *pro-sheltering* communities.

Simply put, when the definition of a community includes everyone, the word loses some meaning. My point is not to engage in a pedantic argument over the term *community*. Rather, I plan to demonstrate that where cybersecurity efforts are community-driven, they thrive. Likewise, when cybersecurity is done individually, opaquely, and in isolation, it often flounders.

For example, public and open-source projects such as VirusTotal, Wireshark, Metasploit, and OWASP provide critical resources to our field. Individuals with an interest in cybersecurity support and manage these efforts in a non-competitive way that makes them useful for everyone. By contrast, cybersecurity companies have little motivation to make their solutions play well with competitor's products. This is a

natural consequence of market competition where each vendor wants to sell their branded suite of solutions.

Unfortunately, this proprietary approach leads to massive difficulties when SOC analysts and service providers try to integrate multiple third-party tools into their security stack. Most medium enterprise SOC's use over 50 security tools, and getting them to work together is extremely difficult. Every hour spent troubleshooting, integrating, and engineering workarounds for existing security solutions is time SOC analysts are not focused on detections and response.

Build a Community of Competitors?

There are two primary forces keeping cybersecurity vendors from forming a truly cooperative community. First, vendors need to make money to stay in business, and that puts their individual interests in direct opposition to all competitors in their space. Second, many vendors sell solutions whose effectiveness partially relies on keeping their operational details a secret. These factors alone make building an open community among private cybersecurity organizations highly unlikely.

Instead, we should accept that the competitive nature of business is not going to change. Nor are cybersecurity vendors going to publicly divulge their lucrative secrets for the sake of doing a good deed. In fact, doing so would be like asking a bank to post the blueprint of their vault online. Yes, other businesses might gain security knowledge from studying the vault design, but bank robbers would too.

The downstream effect of this necessary secrecy are SOC's filled with dozens of opaque solutions, requiring large teams of experts to manage. Ironically, many zero trust environments consist of security analysts absolutely trusting countless black-box vendor solutions. While vendor-trust is common for businesses, we regularly see stories of attackers compromising organizations who use the most esteemed security vendors in our market. Last year, we also saw an honest mistake from a large vendor cause the largest IT outage in history. These lessons should remind us that there is a stark difference between securing your organization, and trusting someone else to do so.

The market forces driving secrecy and competition among cybersecurity vendors force many businesses to trust tools they cannot fully audit. However, this does not mean we cannot reap the benefits of fostering a cybersecurity community in other ways. There are resources available today that help third-party security solutions work transparently and cooperatively, even when their patent holders will not.

Community Built by Cloud, APIs, and Automation

The key to realizing the benefits of a *cybersecurity community* relies upon adopting a vendor-neutral cloud platform for centralizing security resources. Such a platform frees your organization from being locked into vendor-specific solutions while also creating a space to integrate your existing security stack. Rather than asking your SOC to wrangle countless third-party tools, you create a cloud-based control center for centralized management of all security resources.

Integrating your security stack via API on a cloud platform greatly simplifies tool use, management, and coordination. Those of you familiar with IT operations will recognize this approach as infrastructure-as-a-service. For cybersecurity, the equivalent of adopting AWS/GCP to manage infrastructure is found in the SecOps Cloud Platform (SCP). Instead of hiring several analysts to monitor dozens of solutions and manage their infrastructure, you retain a few experts to operate a SCP.

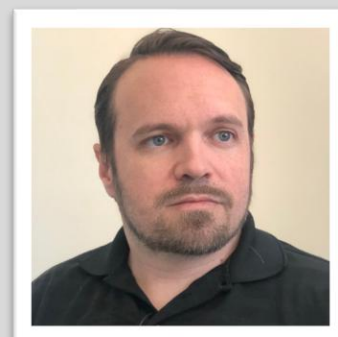
An SCP normalizes data, allowing security tools, services, and telemetry sources to communicate using a common language. Communications happen via API, which fosters rapid information sharing throughout the platform and simplifies automation. For example, if you receive an O365 alert indicating a suspicious login you could have a script immediately disable the account pending further review. Once your security stack is integrated on a common cloud platform you have extreme control over its behavior and operation.

Cloud consolidation does not provide visibility into precisely how private vendors make detections with their black-box solutions. However, you will have full visibility into how your security stack handles information from all sources and control over how it responds to detections. This informative birds-eye view can help you discover redundancies, lapses in coverage, and areas of exposure.

Adopting an SCP frees your team from the drudgery of maintaining cumbersome infrastructure. It consolidates security solutions from the hands of competitive vendors and turns them into cooperative resources focused on a common task. In other words, a SecOps Cloud Platform transforms security resources into a true *cybersecurity community* and reliably delivers the benefits we gain from working together.

About the Author

Maxime Lamothe is the Founder and CEO of LimaCharlie. He is an accomplished computer scientist and information security specialist. As part of the Canadian Intelligence apparatus, Maxime worked in positions ranging from development of cyber defense technologies through Counter Computer Network Exploitation and Counter Intelligence. Maxime led the creation of an advanced cyber security program for the Canadian government and received several Director's awards for his service.



After leaving the government, Maxime provided direct help to private and public organizations in matters of cyber defense and spent some time working with CrowdStrike. For the past few years Maxime has also been providing analysis and guidance to major Canadian media organizations. Maxime was a founding member of Google X's Chronicle Security. He left in 2018 to found LimaCharlie.

Maxime can be reached online at LinkedIn <https://www.linkedin.com/in/maximelb/> and at our company website www.limacharlie.io.



Securing the Connected Factory Floor

By Almog Apirion, CEO and Co-Founder of Cyolo

As manufacturers strive to keep pace with changing demands and quickly evolving technologies, many are embracing digitalization and increased connectivity between information technology (IT) and operational technology (OT) environments. The upsides of this transformation include greater productivity and improved efficiency.

The downside? Unprecedented cybersecurity attacks against cyber-physical systems (CPS).

A recent Telstra survey found that 80% of manufacturing firms experienced increased security incidents in the past year, highlighting the urgent need for more effective OT/CPS security strategies. While IT systems have long been equipped with security controls, cybersecurity is still emerging as a key priority for many industrial enterprises. At the same time, cyber-threats often evolve faster than OT networks can keep up with, creating new vulnerabilities at every turn.

For these reasons, securing OT environments requires a paradigm shift – moving beyond traditional security approaches such as VPNs and perimeter-based defenses to embrace zero-trust security, identity-based access, and real-time monitoring. Critically, this shift must also acknowledge the fundamental difference between detection and protection. While detection mechanisms focus on

identifying threats after they have infiltrated a network, true protection is about preventing unauthorized access in the first place, ensuring that cyber threats are stopped before they can cause harm.

Expanding Cyber Risks

Over the past decade, the manufacturing industry has rapidly integrated IoT devices, robotics, real-time analytics, and cloud-based capabilities into more traditional industrial operations. With these connected systems and devices now at the heart of many factories, the attack surface for cyber-threats is wider than ever.

As IT/OT convergence accelerates, attackers can more easily exploit IT vulnerabilities to infiltrate OT systems. Indeed, increased connectivity and data visibility within the manufacturing ecosystem – all hastened by the recent explosion of digital connectivity – have made it a prime target for cyberattacks. In fact, 2024 was the third consecutive year in which the sector experienced its highest number of attacks, comprising [25%](#) of all hacks globally.

Among the most common OT security blind spots is overreliance on outdated network access solutions. These solutions often require only one set of credentials across numerous access points, resulting in cases where a single set of shared credentials grant a third-party vendor unrestricted access to critical systems. As a result of maliciousness or simple human error, this level of unintended privileged access could lead to catastrophic consequences, far beyond financial loss or reputational damage – consider that a cyber-attack affecting equipment in a manufacturing facility can cause serious physical consequences for workers on the floor.

Challenges in Securing OT Environments

The legacy assets present in many OT environments typically lack built-in authentication or encryption, making them easy targets for cyberattacks. But upgrading legacy systems can be costly and disruptive, leading to patchwork security solutions that create substantial gaps.

The risk posed by legacy infrastructure is compounded by the fact that manufacturers frequently depend on third-party vendors or external contractors for maintenance, software updates, troubleshooting, data storage, and more. Traditional remote access solutions, such as VPNs and jump servers, provide no visibility or control after the initial connection. Unless additional controls are implemented, third-party users who connect via such tools have veritable free rein once they're inside the network. An oft-cited example is the [2021 Colonial Pipeline breach](#), a ransomware attack where hackers gained entry through a compromised VPN password.

Many industrial organizations also struggle to maintain real-time inventories of connected assets, and this issue will only continue to grow if cross-channel monitoring solutions are not put in place. According to a 2024 report from Ponemon Institute and Cyolo, as many as [73% of organizations lack an authoritative OT asset inventory](#). But asset inventories alone are not enough. Once an organization has full visibility into its assets, it must proactively secure them. Knowing what's connected is only half the battle; fortifying

those connections is what truly mitigates risk. Without proper asset visibility and access segmentation, a single compromised credential can provide an attacker with full access to the entire OT network.

Strengthening OT Security

So how can enterprises best mitigate growing risks without compromising on the benefits of digital connectivity?

Start with a zero-trust approach to access management for all users: i.e., implementing identity-based authentication and tightening access protocols so that they are at least as secure and restrictive for contractors and third-party vendors as they are for internal employees. This requires replacing or augmenting traditional VPNs with more advanced remote access solutions and enforcing multi-factor authentication (MFA) across all access points, including legacy OT systems. Too many companies concentrate on securing more modern applications but leave legacy infrastructure unprotected and thus highly vulnerable.

To further strengthen third-party access security, enterprises should require their vendors and third-party integration hosts to authenticate using identity-based access solutions rather than shared credentials or perimeter-based models. Session-based access controls, for instance, can automatically revoke vendor access once a task is completed, reducing the risk of lingering security gaps.

Another critical aspect of robust OT security is Remote Privileged Access Management (RPAM) – a relatively new approach to securing and controlling privileged access to essential systems, data, and resources. By enforcing the highest level of security for

privileged users, such as third-party vendors, remote workers, and anyone accessing mission-critical assets, RPAM solutions punch far above their weight when it comes to mitigating risk. However, when it comes to CPS environments, generic RPAM solutions are not enough. Secure remote privileged access for CPS must be purpose-built to meet the unique needs of these environments, ensuring that real-time industrial processes are protected without disrupting operational continuity.

Leveraging Regulation

Beyond the direct internal benefits of heightened OT security, implementing security best practices will help organizations comply with a growing list of regulations and compliance mandates. Frameworks such as ISA/IEC 62443, ISO 27001, and NIST CSF create a baseline for OT cybersecurity resilience, allowing organizations to maintain compliance while reducing the potential operational downtime caused by cyber-incidents. Many manufacturers still see compliance as a checkbox exercise but in reality, regulatory alignment can make the difference between a minor security event and a full-scale operational crisis.

Finally, there is the *Purdue Model*: an approach to segmenting industrial control systems (ICS) into hierarchical layers. This is done to limit access between IT and OT and, in turn, reduce cyber vulnerabilities. Network segmentation enforces strict access controls, preventing threats from spreading laterally between networks. Each zone of the Purdue Model has its own security considerations, with

greater connectivity being allowed as one moves further from the most critical OT assets. By adhering to the Purdue Model, organizations can reap the benefits of connectivity while minimizing risk.

Don't Save OT Security Until Overtime

The connectivity of modern manufacturing environments has made remote access security a top priority.

Traditional VPNs and perimeter-based defenses are no longer sufficient – manufacturers must instead adopt a proactive OT security approach, defined by zero-trust security, identity-based access and authentication, continuous monitoring and decisive action to secure assets. Only by securing access at every level and ensuring that only the right people with the right credentials can reach critical systems can manufacturers protect their most critical processes, ensure operational resilience, and mitigate costly cyber-threats.

Adopting the right secure remote access tools is about more than just meeting regulations and going through the motions of securing industrial environments – it's about maintaining competitiveness and growth trajectories in a world where a single hack can result in disaster.

About the Author

Almog Apirion is CEO and Co-Founder of Cyolo. He is an experienced technology executive, a "recovering CISO," and the founder of the Israeli Navy Cyber Unit. Almog has a long history of leading the cybersecurity and IT technologies domain, with a background that includes building and securing critical infrastructures at large organizations, and leading teams to success.





Small Manufacturers, Big Target: The Growing Cyber Threat and How to Defend Against It

By Brian Winters, Chief Technology Officer, ECI Software Solutions

Digital transformation in manufacturing has opened doors to promising possibilities, but not without new risk exposure. With expansive transformation comes additional threats. As manufacturers embrace automation, IoT integration, and cloud-based operations, they also become prime targets for cybercriminals seeking to exploit vulnerabilities in increasingly interconnected systems.

Deloitte's Cybersecurity Threat Trends Report 2024 revealed a staggering 400% surge in cross-industry IoT malware attacks, with the global manufacturing sector being the most targeted. This sharp increase underscores the urgent need for manufacturers to fortify their cybersecurity posture, as reliance on digital infrastructure continues to grow.

Legacy systems, looming threats

As small to mid-sized (SMB) manufacturers continue using legacy systems, cyber-attack risks increase. Aging and non-updated operating systems as well as industrial control systems without modern security controls leave known cyber exploits vulnerable, creating a significant operational and financial risk. Threat actors, primarily ROI-driven cybercriminals, exploit these dated systems' vulnerabilities with the specific goal of financial gain through ransom payment as manufacturers scramble to get impacted systems back online. Deloitte reports that [34 of the 39](#) most popular IoT exploits took advantage of vulnerabilities that had been present for over three years.

A recent World Economic Forum survey highlights an [125%](#) annual increase in the global cost of cyberattacks in the manufacturing industry, with ransomware playing a role in 71% of incidents. As attacks grow in frequency and sophistication, the financial and operational stakes continue to rise. Beyond immediate ransom payments, manufacturers face costly downtime, supply chain disruptions, regulatory fines, and reputational damage that can have long-term consequences.

For SMB manufacturers operating on tight margins, these attacks can be devastating, halting production and eroding customer trust. The reliance on IoT-connected devices has increased the risk, as outdated security protocols leave critical infrastructure exposed. Without proactive security measures, manufacturers risk attack by cybercriminals that have been successful in extorting ransoms in the manufacturing sector.

Smaller size, not lower risk

While many small and medium-sized businesses think that they are too small for cyberattacks, reality and data say otherwise. Taking advantage of a false sense of security, smaller companies often put off implementing cybersecurity controls due to limitation of resources missing crucial steps like encryption and data file backup. As a result, the manufacturing industry lags behind other sectors in cyber maturity. Implementing best practices for safeguarding is crucial for manufacturers.

The importance of maintaining good cybersecurity hygiene

For manufacturers, regular cybersecurity training is crucial and should be an ongoing initiative and a top organizational priority. Despite this, a Deloitte report found that only [29%](#) of manufacturing companies surveyed have implemented appropriate control measures to mitigate cyber risk. Common threats, including malware, phishing emails, credential theft, and ransomware attacks, continue to burden the manufacturing industry, emphasizing the need for established training programs.

Incorporating interactive exercises, real-world scenarios, and periodic simulated attacks to assess employee responses ensures that training remains effective and engaging. To build a cyber-resilient culture, manufacturers must address employees' reluctance to report suspicious activity for fear of repercussions. As such, businesses should maintain cybersecurity hygiene, establishing clear guidelines

for protecting sensitive customer data. Cybersecurity awareness is not an optional activity to tick off – it's a necessary practice to ensure an appropriate level of protection for a company.

Double defense: password management and MFA for stronger cybersecurity

For small manufacturers, multi-factor authentication (MFA), paired with a strong password management system, offers an efficient and inexpensive security solution. Password managers provide simplified solutions for the creation and storage of strong, original passwords for each account, reducing the likelihood of breaches spurred by weak or reused credentials, the primary cause of data breaches. In addition, there are helpful tools to provide features such as centralized admin controls, secure password sharing, and integration with MFA tools.

MFA enhances security by requiring multiple forms of verification, such as a one-time code from an authenticator app or text message, adding an extra layer of protection. For small businesses, implementing a strong MFA strategy is one of the most valuable technical safeguards. When combined with password managers, these tools create a simple yet highly effective security framework, even for teams without dedicated IT support.

Cloud coverage: backup to weather cyberattacks

Regular data backups are essential safeguards against cyberattacks, hardware failures, human error, and natural disasters. It's crucial to back up critical data, such as HR records, financial files, and databases, offline and in secure cloud environments. Organizations should prioritize solutions that allow the creation of immutable offline copies, as many ransomware attacks specifically target backup data to hinder recovery efforts. In fact, [McKinsey](#) found that most modern ransomware attacks begin by encrypting backup data to prevent restoration.

For manufacturers without dedicated cybersecurity teams, a cloud Enterprise Resource Planning (ERP) provider serves as a built-in security partner—offering enterprise-grade backup strategies without the in-house burden. Cloud ERP vendors ensure that software, security patches, and compliance updates are automatically maintained, reducing risk from outdated systems. Migrating business-critical systems like ERP and HRM to the cloud means that security best practices, including regular encrypted backups and rapid disaster recovery, are managed by experts, offering enhanced protection and peace of mind.

Preparing for tomorrow's cyber threats

Cyber threats are constantly evolving, and even the most secure systems remain vulnerable to advanced attacks and human error. Prioritizing a cloud-first approach, paired with strong password management, multi-factor authentication, endpoint detection, automated data backups, regular vulnerability assessments, and ongoing employee training, lays the groundwork for a resilient defense.

Cybersecurity isn't about eliminating all risks; it's about strengthening adaptability. By leveraging cloud-based systems, detecting threats early, and establishing clear recovery protocols, small manufacturers can reduce downtime, limit damage, and ensure business continuity even in the face of an attack.

About the Author

As Chief Technology Officer, Brian Winters leads the delivery of ECI Software Solutions' cloud-based SaaS solutions, the constant evolution of their cybersecurity stance, and the management of corporate information technology operations. Brian is a seasoned technology executive with a passion for customer delivery. Along with his customer-first mentality, he brings more than 15 years of leadership experience. Brian specializes in building and managing the infrastructure and operations necessary to deliver business-critical services securely via the cloud, and in positioning PE companies to maximize value.





The Cost of Ignoring Patches: How State and Local Governments Can Mitigate Damaging Security Breaches

By Joao Correia, Technical Evangelist, TuxCare

According to a recent report released by the [Multi-State Information Sharing and Analysis Center](#), governmental agencies are facing an increase in ransomware attacks from nation-state actors and other increasingly clever hackers. In the past, when considering who might be the most vulnerable to a cyberattack, large corporations and federal agencies seemed like the most obvious choice. But over time, more local, essential services such as public safety, social services, education and health sectors find themselves in the crosshairs.

From social security numbers to medical records and private tax information, state and local organizations are home to loads of personal information that can make money-hungry crooks salivate. Combine a wealth of private data with a more rural community with lackluster security safeguards, and cybercriminals often think they can grab themselves a fairly tantalizing feast.

Perhaps one of the biggest weaknesses the public sector faces is the lack of intentionally proactive cybersecurity plans. This is largely due to insufficient funding, limited access to cybersecurity professionals, and an overall lack of documented processes. While many organizations have taken steps to strengthen cyber protections through cybersecurity awareness training, identity management and multi-factor authentication (MFA), powerful vulnerability patch management fails to be included. Failing to prioritize proper vulnerability management through the patching process can create massive security gaps that create backdoors for hackers and provide a broader attack surface.

Managing cyber risk should be the highest priority for a government entity. The consequences of an attack could range from disastrous breaches of national security to severe disruptions to critical infrastructure. As a result, it is crucial for entities to supplement these controls with modern approaches that leverage vulnerability management, increase threat intelligence and invest in cyber awareness training for personnel. Local, state, and even federal levels of government are no strangers to working off of legacy systems, many of which are outdated or lack the flexibility to meet modern needs. In turn, this makes legacy systems quite costly to maintain and requires even more downtime for routine maintenance windows.

With extensive systems and networks continuing to run off of fragmented groups of IT teams across various departments, many offices and out-sourced IT contractors find themselves in a particularly challenging position when it comes to patching vulnerabilities in their operating systems. Coordinating necessary downtime and repeatedly scheduling maintenance windows threatens daily business operations and also puts the sensitive data of the citizens who depend on their service at risk. Because of this, security vulnerabilities can remain unpatched for weeks or even months as tight budgets and overworked IT teams struggle to keep up with demands. Meanwhile, cybercriminals are given an all-access pass to cause widespread disruptions that can cost organizations millions, harming not only day-to-day operations but further reduces public trust.

Currently, the go-to process for addressing security vulnerabilities involves traditional methods that manually apply patches and bug fixes to vulnerabilities during scheduled system reboots. Because of this, patch management gets viewed as a highly disruptive, all-consuming process that often gets repeatedly pushed aside. This is where choosing to fight automation with automation in the patching process can be the difference between a company going under or narrowly avoiding a damaging attack.

Stepping away from traditional methods and switching to rebootless patching, or “live” patching, especially on out-dated enterprise systems, can allow IT teams to significantly streamline the process by automatically applying security patches in the background as soon as they become available or as soon as a vulnerability is detected. Immediate patch deployment also eliminates necessary downtime, minimizing the windows of exploitable vulnerabilities and allowing public service to continue operating at a smooth pace. Additionally, placing such a tedious task on autopilot further ensures that agencies remain compliant with regulations while reducing the number of resources and labor required to do so.

While patching is crucial, it is only one of the tools to have in your cybersecurity toolbox. A robust security strategy also involves proactive incident response plans and an increased cyber awareness that starts from the inside out. Human error is a significant reason for many repeated security breaches. Tired employees opening that last email of the day may accidentally click a phishing link without thinking or open a spam email that infects a computer within minutes.

Public service employees face an abundance of risk every time they sit behind a government issued computer. Their extensive networks create a high-profile target for hacking efforts due to the ease of access to critical infrastructure, public services and even security data. As a result, vigilance, least-privilege access and multi-factor authentication services are vital to the cyber success of an entity. While it is true that government employees often undergo cyber awareness training at the beginning of their service, it is essential to maintain these threat detection skills and establish annual ongoing education. By taking these practical steps to leverage automated solutions, understanding the importance of timely patching and prioritize proactive threat response and mitigation through cyber awareness, state and local communities can dramatically reduce threats and their associated costs.

About the Author

Joao Correia serves as the Technical Evangelist at TuxCare, an innovator in enterprise-grade cybersecurity for Linux. Joao can be reached online at @jcorreiacl and at our company website <https://www.tuxcare.com/>





The Growing Threat of AI-powered Cyberattacks in 2025

By Stephen Kines, COO and Co-Founder of Goldilock

Data breach costs are rising at breakneck speed. IBM reported that the global average security breach cost is [\\$4.9 million](#), marking a 10% increase since 2024. And it won't stop here — USAID predicts that the global cost of cybercrime will climb to [\\$24 trillion](#) by 2027.

While various factors contribute to this spike, AI-powered malware poses a significant threat. AI has revolutionized business operations and innovation, but it's also become a tool for cybercriminals. AI-driven attacks can bypass traditional security measures, automate malicious activity, and exploit vulnerabilities at a record scale.

Staying ahead of evolving cyber threats is crucial as businesses operate in an increasingly interconnected world. It's time for organizations to strategize and proactively strengthen their security frameworks, positioning themselves for detecting and neutralizing threats before they escalate.

AI: A devil in disguise?

In recent years, AI has made groundbreaking strides — it's transformed industries and strengthened cybersecurity systems, with automated detection and response strategies for example. However, with this has come a new wave of cyber threats that are more sophisticated and unpredictable than ever before. Unlike traditional malware that follows static attack patterns, AI-powered malware can adapt to environments and analyze security measures, adjusting tactics to bypass defenses. These advanced AI-driven threats refine their attack strategies in real-time, making them increasingly difficult to detect and pose a greater threat to networks.

[BlackMatter ransomware](#) is a prime example. A direct evolution of the notorious [DarkSide](#) strain, BlackMatter has quickly gained a reputation as one of the most advanced ransomware threats. It uses AI-driven encryption strategies and live analysis victim defenses to evade traditional endpoint detection and response (EDR) systems, defeating standard cybersecurity tools.

As AI-powered cyber threats increase in sophistication, businesses must recognize the risks and understand the growing challenges in defending against them, so they can outsmart AI-driven malware before it strikes.

Independent attacks

As AI has advanced, it's developed a mind of its own and can operate autonomously without any human supervision or intervention. It's learned how to evade detection in real-time and slip past traditional cybersecurity defenses. This has led to more frequent attacks and successful breaches, which have overwhelmed security teams.

What's more, AI-powered malware can operate without instruction. Once it's infected a single device, it can automatically copy its behaviour across other networks, rapidly polluting multiple connected systems in minutes.

Intelligent attacks

Ransomware attacks have become even more destructive as AI-driven malware has learned to pinpoint the most valuable files and systems to exploit. AI can target databases like financial records, proprietary information, or intellectual property to maximize disruption and force victims to pay a ransom.

With machine learning, AI-powered malware can mimic legitimate system activity, making it harder for traditional security tools to detect. It can even time its attacks strategically, waiting until out-of-hour periods to execute malicious actions and avoid detection.

Precision-targeted cyber attacks

With the help of AI, cyberattacks are becoming more targeted. They can analyze vast amounts of data, such as social media activity and network behavior, to craft highly personalized phishing emails that are much harder to recognize. For example, an AI-generated phishing email might reference a familiar contact, a recent online purchase, or even adopt the writing style of a trusted colleague. This level of customization makes it easier to trick individuals into clicking malicious links with infected attachments or handing over sensitive information — dramatically increasing the success rate of cyber scams.

Defending against cyber threats with AI

Cybercriminals are adopting AI at a growing rate, making it imperative for defenders to do the same. Organizations should adopt AI-powered threat intelligence solutions to strengthen their security strategies to stay ahead. According to IBM, companies that consistently use AI and automation in cybersecurity save an average of [\\$2.2 million](#), compared to those that don't.

One approach to applying AI to defense is via AI-driven anomaly detection, which continuously monitors systems and analyzes behavior to identify real-time threats. For example, it can flag suspicious activity, such as abnormal spikes in entropy within software code, helping security teams respond faster and more effectively.

Physical network segmentation

Software-based security measures play a crucial role in any cybersecurity strategy. However, to effectively protect data and systems, businesses should adopt a hardware-focused approach like physical network segmentation. This is a new approach to protecting networks in today's highly interconnected, "always-on" world.

Physical network segmentation works by dividing a network into isolated sections using dedicated hardware. Think of it like creating separate, self-contained networks within your larger network. Each section operates independently, limiting the impact of any security issues to just that specific area. This isolation should be a core security practice, protecting sensitive data and systems by preventing unauthorized access and containing potential breaches.

Disconnecting digital assets from the internet when they're not in use drastically reduces the attack surface. This offers a much higher level of security — especially for sensitive infrastructure, operational technology, and research data that don't need to be constantly connected.

In the event of an attack, this segmented approach helps contain the damage. If one part of the network is compromised, threats can't quickly spread, and disruption is minimized by cutting off access before the situation escalates. Physical network segmentation acts as a defense-in-depth strategy, making it significantly harder for cyber threats to move across an entire network and target high-value systems.

Preparing for an uncertain future

AI-powered malware illustrates a fundamental shift in the cyber threat landscape. With its ability to learn, adapt, and execute highly targeted attacks, traditional security measures will no longer protect businesses against cyber-attacks.

To combat these intelligent threats, businesses must embrace a multilayered cybersecurity strategy that combines AI-powered detection tools with proactive risk mitigation techniques, such as physical network segmentation. By implementing these defenses, organizations can stay one step ahead.

About the Author

Stephen Kines is the COO/Co-Founder of the multi-award-winning cybersecurity company Goldilock with its multi-patented technology allowing remote physical disconnect of any device or network in the world without using the internet. Stephen is an international corporate lawyer with expertise in tech M&A in UK and EU. He has been a general counsel for ultra-high net worth individuals and families as well as a partner in international law firms. Stephen is focused on emerging technologies, including blockchain and cybersecurity. He is known for his avid community engagement and commitment to sustainability at all levels. A former military officer, Stephen serves as Goldilock's second-in-command, ensuring the company remains focused on its strategic objectives.



Stephen can be reached online at <https://www.linkedin.com/in/kines/> and at our company website <https://goldilock.com/>



The Impact of Quantum Decryption

Understanding the Risks and Preparing for the Quantum Computing Challenge

By Alyssa Walton, Senior Information Security Analyst, Deep Dive Cyber

I. Executive Summary

Quantum computing's rapid progress poses a significant threat, potentially rendering current encryption methods and nearly all encrypted data vulnerable. This includes sensitive data that has already been stolen or leaked. Some of this data is being stored in anticipation of future decryption capabilities. This is typically referred to as “harvest now, decrypt later.” Its eventual decryption could lead to severe financial losses, major security breaches, and vast global consequences. To counter this threat, an urgent migration to post-quantum cryptography standards (PQC) is imperative.

II. Introduction: The Quantum Horizon and Encrypted Data

Quantum computing presents a fundamental challenge. Its theorized capabilities cause concern because they challenge the backbone of digital security and may render many if not all of our current encryption standards obsolete. These concerns are further amplified due to the large amounts of encrypted data already stolen via data breaches. In 2023, IBM estimated the average data breach involved 4.35 million records, 83% of which included encrypted data. IBM also estimated that 83% of those breaches included encrypted data. Such figures suggest over 10 billion encrypted records may be stolen annually. There are likely several petabytes (1 petabyte = 1,000 terabytes) of encrypted data already stolen.

III. The Quantum Threat to Modern Cryptography

A. Principles of Quantum Computing

There are two key quantum mechanical phenomena, superposition and entanglement, that enable qubits to operate fundamentally differently than classical bits. Superposition allows a qubit to exist in a probabilistic combination of both 0 and 1 states simultaneously, significantly increasing the amount of information a small number of qubits can hold. Entanglement, links the quantum states of two or more qubits together in such a way that they become correlated, regardless of the physical distance separating them. These capabilities allow quantum computers to explore a vast number of possibilities concurrently, potentially offering exponential speedups over classical supercomputers.

IV. The Land of Encrypted Stolen Data

A. Today's Common Encryption Methods Used

The vast majority of sensitive data is protected using prevalent encryption algorithms. Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) are widely employed for public-key cryptography. Advanced Encryption Standard (AES) is a widely adopted symmetric encryption standard used to encrypt large amounts of data.

B. Types of Sensitive Data Targeted

A wide range of sensitive data, including financial records, Personally Identifiable Information (PII), intellectual property, and government secrets, is encrypted and stored by individuals, organizations, and governments. This information is highly sought after by malicious actors for purposes such as financial fraud, identity theft, corporate espionage, and compromising national security. Consequently, a market exists on the dark web where various types of stolen data are sold at different prices. For instance, personal data profiles can cost \$10-\$100, financial details like credit cards range from \$5-\$120, compromised corporate databases can fetch \$500-\$100,000, and government credentials like passports may sell for \$500-\$3,000, with prices varying based on the data's sensitivity and completeness.

C. The "Harvest Now, Decrypt Later" (HNDL) Strategy

These marketplaces highlight the viability of the strategy called "harvest now, decrypt later" (HNDL). CISA warns that threat actors, particularly nation-states, are collecting encrypted data now, anticipating future decryption via quantum computers. The data types most likely targeted are those with enduring value, such as government secrets, intellectual property, and sensitive personal or financial records.

V. Unlocking the Past: The Impact of Quantum Decryption

A. Cryptographically Relevant Quantum Computers

Predicting when quantum computers can break current encryption standards remains complex. Some experts are forecasting the first quantum computer capable of breaking RSA-2048 encryption will be available within the next 5 to 10 years, potentially as early as 2029 or 2030. However, some other experts believe this timeline is further out, suggesting it might take until 2034 or even 2044 for such a quantum computer to be available.

B. Implications and Time Sensitivity

Quantum decryption of data stolen using current standards could have pervasive impacts. Government secrets, more long-term data, and intellectual property remain at significant risk even if decrypted years after a breach. Decrypted government communications, documents, or military strategies could compromise national security. An organization's competitive advantage could be undermined by trade secrets being exposed. Meanwhile, data such as credit card information will diminish over time due to expiration dates and the issuance of new cards. However, compromised personal information poses long-term risks like identity theft and fraud, even years after exposure.

C. AI's Role in Enhancing Quantum Decryption Capabilities

Artificial intelligence (AI) further amplifies the threat to encrypted data. AI could potentially optimize quantum decryption algorithms. AI could also rapidly analyze decrypted data, helping threat actors identify and exploit valuable information. This synergy between quantum computing's decryption power and AI's analytical capabilities could significantly increase the impact and effectiveness of cyberattacks.

VI. Post-Quantum Cryptography

A. Leading PQC Algorithm Solutions

Several families of PQC algorithms have been selected by The National Institute of Standards and Technology (NIST) as replacements for current vulnerable methods.

Lattice-based cryptography (CRYSTALS-Kyber and CRYSTALS-Dilithium) is a key encapsulation mechanism (KEM). Lattice-based cryptography relies on two difficult mathematical problems. The first, Learning With Errors (LWE), gives a set of linear equations with small errors added. This makes recovering the original value extremely difficult. The second, Short Integer Solution (SIS), requires finding

a small nonzero integer solution that satisfies the given equation. These two mathematical problems attempt to make this cryptography quantum proof.

Stateless hash-based cryptography (SPHINCS+) utilizes cryptographic hash functions and Merkle trees to create digital signatures that are believed to be resistant to quantum attacks. This is believed to be quantum resistant due to the hash functions designed to be one-way and highly linear. This means they do not have an algebraic structure that can be as easily exploited by quantum algorithms.

B. Challenges of PQC Adoption and Implementation

To navigate the new complexities PQC presents, organizations need to prioritize "crypto agility," the ability to quickly and seamlessly switch between cryptographic algorithms as threats evolve and new standards emerge. This will likely require infrastructure upgrades across various systems and applications. During the transition period, some organizations might also consider adopting hybrid cryptographic systems that combine existing and post-quantum algorithms to provide an added layer of security.

VII. Potential Financial Damages

A. Potential Impacts

Quantum decryption of stolen personal and financial data could trigger a surge in identity theft and financial fraud, as criminals exploit previously inaccessible information. Furthermore, the exposure of sensitive personal details, such as medical histories and private communications, could cause significant erosion of personal privacy.

For organizations, the ability of quantum computers to decrypt previously stolen data could result in substantial financial losses due to data breaches, corporate espionage, and potential legal liabilities. The exposure of sensitive corporate information, such as trade secrets and strategic plans, could provide competitors with an unfair advantage, leading to significant financial harm. Organizations could face significant reputational damage and a loss of customer trust if their previously secured data is exposed due to quantum decryption.

B. Quantifying Potential Future Damages

Quantifying financial damages from future quantum decryption is challenging, but existing reports offer insight into the potential scale of the impact. A report from the Hudson Institute's Quantum Alliance Initiative estimated that a quantum-enabled attack on the Federal Reserve's payment system could result in a direct loss of 10-17% of US GDP and between \$2 and \$3.3 trillion in indirect losses. While these figures represent current data breach costs and specific potential scenarios, they highlight the immense financial risks associated with the future decryption of sensitive data.

VIII. Potential Global and Geopolitical Implications

A. National Security Risks

Quantum decryption poses significant national security risks and the potential for substantial intelligence advantages. Nations that achieve this capability first could gain unprecedented access to sensitive government and military communications, defense strategies, diplomatic negotiations, and intelligence operations. This could lead to significant shifts in geopolitical power and potentially destabilize international relations.

B. Reputational Dangers for Organizations

The security of e-commerce, online banking, digital communication platforms, and critical infrastructure all rely heavily on robust encryption. If this security is compromised by a quantum computer, it could undermine public confidence, potentially disrupting the economy and societal norms. Alternatively, if an organization in this field implements post-quantum encryption standards and withstands attacks, it could exponentially bolster their reputational standing in the industry.

C. Geopolitical Power Shifts and International Relations

The development of quantum computing technologies are becoming critical factors in the geopolitical landscape. Major global powers are engaged in a "quantum race" to achieve technological superiority in this domain. The nation that first develops a robust and scalable quantum computer capable of breaking encryption could gain a decisive strategic advantage in intelligence gathering, cyber warfare, and overall global influence.

IX. Recommendations and Strategic Initiatives

A. For Individuals

Individuals should adopt proactive data protection practices to mitigate the potential future impact of quantum decryption. This includes using strong, unique passwords for different online accounts and enabling multi-factor authentication wherever possible. For individuals, multi-factor authentication will continue to be one of the best tools to mitigate against data breaches and account takeovers. Individuals should also regularly update software and operating systems on all devices to patch known vulnerabilities. Individuals should be cautious about sharing sensitive personal information online and should regularly monitor their financial accounts and credit reports for any suspicious activity. Individuals should remain aware of updating encryption standards and tools as these services actively transition to the post-quantum cryptographic standards. Adopting encrypted messaging services or platforms that offer post-quantum encryption standards when available would be valuable. While these measures may not directly prevent the decryption of already stolen data, they can significantly reduce the risk of future data breaches.

B. For Organizations

Organizations must recognize the urgency of transitioning to post-quantum cryptography to safeguard their sensitive data against future quantum threats. Imminently, organizations should conduct organization-wide audits to identify where legacy encryption methods and data are most vulnerable. Organizations should establish a committee or task force to oversee the “quantum readiness” implementation and migration. This task force must remain up to date on quantum-secure technologies such as post-quantum VPNs and quantum key distribution solutions. Implementing robust data minimization policies to reduce the amount of sensitive data stored long-term will also limit the potential impact of future decryption. Building “crypto agility” into their systems is crucial to enable a smooth and efficient transition to new cryptographic algorithms as they become standardized and available. Utilizing a phased migration that combines classical and quantum-resistant cryptography standards will assist with ensuring a smooth transition. Organizational audits should assist in identifying and prioritizing the most at-risk data, systems, and encryption standards within the organization so these can be monitored heavily until they are moved to a post-quantum cryptography standard.

C. For Governments

Governments must invest in and expedite PQC research in standardizing efforts for post-quantum cryptography. International cooperation in establishing global quantum security standards and protocols is essential given the transnational nature of cyber threats. Raising public awareness and providing education about the potential quantum threat and the importance of adopting quantum-resistant security measures will also be crucial for a coordinated global response. The government must foster partnerships between private enterprises such as cybersecurity firms and research institutions to further accelerate quantum security adoption.

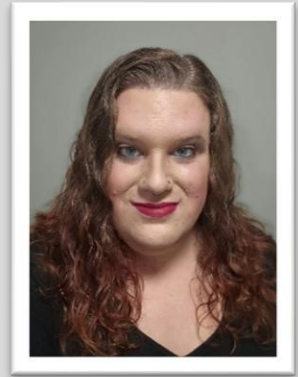
X. Conclusion: Preparing for the Quantum Decryption Reality

Quantum computing's potential to break current encryption poses an imminent threat to the vast amounts of encrypted data that have already been stolen or leaked. The potential for severe financial repercussions, significant security breaches, and profound geopolitical consequences underscores the gravity of this situation. As we stand on the cusp of the quantum era, it is imperative that individuals, organizations, and governments recognize the urgency of this challenge and prioritize the transition to post-quantum cryptography. Proactive security, data minimization, and international collaboration are key to preparing for the quantum decryption reality and safeguarding our digital future.

About the Author

Alyssa Walton has 10 years of experience in Information Technology and Cybersecurity. Her diverse professional background includes roles as Senior Information Security Analyst, Security Engineer, Information Technology Manager, and Systems/Network Engineer.

Alyssa's academic qualifications include a Master of Science in Cybersecurity and a Bachelor of Science in Information Systems. Alyssa can be contacted via email at alyssawalton91@gmail.com or via LinkedIn at <https://linkedin.com/in/alyssawalton001>.





Ongoing Money Laundering Insights

By Milica D. Djekic, Independent Researcher, Subotica, Serbia

Abstract

Money laundering is a major financial crime that involves introducing illicitly obtained funds into legitimate financial systems to disguise their criminal origins. Beyond concealing criminal activity, laundered funds are frequently redirected to exert economic influence, finance organized crime, or destabilize regional and international systems. This paper examines the mechanisms through which illicit capital infiltrates legitimate businesses—particularly vulnerable small and medium-sized enterprises (SMEs)—and how such financial interference can precipitate economic crises. Once these businesses become dependent on illicit financing, any disruption in funding can lead to mass bankruptcies, widespread unemployment, and systemic socioeconomic decline. This analysis explores how money laundering not only supports criminal enterprises but also acts as a catalyst for broader social and psychological destabilization. Strategic recommendations are provided to mitigate the threat of financial criminality on national and global levels.

Keywords: money laundering, financial crime, economic destabilization, transnational crime, business infiltration, recession risk

1. Introduction

Recent global events—such as the Great Recession, transnational terrorism, the spread of misinformation, and public health crises—highlight the vulnerabilities within legal and financial systems worldwide. These systemic weaknesses are increasingly exploited by organized criminal networks, which use sophisticated methods to infiltrate legitimate markets and institutions. Of particular concern is the strategic integration of criminal proceeds into legal economies, enabling such actors to accumulate both financial and geopolitical influence.

Transnational criminal organizations, including those that fund extremist activities, operate on a profit-driven model and maintain extensive global networks. These groups undermine national and international security by investing in legitimate enterprises, leveraging economic crises to their advantage, and fostering political instability. For instance, the ripple effects of the global financial crisis destabilized both developed and developing economies, exposing millions to unemployment, poverty, and erosion of institutional trust.

The interconnectedness of the modern world demands robust international cooperation. Isolated national responses are insufficient to counter globally networked financial threats. This paper argues for a systemic, coordinated defense against the misuse of legal financial infrastructure by criminal entities.

2. Mechanisms of Financial Infiltration and Economic Disruption

Money laundering is not limited to cash concealment—it is often used as a strategic tool to achieve broader economic disruption. Criminal enterprises exploit legal channels, investing in or acquiring businesses under the guise of legitimate activity. In some cases, newly established firms or recently acquired companies become vehicles for laundering illicit capital, creating an illusion of economic vitality while remaining financially dependent on criminal proceeds.

Once these businesses are embedded within the economic system, they can significantly influence employment, supply chains, and regional growth metrics. However, when the flow of illicit funds ceases—either due to enforcement actions or strategic withdrawal—the result is often a cascade of business failures, mass layoffs, and localized economic collapse. The socioeconomic fallout includes mortgage defaults, rising homelessness, and increased dependence on public assistance programs—consequently burdening government resources and destabilizing families and communities.

This disruption is compounded by psychological operations and disinformation campaigns, which further erode public trust in institutions. Youth populations are especially vulnerable, as family instability can increase susceptibility to criminal recruitment and radical ideologies.

3. Financial Criminality in the Legitimate Economy

Criminal organizations use a variety of methods to integrate illicit funds into legitimate business activities. These may include:

- Direct investment in SMEs or startups
- Acquisition of struggling businesses
- Establishment of front companies
- Manipulation of ownership structures to obscure the source of capital

These entities often operate at a loss, relying on illicit funding rather than sustainable revenue models. The goal is not long-term profitability but strategic economic control. Such businesses may undercut market prices, displace legitimate competitors, and distort regional economic indicators.

When criminal investors simultaneously withdraw support across multiple firms, the resulting economic shock can trigger localized or national recessions. This tactic effectively weaponizes economic interdependence to generate systemic instability.

4. Global Implications and Strategic Vulnerabilities

The infiltration of legal economies by transnational criminal networks has far-reaching consequences. In regions where money laundering is pervasive, entire industries may become dependent on illicit capital, creating systemic vulnerabilities. When these systems collapse, the effects mirror those of a natural disaster or act of war—mass unemployment, reduced consumer spending, and erosion of social cohesion.

Crisis environments also create opportunities for criminal profiteering. Distressed assets can be acquired at deflated prices, only to be resold or exploited once economic recovery begins. This cyclical exploitation of crisis and recovery allows bad actors to accumulate both capital and influence.

Governments are often under pressure to stabilize the economy may prioritize short-term recovery over long-term security measures. In doing so, they may inadvertently create conditions favorable to further criminal infiltration.

5. Discussion and Conclusion

Money laundering is more than a financial crime; it is a strategic threat to national and international stability. It enables organized crime to establish control over critical sectors of the economy, manipulate labor markets, and undermine public trust in governance.

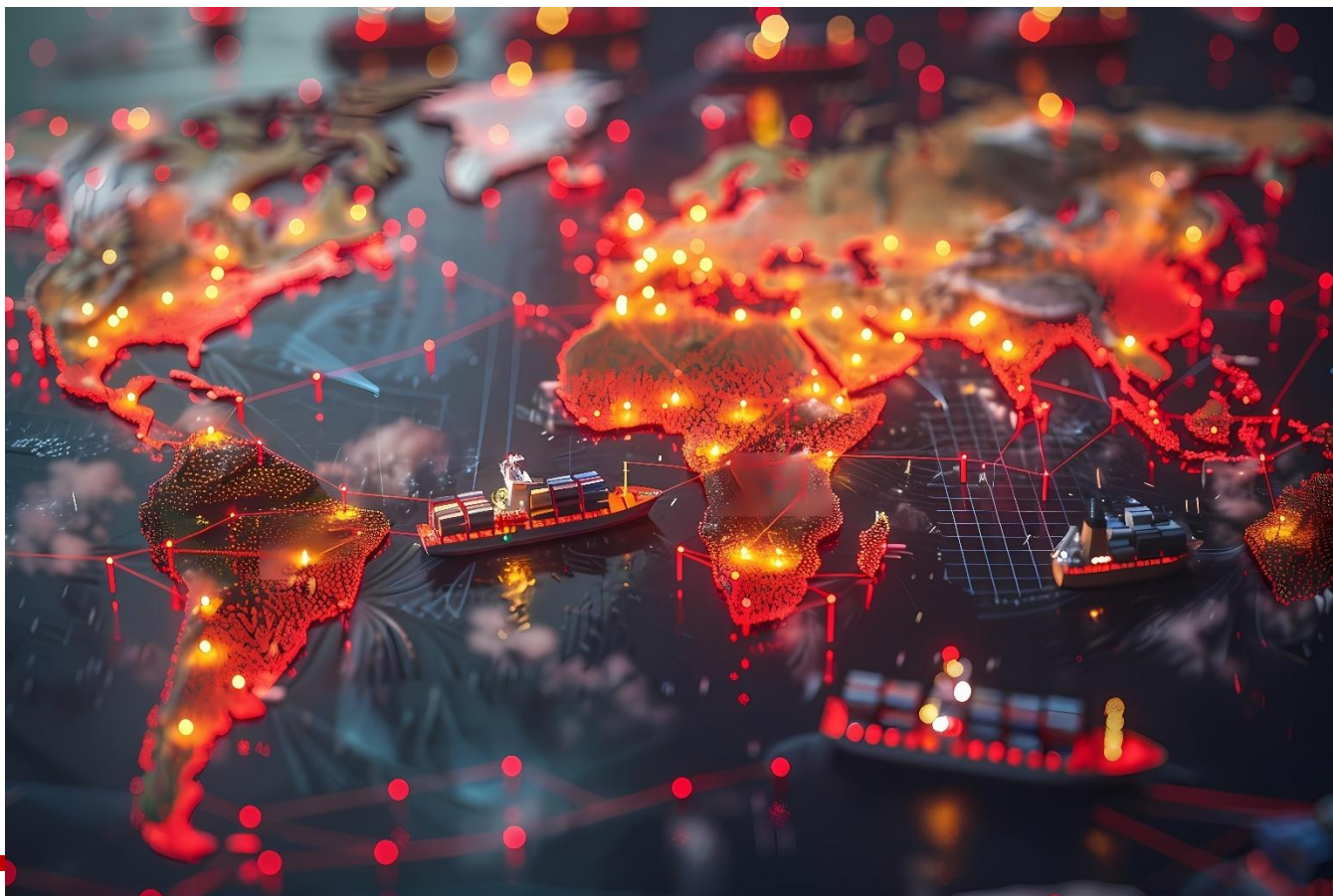
As demonstrated in the aftermath of the Great Recession, the collapse of illicitly funded enterprises can devastate working families, deplete public resources, and catalyze political instability. Over time, these effects can erode even the most resilient economies. When global criminal syndicates manipulate financial systems on this scale, the result is a form of economic warfare that demands a coordinated, multidimensional response.

Addressing this threat requires stronger international frameworks for financial intelligence sharing, enhanced due diligence requirements, and targeted interventions to disrupt money laundering channels. Equally important is a renewed focus on societal resilience—ensuring that families, businesses, and institutions are equipped to resist and recover from financial manipulation.

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 presses 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.





The Quantum Supply Chain Risk: How Quantum Computing Will Disrupt Global Commerce

By Blake Lazarus, Security Insights Contributor, Zeroproof

The Global Supply Chain Is Already on Fire — We Just Don't See the Smoke.

The global supply chain is not a just a system — it's a network of fragile interdependencies connected together with trust, timing & software at its very core. Every container, shipyard, import & semi-truck is the result of hundreds of dependencies that span across multiple countries, vendors, suppliers and intermediaries connecting them all. The thin layers of the global supply chain have become increasingly digitized in the past decade with automation, software and AI serving as the new foundation for connected trade. But even today, the supply chain is constantly being exploited by nation-state actors resulting in often times detrimental breaches that compromise the integrity of global systems. From embedded malware to hijacking of entire codebases, bad actors have learned to leverage AI & ML to intercept valuable data and penetrate operational technology that can have real stopping power on modern trade

around the world. Now imagine the current level of risk — but with the capabilities of quantum computers layered on top.

Quantum Won't Just Break Encryption — It Will Break Global Trust

Quantum computing poses a threat to more than just encryption. In a world where trust in software, hardware, data & communications lies in digital signatures and cryptographic certificates, quantum computing stands to disrupt decades worth of security & infrastructure. Algorithms like RSA and ECC are used to create digital signatures and manage public-key cryptography. This allows systems to verify the authenticity and integrity of code, updates, and different digital identities. It's the reason why your laptop knows firmware updates are coming from Apple and not a bad actor, or how servers know to trust packages from AWS. Quantum computing threatens to break the most secure encryption algorithms, keys & forge these proofs of authenticity rapidly. Once quantum computers can mimic these cryptographic fingerprints, authenticity, identity & security has the potential to collapse. In a post-quantum world, trust may become the weakest link in the chain, threatening the security of global supply chains.

The Real Target is Trade Infrastructure

Whether its API's, middleware, firmware embedded devices or operational technology, they're all built on the same outdated encryption and systems of trust. One of the biggest threats from quantum computing will be on all this unseen machinery that powers global digital trade. These systems handle the backend of everything from routing to cargo to scheduling deliveries and clearing large shipments, but they were never designed to withstand the threat of quantum. Attackers will be able to break in quietly — injecting malicious code into control software, ERP systems or impersonating suppliers to communicate malicious information and hijack digital workflows. Quantum computing won't necessarily affect the industries on its own, but it will corrupt the systems that power the global economy.

Quantum Espionage Will Be a Silent Killer — Harvest Now, Detonate Later

Some of the most dangerous attacks are being staged today, with many nation-states and bad actors storing encrypted data, from procurement orders to shipping records. When quantum computers are finally able to break those encryption schemes, attackers will be able to decrypt them in what's coined a Harvest Now Decrypt Later (HNDL) attack. These attacks, although retroactive in nature, represent one of the biggest threats to the integrity of cross-border commerce. Global trade depends on digital provenance or handling goods and proving where they came from. Once attackers can forge, backdate or supplement data, it will destroy transparency, traceability and regulatory compliance that so many importers and exporters rely on. This is called temporal warfare, and it's a silent, patient attack, waiting to corrupt supply chains over time and destroy trust in global systems.

Digital Provenance Will Collapse Without a New Standard

Provenance systems such as signed software, encrypted communications and blockchain traceability rely on public-key cryptography, the exact encryption schemes that quantum is expected to break. When RSA and ECC fall, signatures and certificates will no longer have the same trusted security capabilities that they used to. The blockchain record may represent itself as authentic, but attackers with forged quantum-signed keys will be able to inject themselves into the chain without leaving a trace. Without quantum-resistant, provable standards for post-quantum cryptography and key distribution, compliance, insurance, legal accountability and more are dead in the water.

Conclusion

Quantum computing may upend trade and commerce as we know it, but it doesn't have to break it. The risks are very real — authentication will be challenged, provenance disrupted, and digital and physical trust will be put to the test. But this doesn't mark the end of digital trust, but rather a very uniquely positioned time to rebuild it. Across the globe, researchers and innovators are developing the next generation of post-quantum security. Post quantum cryptography candidates have now been approved by the National Institute of Standards and Technology (NIST), and secure key distribution methods are next to hit their stride. This is an inflection point in digital security and, for the first time in decades, marks the start of a new decade of core system redevelopment. Those that take action today to integrate post-quantum systems and protect themselves from future attacks will hold the blueprint for a more resilient, transparent and secure global economy in the years to come.

About the Author

Blake Lazarus is the CMO and security insights contributor for Zeroproof. At Zeroproof we develop quantum-resistant key distribution systems for the next generation of enterprise security.

Blake can be reached online at blake@zeroproof.com and at our company website <https://www.zeroproof.com>





The Rise of Identity Risk Intelligence

By Andres Andreu, COO and CISO, Constella Intelligence

For many years, cybersecurity professionals have relied on Indicators of Compromise (IOCs) such as IP addresses, domain names, and file hashes to defend against a number of cyber threats. While these technical artifacts provide valuable data points, their effectiveness as a primary defense mechanism is waning in the face of increasingly strategic adversaries. Time has shown that adversarial strategies gravitate towards paths of least resistance.

The Limitations of Traditional IOCs

Attackers can easily spoof traffic sources and rapidly change their operational infrastructure, rendering techniques like IP address blocking efforts futile. An IP address identified as malicious today might be obsolete tomorrow. Additionally, threat actors can manipulate malware file hashes in seconds, bypassing signature-based detection systems. The proliferation of polymorphic malware, which automatically alters its code, further diminishes the effectiveness of traditional hash-based detection methods.

Cybersecurity teams are often overwhelmed by the sheer volume of data from threat intelligence feeds, much of which quickly becomes irrelevant. These massive "blacklists" of IOCs are often outdated due to the ephemeral nature of attacker infrastructure and the ease of modifying malware signatures. This data overload makes it difficult for security analysts to identify genuine threats and implement effective

proactive measures. Furthermore, traditional threat intelligence often lacks the context needed to identify the actor behind an attack, hindering preventative efforts.

The Shift Towards Identity-Centric Security

The reality is that identifying malware before user execution is increasingly challenging. Modern security breaches frequently involve compromised identities, an element that traditional IOC feeds often miss. [Verizon's 2024 Data Breach Investigations Report](#) (DBIR) indicates that stolen credentials have been a factor in nearly one-third (31%) of all breaches over the past decade. Research from [Varonis](#) in 2024 reveals that 57% of cyberattacks begin with a compromised identity. Attackers are increasingly choosing to "log in" rather than "hack in," exploiting either valid username and password combinations or exposed session objects (e.g. cookies) obtained through various means. This approach allows them to bypass security controls by impersonating legitimate users. Multi-Factor Authentication (MFA), while valuable, does not fully mitigate the risks associated with compromised identities, especially when considering session objects exfiltrated through infostealer malware. Traditional defensive strategies and IOC-based defenses are often blind to these incursions, as malicious activity appears to be legitimate user behavior.

This evolving threat landscape necessitates a proactive approach, driving cybersecurity professionals to adopt identity-centric cyber intelligence. This approach shifts the focus from chasing transient technical indicators to monitoring human and non-human entities within digital ecosystems. Instead of solely focusing on blocking malware or IP addresses, cybersecurity teams are now prioritizing questions like "which identities, credentials, sessions, or personal data have been compromised?". This evolved strategy involves correlating various seemingly disparate signals, such as usernames, email addresses, and passwords, across multiple data breaches and leaks to develop a comprehensive understanding of risky identities and the threat actors behind them. The effectiveness of this approach is directly related to the volume and hygiene of the data analyzed; more high fidelity data leads to richer and more accurate intelligence. For example, identity-centric cyber intelligence can quickly verify if a user's email and password have been exposed in recent data breaches and analyze historical data to identify patterns of misuse. Correlating timely and comprehensive data provides a level of contextual awareness that traditional threat intelligence lacks.

The Power of Identity Signals

Identity signals are crucial for distinguishing legitimate users from imposters or synthetic identities. The rise of remote and hybrid work models, cloud services, and VPNs has made it easier for attackers to create synthetic identities or compromise valid user identities. While traditional indicators like source IP addresses are insufficient to determine the legitimacy of a user, an identity-centric approach excels in this area. By analyzing multiple attributes associated with an identity against extensive data stores of breached data and fraudulent identities, organizations can identify risky identities. For instance, an email address with no prior legitimate online presence that suddenly appears in numerous unrelated breach datasets could indicate a synthetic profile.

Advanced threat intelligence platforms utilize entity graphing to visually map and correlate seemingly unrelated signals, revealing hidden connections. These interconnected graphs can expose relationships between threat actors, even when they use obscure data points. This high-fidelity intelligence can identify not just isolated threat artifacts but also the human adversaries orchestrating malicious campaigns. Understanding the identity of the individual behind the keyboard is as critical as understanding their Tactics, Techniques, and Procedures (TTPs).

Historical Context: The Power of Signal Analysis

The concept of analyzing signals for threat intelligence is not new. The National Security Agency (NSA) project labeled [ThinThread](#) (circa 1990s) aimed to analyze phone and email metadata to identify potential threats. ThinThread demonstrated the potential of analyzing seemingly disparate signals to gain critical insights. The core component of ThinThread, known as MAINWAY, which focused on analyzing communication patterns, was eventually deployed and became a key part of the NSA's domestic surveillance program. This historical example illustrates the potential of analyzing seemingly disparate signals to gain critical insights into potential threats, a principle that underpins modern identity risk intelligence.

Real-World Example: North Korean Cyber Espionage

Recent events highlight the urgent need for identity-centric intelligence, particularly the numerous cases of North Korean intelligence operatives infiltrating companies by posing as remote IT workers. These highly skilled agents create elaborate fake personas with fabricated online presences, counterfeit resumes, stolen personal data, and AI-generated profile pictures to secure employment. Once employed, they often exfiltrate data. In some cases, they diligently perform their IT work to avoid suspicion. U.S. investigators have corroborated the widespread nature of this tactic, revealing that North Korean nationals have fraudulently obtained employment by presenting themselves as citizens of other countries. These operatives create synthetic identities to pass background checks and interviews, acquiring personal information to appear as proficient software developers or IT specialists. One North Korean hacker even secured a software developer position at a cybersecurity company using a stolen American identity and an AI-generated profile photo, deceiving HR and recruiters. In some instances, these actors exfiltrate sensitive data within days of employment. KnowBe4, a security training firm, discovered a newly hired engineer who was a North Korean operative downloading hacking tools onto the company network. The operative was only apprehended because of the company's proactive monitoring systems.

This example underscores that traditional security measures, background screenings, and network monitoring may be insufficient to detect these sophisticated threats. Intelligence that can unmask these malicious actors early in the process is crucial, highlighting the value of identity risk intelligence. Proactively incorporating identity risk signals early in the screening process can help organizations identify potential imposters before they gain network access. For example, an identity-centric approach might have flagged the [KnowBe4 hire](#) as high-risk before onboarding by uncovering inconsistencies or prior exposure of their personal data.

Identity risk intelligence enables several types of disinformation security measures:

- **Digital footprint verification:** Cybersecurity analysts can investigate a job applicant's claimed identity by leveraging breach and darknet databases. Discrepancies, such as an email address or name appearing in breach data associated with different individuals, or a supposed U.S.-based engineer's records tracing back to foreign IP addresses, should raise concerns. In disinformation security, this helps identify fabricated identities used to spread false information or gain unauthorized access. Digital footprint analysis involves thoroughly examining a user's online presence across platforms to verify their legitimacy. Inconsistencies or a lack of a genuine online presence can indicate a synthetic identity.
- **Proof of life / Synthetic identity detection:** Advanced platforms can analyze combinations of Personally Identifiable Information (PII) to determine the likelihood of an identity being genuine versus fabricated. Non-existent social media presence or AI-generated profile photos are strong indicators of a synthetic persona. This is crucial for disinformation security, as threat actors often use AI-generated profiles to create believable fake identities. AI algorithms and machine learning techniques are essential for detecting these anomalies within large datasets. Behavioral biometrics, which analyzes unique user interaction patterns, can further aid in distinguishing between genuine and synthetic identities.
- **Continuous identity monitoring:** Monitoring activity and credentials can expose anomalies even after an individual is hired. For example, an alert could be generated if a contractor's account appears in a credential dump online. For disinformation security, this allows for the detection of compromised accounts used to spread malicious content or propaganda.

Sophisticated disinformation campaigns highlight the importance of linking cyber threats to identity risk intelligence. Static IOCs cannot reveal the danger of a seemingly "normal" user account belonging to a hostile actor; nor can it reveal if a "normal" user's data is actively being used by a nefarious actor. However, identity-centric analysis can provide early warnings by meticulously vetting an individual's true identity and determining if their digital persona connects to known threat activity. This is threat attribution in action: prioritizing identity signals makes it possible to attribute suspicious activity to the actual threat actor. The Lazarus Group, for instance, utilizes social engineering tactics on platforms like LinkedIn to distribute malware and steal credentials, highlighting the need for identity-focused monitoring even on professional networks. Similarly, APT29 (Cozy Bear) employs advanced spear-phishing campaigns, underscoring the importance of verifying the legitimacy of individuals and their digital footprints.

About the Author

Andres Andreu serves as both the Chief Operating Officer (COO) and Chief Information Security Officer (CISO) at Constella Intelligence. He is a 4X CISO and distinguished cybersecurity leader with credentials including CISSP, ISSAP, and Boardroom Certified Qualified Technology Expert (QTE). His diverse career spans federal law enforcement—where he earned three U.S. Department of Justice awards for contributions to lawful intercept technology—corporate leadership at Hearst, Ogilvy & Mather and 2U, Inc./edX, and entrepreneurial success as a founding executive at Bayshore Networks (acquired by Opswat in 2021). Recognized as a Top 100 CISO (C100) and a Top 50 Information Security Professional, he balances offensive and defensive cybersecurity strategies with a leadership philosophy that aligns executive and employee objectives. An acclaimed author of *The CISO Playbook* and *Professional Pen Testing Web Applications*, he also holds patents in cybersecurity innovations and advises at Forgepoint Capital's Cybersecurity Advisory Council.

Andres can be reached online at [LinkedIn](#) and at our company website <https://constella.ai/>





The Rising Deepfake Risk for Businesses: A Step-By-Step Defense Strategy Built Around the Basics of Security

By Matthew Martin, CEO, Two Candlesticks

Deepfakes are the exciting new thing in cyber security, but at their core they are not a new threat – social engineering has been around since the beginning. Advancements in artificial intelligence (AI) are taking social engineering attacks on organizations to a whole new level though, showing up in new ways. As AI models become faster and more sophisticated, deepfakes become more automated and convincing. This enables threat actors to be much more efficient and effective, ramping up the risk to organization's critical data and infrastructure.

It's clear to see that deepfakes are an increasing threat to organizations, with 1 in 4 companies experiencing deepfake fraud in the last 12 months, according to [Deloitte](#). These attacks are generated using AI and machine-learning (ML) algorithms, arming threat actors with the tools to create highly convincing, yet completely fake digital content.

While this is nothing new, the ease of execution has made deepfakes an even bigger threat – modern AI advancements mean threat actors can now swiftly bypass verification processes or trick employees into sharing sensitive information. In turn, this allows threat actors to cast their nets wider. While larger, highly profitable organizations were once the top target for deepfake attacks, threat actors are now setting their sights on smaller businesses.

The Leadership Disconnect

In recent years, the barrier to entry for cybercriminals has been lowered. Why? Because GenAI tools used in deepfakes have become more widely accessible and available. Threat actors can now not only create more believable deepfakes but launch attacks on a much wider scale than before.

Here's where leadership fails most organizations: around one quarter of company leaders are barely or not at all familiar with deepfake technology, according to business.com. Meanwhile, more than half admit their employees haven't received any training on identifying these attacks.

This knowledge gap is inexcusable. As a CEO who's spent decades in cybersecurity, I've watched too many organizations chase the latest detection tools while ignoring the fundamentals of good security leadership. This is creating a dangerous disconnect where sophisticated threats meet unaddressed security gaps.

Building a Secure Foundation

Let's be clear: deepfakes are not a one-size-fits-all threat. They can take many forms – from live and recorded videos to static images and personalized phishing attacks. When assessing the impact of these different types of attacks, a good place to start is understanding your specific areas of vulnerability.

Every organization has different vulnerabilities, and some organizations will be targeted by specific types of deepfakes more than others. This often comes down to factors including the nature of your organization, what types of data you have, and the ways this data can be accessed.

For organizations that don't know where to start, understanding your weaknesses begins with understanding the most common types of deepfake fraud within your industry. Once this has been established, you can then start tailoring your defenses to the risks that matter most to your organizations.

But let's not forget the basics. Building resilience is not about throwing more tools at the problem – it's about ensuring fundamental security practices are performed well. This is where leadership plays a vital role.

When it comes to defending against deepfakes, building a culture that prioritizes security awareness is essential. For organizations that need support with this, working with an expert cyber security consultancy can help strengthen fundamental aspects including:

1. **Employee Education.** One of the most effective ways to prevent deepfake fraud is to ensure your employees understand and recognize the risks. Expanding security awareness training that covers how to spot deepfakes, the risks they pose, and the procedures to follow in the event of an attack is a no-brainer. Organizations that invest in targeted, specific training programs can significantly reduce their chances of falling victim to deepfakes.
2. **Risk Management Practices.** Solid risk management practices not only help with managing and mitigating deepfakes but defending against all major types of cyber-attacks. When it comes to

managing risk, organizations should follow a multi-step process. This includes identifying risk, assessing risk based on the potential impact, prioritizing risk and then monitoring to ensure defenses are working as intended.

3. **Best Practice Processes.** A workplace culture built around security-first processes is an essential part of defending against deepfakes. This is where best practice comes in: employees should always call unknown numbers back using trusted contact information and multi-factor authentication (MFA) should be deployed where possible to avoid unauthorized access.
4. **Phishing Simulation.** Deepfakes make business email compromise (BEC) attacks even more dangerous through realistic personalized messages. As threat tactics advance, traditional phishing simulations won't cut it anymore. Instead, organizations need exercises that match up to real-world deepfake fraud. This includes realistic simulated attacks that may impersonate executives within their own organization.

Dedicated Defenses Against Deepfakes

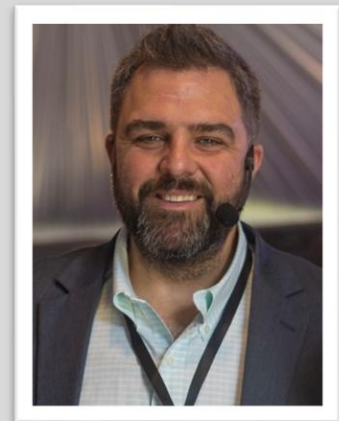
There is no silver bullet to mitigate deepfakes. At the end of the day, the key to defending against this rising risk lies not in any one tool or technique, but in ensuring that your security fundamentals are rock solid.

Now is the time to take control of your security outcomes. By leveraging a trusted cybersecurity expert who provides deep expertise, organizations can proactively prepare for what's to come, rather than reacting to attacks once it's already too late.

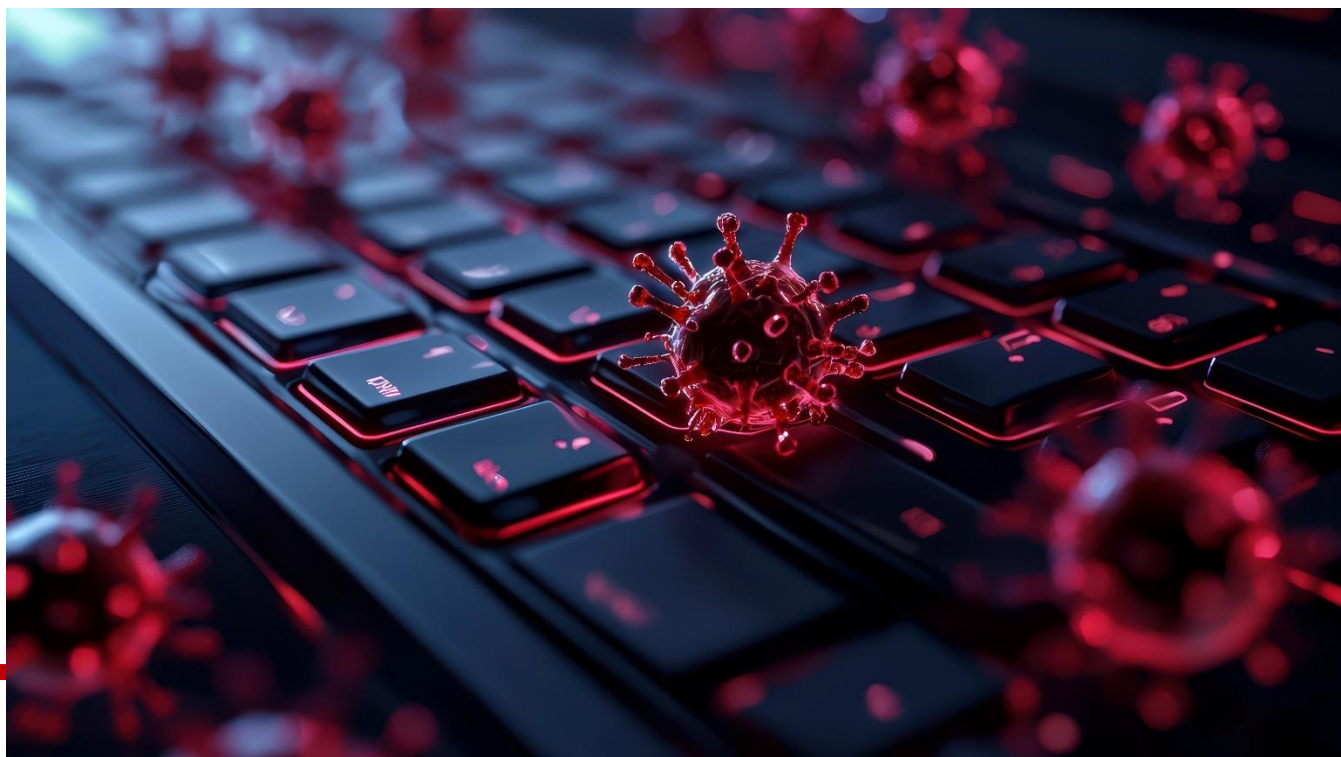
About the Author

Matthew Martin is the founder and CEO of Two Candlesticks and an international leader in cybersecurity, risk, and technology. Matt is a trusted security executive, international speaker, and board advisor for venture studios, private equity, and various startups with a focus on supporting overlooked markets and regions.

With over 25 years of experience in the cybersecurity industry, Matt has led and implemented security organizations at Fortune 100 financial services companies and currently provides high-level consultancy to companies within diverse industries around the world. He has a passion for serving the underserved in cybersecurity to create positive impacts for organizations, end users, and society.



Matthew can be reached online at MatthewMartin@two-candlesticks.com, <https://www.linkedin.com/in/mattmartin/> and at our company website <https://www.two-candlesticks.com/>



The Digital Pandemic: Inside 2024's Most Devastating Cyber Breaches

By Ashwany Pillai, Global Head of Marketing, Network Intelligence

The cybersecurity landscape of 2024 has revealed an unprecedented surge in both the frequency and sophistication of data breaches, setting new records that demand immediate attention from security professionals and organizations alike. According to IBM's latest Cost of a Data Breach Report, the year witnessed 3,158 confirmed breaches - a staggering 22% increase from 2023's 2,587 incidents.

The Growing Impact: Beyond Numbers

While statistics paint a concerning picture, the real impact extends far beyond mere numbers. The average cost per breach climbed to \$4.88 million, marking a significant increase from \$4.45 million in 2023. This trend indicates not just more frequent attacks, but increasingly devastating consequences for affected organizations.

Key Findings That Demand Attention

The shifting landscape has revealed several critical trends that security professionals must address:

Financial services have overtaken healthcare as the most targeted sector, experiencing a 43% increase in attacks compared to 2023. This unprecedented shift, confirmed by Verizon's 2024 Data Breach Investigations Report, signals a fundamental change in attacker priorities and tactics.

The third-party vendor ecosystem has emerged as the primary vulnerability, with 80% of major breaches originating through vendor access. This highlights a critical gap in current security approaches and the urgent need for comprehensive supply chain security measures.

The Most Impactful Breaches of 2024

The U.S. Federal Database Breach

This incident exposed 2.9 billion records affecting 1.3 billion individuals through a single misconfigured database permission. The breach's discovery by a 16-year-old security researcher, rather than the internal security team, underscores the need for fresh perspectives in security monitoring.

Ticketmaster's Terabyte Disaster

The leak of 1.3 terabytes of data, containing 560 million customer records, led to a flood of synthetic identity fraud and a 12% drop in live event attendance during Q3, demonstrating the direct business impact of security failures.

Critical Action Items for Organizations

Based on 2024's breach patterns, organizations must implement several game-changing strategies:

1. Implement Zero-Trust Architecture

- Eliminate traditional perimeter-based security
- Require continuous verification for all access attempts
- Deploy microsegmentation for critical assets

2. Revolutionize Third-Party Risk Management

- Establish continuous monitoring of vendor security postures
- Implement real-time risk scoring systems
- Create automated response protocols for vendor security incidents

3. Enhance Human-Centered Security

- Design security controls that work with natural human behavior
- Implement context-aware security measures
- Develop targeted security awareness programs based on role-specific risks

Looking Forward: The New Security Paradigm

Organizations must recognize that cybersecurity has evolved beyond an IT concern into a fundamental business survival issue. Success in 2025 and beyond will require:

- Integration of security considerations into all business decisions
- Adoption of advanced threat detection and response capabilities
- Development of robust incident response plans that account for modern attack vectors

Conclusion

The cybersecurity landscape of 2024 has demonstrated that traditional security approaches are no longer sufficient. Organizations must embrace comprehensive, innovative security strategies that address both technical and human elements while maintaining operational efficiency.

The path forward requires a fundamental reimagining of how we approach data protection, third-party risk, and security architecture. Only through this transformation can organizations hope to effectively counter the evolving threat landscape and protect their critical assets in 2025 and beyond.

About the Author

Ashwany Pillai is Global Head of Marketing at Network Intelligence, a leading cybersecurity services provider. He brings 15+ years of strategic marketing expertise across healthcare, B2B SaaS, and IT sectors, with specialized focus on cybersecurity market dynamics and digital transformation. His innovative approach to cybersecurity marketing combines data-driven strategies with advanced marketing automation, helping organizations navigate the complex security landscape. Currently focused on developing cutting-edge marketing frameworks for cybersecurity services adoption, Ashwany pioneers the integration of AI-driven marketing strategies with traditional cybersecurity communications. He holds multiple certifications in Digital Marketing, SEO, and Content Marketing from industry leaders including LinkedIn, SEMrush, Google, and HubSpot Academy.



Ashwany can be reached at <https://www.linkedin.com/in/ashwanypillai/> and at Network Intelligence <https://networkintelligence.ai/>



The Evolving Cloud Security Landscape: Empowering Startups in a Post-Acquisition World

By Allan Thompson, CEO & President, AcceleTrex Corporation

The cybersecurity industry is in constant flux, driven by escalating threats, emerging technologies, and strategic market maneuvers. This dynamic environment, characterized by 4,500 cybersecurity start-ups, is further complicated by significant market shifts, such as Google's recent acquisition of Wiz. While this move validates the importance of Cloud Security Operations, it also creates new opportunities and gaps in the market.

In this context, innovative approaches to go-to-market strategies are more crucial than ever. New entrants must find effective methods to build trust, gain visibility, and connect with potential customers. While traditional lead-generation tactics remain important, more organizations are recognizing the value of trusted referrals and expert networks. This realization stems from the inherent advantages referrals offer: increased credibility, faster sales cycles, and greater customer lifetime value.

Leads vs. Trusted Referrals: A Critical Distinction

In today's competitive business landscape, acquiring new customers is more challenging than ever. Companies are continually seeking effective strategies to expand their customer base and drive sales.

Two primary methods for generating potential customers are leads and referrals. While both approaches aim to attract new clients, they differ significantly in their origins, processes, and outcomes.

What is the difference between a *Lead* and a *Trusted Referral*?

Feature	Lead	Trusted Referral
Definition	A potential customer who has shown interest in your product or service but hasn't yet engaged with your business.	A potential customer who has been recommended to your business by an existing customer or a trusted source.
Source	Often generated through marketing efforts like online ads, content marketing, or social media campaigns.	Often come with a higher level of trust and credibility because they are based on personal recommendations.
Conversion	Usually require nurturing through follow-up communications to convert them into customers.	Typically, they are more likely to convert into customers quickly since they come with a positive endorsement.

Leads are generally sourced through marketing efforts and need nurturing, while Trusted Referrals come from personal recommendations and often have a higher conversion rate.

Trusted referrals typically yield a higher conversion rate than leads. Here are some key points:

- Higher Trust: Referrals come from reliable sources, suggesting that the potential customer already has a positive view of your business.
- Improved Conversion Rates: Referral leads yield a 30% higher conversion rate compared to other marketing methods.
- Faster Sales Cycle: Referrals typically convert more quickly because they arrive with a recommendation, which lessens the time required to establish trust and credibility.
- Enhanced Customer Lifetime Value: Referred customers often show increased loyalty and tend to make more purchases.
- Lower Customer Acquisition Costs: Referrals typically have a reduced acquisition cost compared to traditional marketing channels.

While both leads and referrals play crucial roles in customer acquisition, Trusted Referrals consistently demonstrate better outcomes. Trusted Referrals come with inherent trust and credibility, significantly enhancing their conversion rates compared to leads. The personal recommendation that comes with

Trusted Referrals accelerates the sales cycle, decreasing the time and effort needed to convert potential customers into loyal clients.

Additionally, Trusted Referrals frequently lead to greater customer satisfaction and retention, as they tend to resonate with the positive experiences conveyed by the referrer. By emphasizing referral strategies, businesses can harness the power of technology to attain more efficient and effective growth.

Key Considerations for Startups

Cybersecurity startups encounter unique challenges and opportunities. A key consideration is identifying and addressing gaps in functionality or services that may not be fully met. This often requires specialized expertise and a thorough understanding of customer needs. This scenario can create uncertainty, presenting opportunities for agile startups to step in and provide tailored solutions.

In this environment, one might seek to provide an opportunity for emerging companies to connect with seasoned experts, creating a synergistic "exchange" where knowledge and experience are easily shared. Such exchanges could focus on several key areas, including:

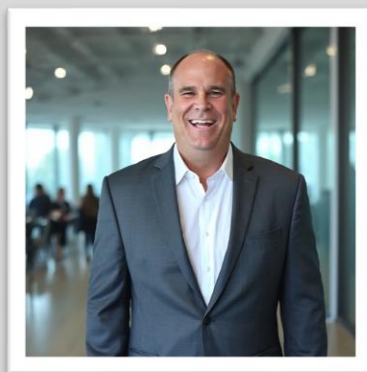
- **Beyond Core Functionality:** Meeting the demand for pre- and post-remediation expertise by utilizing qualified Market Experts to operate at cloud speed, bridging essential gaps that even the largest players cannot address.
- **Empowering the Ecosystem:** Creating a launchpad for innovation by linking emerging companies with market experts who understand runtime cloud mitigation.
- **Market Expertise at Scale:** Accelerating rapid, scalable go-to-market strategies through automated connections and incentives.

Conclusion

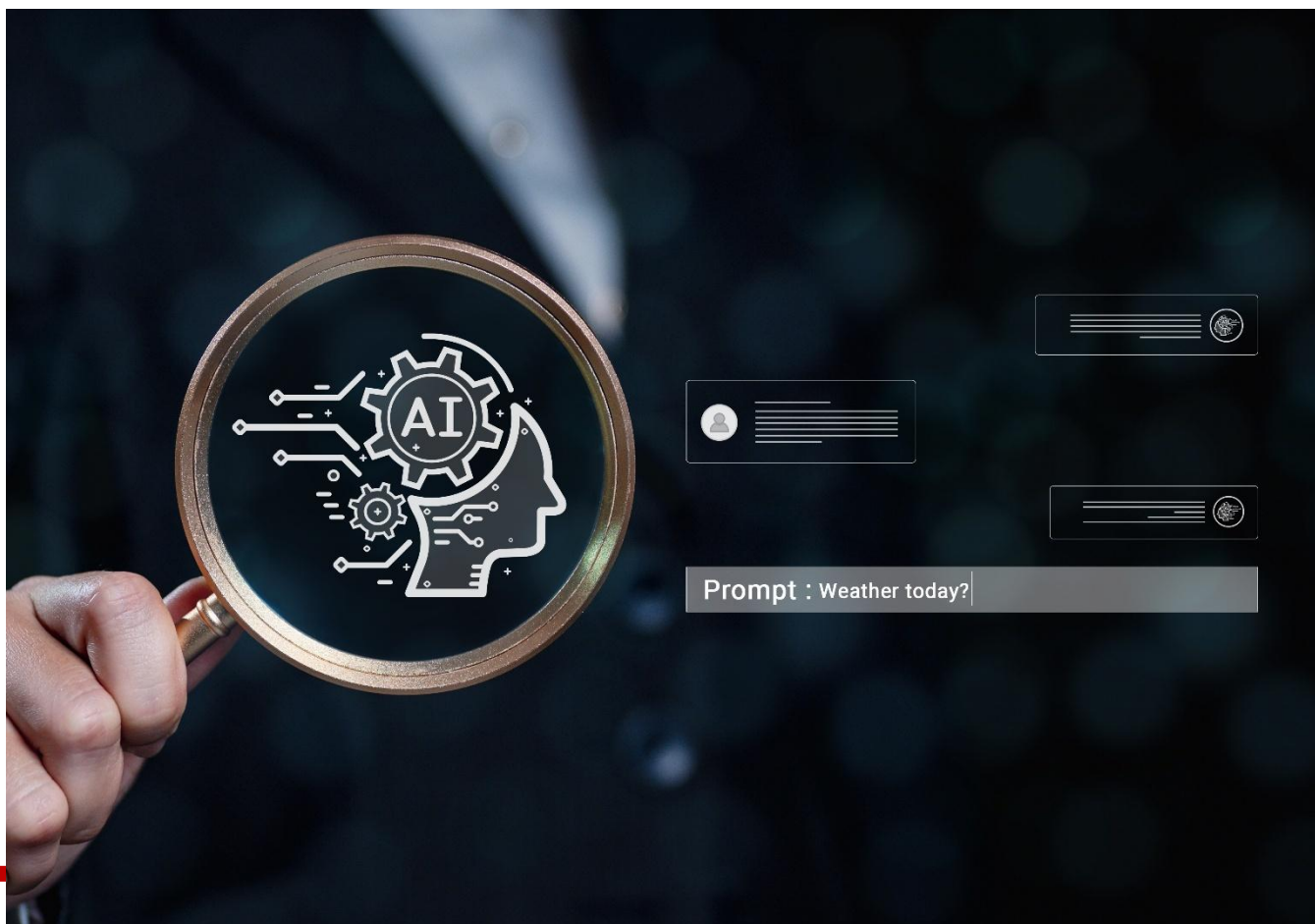
By focusing on these elements, cloud security startups can better position themselves for success in a rapidly evolving marketplace. New players need innovative go-to-market strategies that are efficient, cost-effective, and customer-focused. This approach may also help them build the trust and credibility needed to rise above the noise and establish themselves as reliable partners. Furthermore, startups should prioritize cultivating strong relationships with key industry influencers, analysts, and potential partners to amplify their reach and impact. A well-defined value proposition, combined with a proactive outreach strategy, can assist startups in differentiating themselves and attracting the attention of investors and customers.

About the Author

Allan Thompson brings more than 25 years of cybersecurity expertise to his role as Co-Founder, President, and Chief Executive Officer of AcceleTrex Corporation. In his long tenure as a senior executive for pre-IPO and early-stage companies on both U.S. coasts, Allan led teams in building next-generation product and service solutions that resulted in the multi-billion-dollar IPO with Trend Micro and multiple successful mergers that included IntruVert Networks (acquired by McAfee), Senforce (acquired by Novell), Reconnex (acquired by McAfee), DataGuise (acquired by PKWARE), RedSeal Networks (acquired by STG), and Zenedge (acquired by Oracle). Allan's executive expertise and grasp of cybersecurity challenges, strategies, and solutions positions AcceleTrex to rapidly scale transformative go-to-market strategies under his visionary yet pragmatic leadership.



Allan can be reached online at LinkedIn <https://www.linkedin.com/allangthompson> and at our company website www.acceletrex.com



Why CISOs Need an AI-Native Strategy

By Tom Tovar, CEO, Appdome

The CEO of Nokia, on the eve of being purchased by Microsoft, said “we didn’t do anything wrong but somehow, we lost.” These words describe the reality businesses face: embrace change or get left behind. The same is true for CISOs, particularly in the rapidly evolving AI economy.

The Roots of an AI-First Strategy in Cyber

Let’s look at the digital (r)evolutions that brought us to the AI economy. Each evolution brought benefits, including new efficiencies, capabilities, and competitive advantages. The underlying technologies also brought new security risks and threats:

- **Software & SaaS Era (1990s–2010s):** This period saw automation, increased productivity, and scalable cloud services. However, it also introduced large-scale data breaches, mobile malware, and new attack surfaces.

- **Cloud-Native Era (2010s–2020s):** The rise of cloud computing accelerated time to market and operational agility, while bringing API attacks, supply chain threats, and mobile fraud.
- **AI-Native Era (2020s–Present):** AI is booming, delivering the biggest impact yet. AI is revolutionizing decision-making, automation, and hyper-personalization. However, it is also fueling AI-powered fraud, deepfake scams, and automated cyberattacks.

Despite these shifts, cybersecurity remains stuck in the cloud-native and software era. Cyber functions have not yet declared 2025 to become AI-native – but they should.

AI-Native Threats are Real & Growing

AI introduces threats more sophisticated than ever. Some of the most pressing concerns include:

- **AI-Powered Cyberattacks:** Attackers use AI to automate social engineering scams, generate malware that adapts, and even mimic user behaviors for phishing campaigns.
- **Deepfake and Synthetic Fraud:** AI-generated deepfakes manipulate voice, video, and text to deceive facial recognition, trick executives, and spread disinformation.
- **Autonomous Hacking Tools:** AI-driven attack engines test for vulnerabilities, exploit them, and adapt faster than human attackers.
- **AI-Made Bias and Manipulation:** AI manipulates financial markets, spreads political propaganda, and interferes with decision-making through fake data.

Attackers have embraced AI as their weapon of choice. Defenders must do the same. AI-driven threats magnify existing risks, increasing attack speed, variety, and impact.

CISO's cannot afford to treat AI as an "LLM" or "data leakage" problem. To counteract AI-powered threats, cyber functions must embed AI into their core operations, using AI to code, build, measure, and mitigate threats in real time. They must embrace AI-native platforms to stay ahead of rapidly evolving threats.

The Big Difference with AI Threats

Unlike previous digital evolutions, AI is not just another attack surface—it is now the attack platform itself. In other words, *AI is the source of attack* more than it is the target. Secondly, cyber functions remain understaffed and rely on manual work and external teams to deliver defense. This dependency conflicts with the business teams that are racing to embrace AI.

Starting in 2025, cyber needs an AI-native strategy that includes:

- **Hyper Automation of Cyber Delivery:** Cyber teams rely on IT, DevOps, and external security vendors for implementation and enforcement – creating delays. AI-native solutions enable hyper automation, faster deployment and better control. They also extend security across mobile, VR and other digital spaces.
- **Pre-Emptive Threat Management:** AI already enhances fraud detection, but its true potential lies in preventing threats before they emerge. Manual defenses can't keep up with AI-driven

attacks. AI-native security automates threat detection, fraud prevention and real-time incident response.

- **Combating AI-Generated Threats:** Organizations must match the attacker's AI-driven assault. AI-native defense can protect every attack vector—users, apps, authentication, networks, and systems better and faster than any manual approach. Static defenses cannot keep pace. Security updates must occur at AI speed.
- **Eliminating Friction in SecOps & DevSecOps:** AI optimizes security workflows, reducing manual work, decision making, and validation. AI should fully automate security in software development and decision-making, compliance, detection, and response in production. Security must keep pace with AI adoption across the enterprise.

Final Thoughts: Don't Fight AI—Embrace AI

As cyber threats scale exponentially, cybersecurity teams across all functions must leverage AI's efficiency and adaptability. AI amplifies cyber threats, creating new attack vectors at unprecedented speed. Cyber teams that resist AI-Native defenses risk being outpaced by AI-driven adversaries, butting the business at substantial risk.

Cyber teams must move past AI and LLM risk evaluations and transition to AI-native cyber defense models. The lesson from Nokia's downfall is clear: move too slowly, and obsolescence is inevitable.

About the Author

Tom Tovar is the co-creator and CEO of Appdome – the industry's first platform to automate mobile app protection. A growth entrepreneur and technology leader, Tom has a passion for building products that dramatically improve life and work. At Appdome, his mission is to secure the mobile app economy from the ground up while pioneering a new era of DevSecOps platforms designed to deliver more protection with less work and protect mobile apps, mobile customers, and mobile businesses faster and easier for everyone. Tom can be reached at the Appdome company website, www.appdome.com.





Why Network Disaster Recovery Solutions Are a Non-negotiable for Modern Businesses

Implementing a reliable protocol to protect your services and operations

By Howard Simpson, CTO, CENTREL Solutions

Organizations worldwide rely on technology to function. By 2027, [global spending on digital transformation is projected to reach nearly \\$4 trillion](#), driven by remote working initiatives, international operations, and the continuing popularity of e-commerce.

While these advancements create new opportunities, they also introduce significant risks. Digital business tools require the same level of maintenance and protection as physical assets. Without proper safeguards, companies face devastating consequences, including data loss, operational paralysis, financial setbacks, or even reputational damage.

Fortunately, these risks can be significantly reduced by implementing a disaster recovery plan. A well-defined protocol ensures that in the event of a cyberattack, IT teams can swiftly restore systems and resume operations. In today's digital landscape, a failsafe mechanism is not optional—it's essential.

The high cost of inaction

The dangers of having a vulnerable network are twofold—both operational and reputational. Temporary server outages disrupt efficiency, frustrate clients and stakeholders, and, in severe cases, generate negative press. Security breaches can erode trust, deterring potential customers and damaging long-term business relationships.

Beyond the immediate impact, cyberattacks can have lasting consequences. In some cases, restoring systems to their original state can take weeks, months, or even years. Certain malware strains compromise the core of IT infrastructure, making recovery without a structured protocol an uphill battle that drains valuable resources.

If your company lacks a disaster recovery plan, chances are you already have existing IT practices that can serve as its foundation. Here are a few ways to ensure you can get your systems back up and running if disaster strikes.

IT documentation and automation

Most organizations maintain IT documentation to share internal knowledge, but its role in disaster recovery is often overlooked. Detailed filing enables teams to rebuild systems quickly, reducing downtime and minimizing disruption.

To ensure effectiveness, documentation must be continuously updated. The more precise and comprehensive the records, the faster IT teams can restore configurations, settings, and workflows. However, since IT and business professionals often prioritize troubleshooting, customer support, and daily operations, manual documentation can become an afterthought.

Automation is a powerful solution. By automating system information, businesses ensure they always have accurate, real-time information available. Automated failover mechanisms can further enhance resilience—if a system goes down, another seamlessly takes over, keeping operations running smoothly even in an IT professional's absence.

Key aspects of a disaster recovery plan

The first step for businesses that have not formalized disaster recovery protocols is conducting a **risk assessment**. Identifying potential vulnerabilities allows companies to strengthen their infrastructure proactively rather than reacting to threats after they occur. Risk assessments can also help detect unusual activity early, preventing minor issues from escalating into major disruptions.

Another critical element is **network segmentation**. Implementing a firewalled demilitarized zone (DMZ) isolates different parts of an IT environment, making it harder for external threats to penetrate core systems. If an attack compromises one section, segmentation prevents it from spreading across the entire network. This containment strategy ensures that repairs remain localized and manageable.

Additionally, businesses should establish clear **IT security policies**. These guidelines provide teams with a structured approach to cybersecurity, reducing the risk of breaches caused by human error or inconsistent security practices. If your company operates on-premises infrastructure, disaster recovery protocols should also account for physical risks such as hardware failures and environmental risks.

Why proactivity matters

Creating a disaster recovery plan is only the first step—regular testing and monitoring are crucial to ensuring its effectiveness. Simulating cyber incidents and assessing post-incident procedures help businesses identify weaknesses before real issues emerge. In cybersecurity, proactivity is always more cost-effective than reactivity.

A well-implemented disaster recovery strategy enables businesses to remain operational even when potential cyber threats arise. This not only saves time and resources but also maintains customer trust and satisfaction.

As organizations continue to expand their reliance on cloud and on-premises infrastructure, ongoing vigilance is key. By continuously monitoring and refining disaster recovery strategies, businesses can ensure long-term resilience and operational stability in an increasingly digital world.

About the Author

Howard Simpson is the CTO of CENTREL Solutions, where he has led innovation in IT documentation and automation since 2016. With expertise in technical architecture and software standards, he helps enterprises, MSPs, and public sector organizations enhance efficiency and security. Howard can be reached online on [LinkedIn](#) and through the CENTREL Solutions website <https://www.centrel-solutions.com/>





Why Scale Matters in Today's Cybersecurity Landscape Futureproofing for Better Outcomes

By Glen Williams, CEO, Cyberfort

In today's rapidly evolving and complex threat environment, the cybersecurity industry is reaching a point where scale, comprehensive capabilities, and agility have become essential for protecting businesses. Cyberfort's recent acquisition of ZDL Group demonstrates more than just business expansion - it points to a fundamental shift in how cybersecurity services must be delivered to meet today's demands and challenges.

The need for consolidating security services

The cybersecurity sector has always been known to operate fragmentedly; primarily due to the nature in which the industry has evolved. For example, as new digital technologies and platforms developed, more specialised security challenges emerged that required highly focused expertise. This led to a surge of niche providers with very specific deep technical knowledge including network security, endpoint protection, identity management, cloud security and so on.

While a specialised approach of course has its merits, it also creates significant challenges for businesses trying to maintain comprehensive security postures that cover all the security bases required through multiple vendor relationships. The result of this subsequent fragmentation does cause some problems in

terms of gaps in security measures between different providers. This in turn creates inconsistent security approaches for businesses whereby internal resources are drained by having to manage multiple security relationships - and maintaining visibility across the security landscape becomes increasingly difficult. Our strategic acquisition of ZDL Group directly addresses these challenges by creating a more comprehensive, end-to-end security ecosystem where clients can access multiple capabilities through one single, trusted relationship.

The scaling advantage

Scale in cybersecurity delivers advantages that smaller, more specialised providers can't match. Our expanded team of over 40 additional cybersecurity professionals from ZDL will bring diverse experience across sectors and different types of attack techniques, creating a powerful knowledge base that benefits our clients through broader threat intelligence.

By bringing together Cyberfort's existing strengths with ZDL's expertise in penetration testing, ethical hacking, and specialised training, we can now deliver seamlessly integrated security programmes to strengthen businesses overall security postures - rather than disconnected services. Greater scale also provides the resources to invest in developing proprietary security methodologies and platforms like ZDL's Vendor supply chain risk management solution, which will enhance our innovation capacity. The combined entity serves clients across borders while maintaining the agility and responsiveness that businesses need from their security partners, offering international reach with local expertise.

Looking to the future

As we integrate ZDL's capabilities and continue our strategic growth trajectory, we're focused on creating a new model for cybersecurity service delivery - one that combines the comprehensive capabilities traditionally associated with large global providers with the agility, innovation, and client focus that independent specialists are known for.

This hybrid model represents the future of cybersecurity services - scaled enough to deliver comprehensive protection but also agile enough to adapt quickly to emerging threats and evolving client needs which in today's landscape is ever-changing at pace.

By becoming one of the UK's largest independent cybersecurity providers, we're not just growing a business - we're reshaping how cybersecurity services are delivered to create more resilient businesses in an increasingly complex threat landscape.

The cybersecurity industry is consolidating for good reason. Scale, when properly leveraged, creates better security outcomes. Our acquisition of ZDL Group represents our commitment to leading this transformation for the benefit of our clients.

About the Author

Glen Williams the CEO of Cyberfort is responsible for leading the business, driving organic and inorganic growth and developing key customer relationships. Prior to joining Cyberfort he held CEO roles at North and Damovo. Earlier in his career, Glen was a senior leader at Dell, Computacenter and Lenovo.

Glen can be reached online via [LinkedIn](#) and at our company website <https://cyberfortgroup.com/>





How to Use Open-Source AI in Defense Tech: Cybersecurity Safeguards for Developers

By Yuliia Verhun, Technology & Business Lawyer, General Counsel for Tech Startups

There are multiple initiatives in the USA and European Union to regulate the Open-source AI use – from an ethics perspective to data safety. However, very little attention is being paid to the core – the open-source software component itself.

How does it interact with the proprietary software when embedded as an open-source library?

How are the open-source AI libraries built? Can we trust the training data, or should we double-check the sources? Where is the open-source AI software hosted? Has it been published through a reputable package repository, or is it sourced from platforms with a questionable security track record?

Defense Tech Perspective

For defense tech developers these questions are mission-critical. In today's environment of persistent cyber threats and compromised digital infrastructure, engineers aren't just building software. They are building real weapons to be used on a real battlefield. The [Preliminary Assessment from the Center for Strategic & International Studies \(CSIS\)](#) shows that 96% of the U.S. civil and military codebases are built using open-source software. And it's no different with general product development in the IT industry worldwide.

3 Starting Points for Open-Source AI in Defense Tech:

1. Open-source AI is still an open-source software

It means it's fully open like open-source software in general. Open foundation models provide public access to their architecture, allowing individuals and businesses to review, modify, and utilize them according to their licensing terms.

This openness fosters community which meticulously examines model weights, training data, and the inference code – all this simplifies maintenance and significantly lowers costs for business. The open foundation models can also be customized and incorporated into proprietary solutions.

2. Security & Legal Frameworks for open-source AI are still emerging

While security and legal approaches for traditional open-source software are well-established, the frameworks for open-source AI are only beginning to take shape.

And this is not about AI regulations. It stems from securing the core – the source code and its components, ways to interfere with and compromise them when embedded into proprietary products. The main question each engineer who works with open foundation models should ask themselves is, "What is inside? Is it secure?"

3. Defense Tech is built using open-source software and is now beginning to integrate open-source AI

With the rising popularity of open-source AI, the defense tech is standing at the intersection of cutting-edge innovation, cybersecurity, and heavily regulated governmental procurements. While it's crucial for all components to be transparent and open for state bodies as the end users, it must be balanced with uncompromising safety standards. This raises critical security considerations as the open-source AI safety approaches are more complicated to develop.

Open-Source Safety Initiatives: Applying Best Practices to Open-Source AI

During the last few years (2023-2024) there were multiple attempts from the U.S. information and security state agencies to gather feedback from the IT industry players and open-source community on their suggestions regarding open-source safety measures.

Key initiatives include [the Open Source Software Security Roadmap](#) (September 2023) from the Cybersecurity and Infrastructure Security Agency (CISA) and the [Request for Comment from the National Telecommunications and Information Administration \(NTIA\)](#) (October 30, 2023).

Both efforts focus on identifying and mitigating security risks in open-source software, helping government agencies distinguish between safe and potentially malicious components.

How defense tech developers can apply these findings to open-source AI:

- Developers should aim to check the open-source AI component's Software Bill of Materials (SBOMs) before using this component;
- Developers should integrate tools that generate Software Bill of Materials (SBOMs) during the build process, as these tools have deeper access to detailed and accurate data compared to analysing the artifact;
- Developers should trace and verify the open-source AI's dependencies provenance. Package repositories like [npm](#) and [GitHub](#) (for npm-based projects) offer dedicated tooling for this purpose.
- Developers should verify the package repositories' safety levels – if they at least require multi-factor authentication (MFA) and allow security researchers to report vulnerabilities – key criteria for Level 1 security maturity. [The Principles for Package Repository Security](#) should serve as a determining guideline while integrating the open-source AI components in defense tech proprietary products.

Change of Shift with Change of US Administration?

It may seem that the new U.S. Administration is shifting from the cautious open-source AI approach towards developing unlimited AI capabilities. However, a closer look suggests otherwise – not much has changed in the policy continuity. Trump Administration is doing the same as their predecessors in the White House – they have initiated a new [Request for Information \(RFI\)](#) to shape the U.S. AI Action Plan. They encourage the industry to provide their input on the AI policy ideas, and this is where we can learn from.

One of the most noteworthy industry responses to the RFI [comes from Open AI](#).

In their submission, the Open AI highlights the growing security risks imposed by non-democratic AI increase, which are strengthened with recent attempts from EU regulators to limit the scale of AI models development. These approaches influence the US AI policy and, according to the Open AI statement, hinder innovation.

One of the key takeaways defense tech developers can apply from this response is to verify the origin of the open-source software and the open foundation models they use. Some might indirectly derive from the Tier III countries (non-democratic PRC) and introduce elevated cybersecurity risks and national security concerns, particularly when it comes to defense tech applications.

This awareness is critical as governmental agencies are the largest customers in the defense tech field, and they cannot acquire compromised software components.

Another recommendation is to prioritize the implementation of cybersecurity, model weights security, and personnel security controls, which are likely to become the focus of coordinated global standards under emerging U.S. AI policy directions.

Conclusions

Open-source software often serves as the foundation for proprietary applications, and the defense tech industry is no exception. With the rising popularity of open-source AI, defense tech engineers are now leveraging these cutting-edge technologies to shape international security using new tools that remain relatively underexplored. This introduces unique challenges and risks that need careful attention.

The key policy makers – U.S. state defense agencies like [Cybersecurity and Infrastructure Security Agency's \(CISA\)](#), [National Telecommunications and Information Administration \(NTIA\)](#), and [the Office of Science and Technology Policy \(OSTP\)](#) are constantly gathering feedback from the industry for the insights on how to shape emerging open-source and open-source AI policies.

This is a great resource for the defense tech developers' education that should be prioritized by the businesses during the development cycle. Applying tools in development that generate the Software Bill of Materials and tracking the open-source AI's dependencies' provenance is a crucial first step for the defense tech applications' transparency and cyber safety.

About the Author

Yuliia Verhun is a technology & business lawyer from the IT industry. For over 10 years, Yuliia has been helping international startups with corporate structuring, operations, board governance, intellectual property & data protection in the EU, USA, and Middle East. As General Counsel, Yuliia led investment rounds for tech startups in the UAE and prepared Unichex – an EdTech SaaS platform serving over a million end users for large-scale public procurements in the U.S., and later, for a high-value M&A. These experiences reinforced her belief that transparent and secure software architecture is a strategic asset, consistently scrutinized during due diligence and procurement processes on the international stage. Yuliia is actively engaged in research at the intersection of open-source AI and cybersecurity, with a particular focus on applications in defense technology.



Yuliia Verhun can be reached online at yuliia@verhun.com, <https://www.linkedin.com/in/yuliia-verhun-general-counsel/> and at my company website: <https://generalcounsel.verhun.com/>.



Zero-Trust Architecture in the Era of Quantum Computing: A Proactive Defense Strategy

Navigating the Quantum Threat with Next-Gen Security

By Dinesh Besiahgari, FrontEnd Engineer II, Amazon Web Services

The cybersecurity world is on the brink of a revolution, driven by quantum computing. Quantum computers can also break the encryption systems we depend on daily while powering breakthroughs in medicine, artificial intelligence, and beyond. Organizations must adapt fast as traditional perimeter-based security becomes obsolete. Enter Zero Trust Architecture (ZTA), a proactive, resilient strategy, which is ready to defend digital ecosystems against the looming quantum threat.

The Quantum Threat: Breaking Cryptography as We Know It

Quantum computers are not only faster; they are a different kind of technology. Using quantum mechanics, they can solve some problems in seconds, which would take millions of years for classical computers. One alarming example is Shor's algorithm, which can break most modern cryptographic

protocols, including RSA and Elliptic Curve Cryptography (ECC). These algorithms protect everything from online banking to military communications and networks.

Experts predict that large-scale, fault-tolerant quantum computers that can run Shor's algorithm may appear within 10-15 years (according to the estimates of IBM and Google quantum teams). When that happens, the attackers will be able to decrypt the sensitive data, forge digital identities, and compromise critical infrastructure. The clock is ticking.

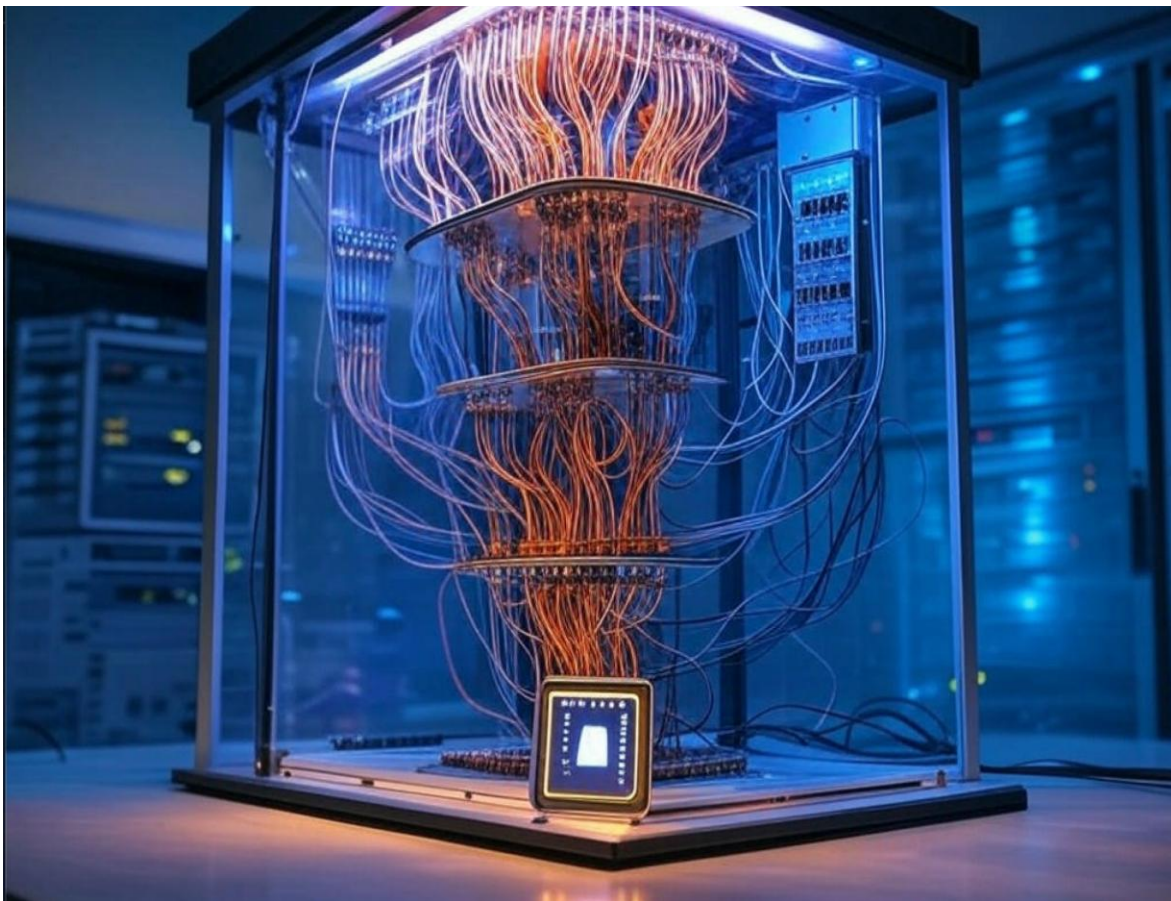


Fig. 1: Quantum Computing's Threat to Encryption

Why Zero-Trust Architecture Is the Answer

Conventional security postures are based on the assumption that everything within the network is secure, which is incorrect in the current environment. Zero-Trust Architecture changes this perspective with the help of a single principle: Never Trust, Always Verify. It means that every user, device, and application is considered a potential threat and requires confirmation of its good intentions.

Here's why ZTA stands out:

- **Least Privilege Access:** Only necessary rights are granted to users and devices. If a breach does occur, it is limited in scope.
- **Continuous Verification:** It is not a static process of trusting. It happens in real time using behavior analysis, device status, and others.
- **Micro-Segmentation:** The networks are segmented into separate compartments that prevent the attacker from moving freely throughout the network.
- **Encryption Everywhere:** The data is encrypted in the rest, in transit and in use – quantum or not, it is very difficult to crack.
- **Comprehensive Monitoring:** Real-time logging and analytics to identify anomalies before they become a crisis.

For instance, Google's BeyondCorp initiative, a real ZTA implementation, migrated security from network perimeter to device and user verification and successfully adapted to a cloud-first environment. It is not just a reduction of the attack surface; it is the creation of a quantum-ready fortress.



Fig. 2: Traditional Security vs. Zero-Trust Architecture

Quantum-Resistant Cryptography: The Perfect Partner

ZTA is powerful, but it is not the only solution. To respond fully to quantum threats, we need quantum-resistant cryptography – the algorithms intended for use against quantum attacks. The National Institute of Standards and Technology (NIST) is the leading body in standardizing options like these:

- **Lattice-Based Cryptography:** The cryptography based on complex lattice mathematics. CRYSTALS – Kyber (NIST selected) is one of them.
- **Hash-Based Cryptography:** Cryptography based on quantum-proof hash functions. SPHINCS+ is excellent.
- **Code Based Cryptography:** The security of this system is based on error correcting codes. As an example, McEliece has proved its effectiveness.
- **Multivariate Cryptography:** It solves complex equations. Rainbow is a notable scheme.
- **Isogeny-Based Cryptography:** It uses secure key exchange using elliptic curve isogenies.

These combined with ZTA provide a layered defense. Picture a cybersecurity onion: peel one layer, and another stands strong.

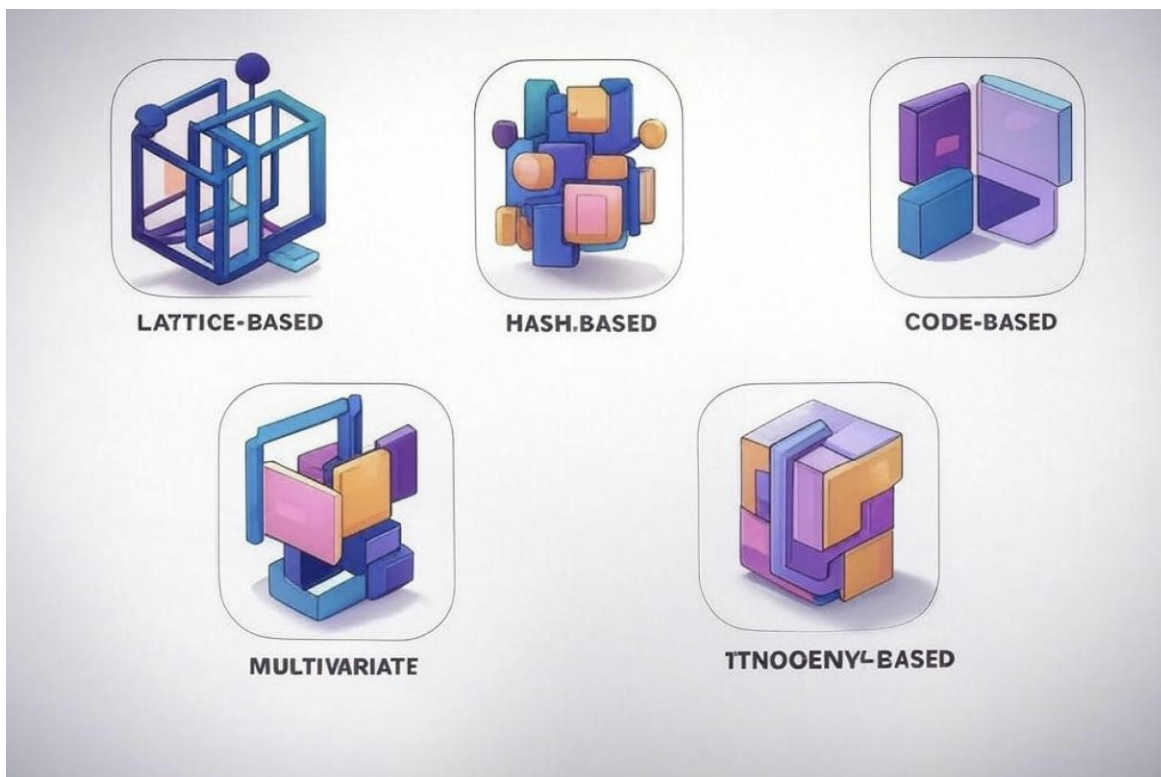


Fig. 3: Five Pillars of Quantum-Resistant Cryptography

Challenges on the Horizon

ZTA and quantum-resistant cryptography are not something that can be implemented easily. The challenges organizations encounter in the process are listed below:

- **Legacy Systems:** Many organizations are using outdated technologies that are incompatible with ZTA or new cryptography. For instance, a bank using 20-year-old mainframes would need a costly overhaul to integrate lattice-based encryption.
- **Performance Tradeoffs:** Some quantum-resistant algorithms like CRYSTALS-Kyber can increase the computational complexity that can slow down the systems or increase the operational costs.
- **Interoperability:** New systems must be compatible with the old ones and with the partners' setups without disrupting the business processes.
- **Cultural Resistance:** This is so because ZTA is a cultural shift. For instance, people who are used to the open network will not like the constant verification.
- **Evolving Threats:** Quantum tech is developing unexpectedly, which necessitates the need for organizations to be flexible.

However, the cost of doing nothing is greater than the cost of doing something. A single quantum breach could cripple a company or a country.



Fig. 4: Hurdles in Adopting Quantum-Ready Security

Collaboration: The Path Forward

No one faces this alone. This is where governments, industries and academia must come together. NIST's Post Quantum Cryptography Standardization Project is a perfect example of how it has brought together people from all over the world to build future proof defenses. They should begin now to identify vulnerabilities, implement ZTA pilots, and engage with peers.

The Future of Cybersecurity

Quantum computing is a two-edged sword: a great invention and a cyber threat. With the help of Zero-Trust Architecture and quantum-immune cryptography, organizations can defend themselves. The way is long, but the action should be taken now for the future. Ready to fortify your defenses? The quantum era waits for no one.

About the Author

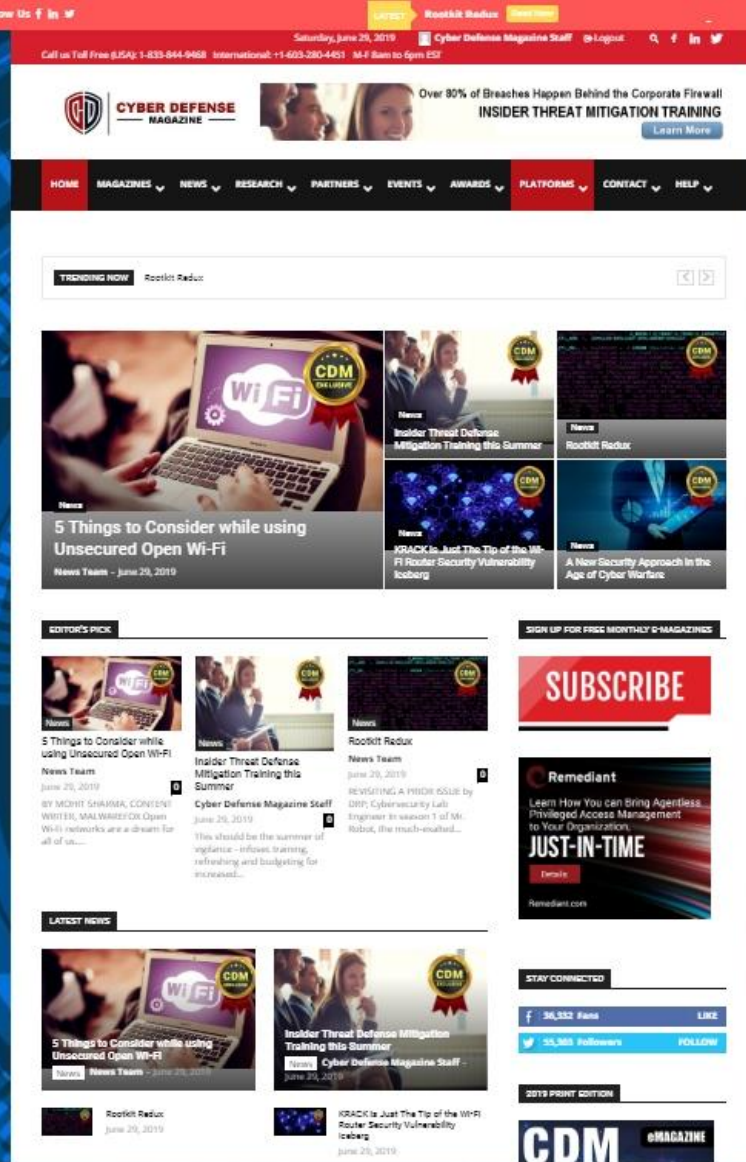
[Dinesh Besiahgari](#) is a Frontend Engineer II at Amazon Web Services, specializing in developing scalable, user-centric web applications. He has a strong background in AI, IoT, and machine learning, with multiple research papers published in IEEE, Springer and patents in advanced technologies. Dinesh's work has been featured in leading industry publications such as Forbes, Cybernews, PYMNTS and more. A global speaker and judge at prestigious tech events, he is widely recognized for his contributions through numerous awards. He is passionate about building secure, intelligent systems and AI-driven platforms that push the boundaries of innovation.

Dinesh can be reached at [Dinesh Besiahgari](#)



Award Winners





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...](https://www.amazon.com/dp/B075N1Y1Y1)

13 Years in The Making...

Thank You to our Loyal Subscribers!

We've Completely Rebuilt [CyberDefenseMagazine.com](https://www.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](https://www.CyberDefenseMagazine.com) up and running as an array of live mirror sites and our new B2C consumer magazine [CyberSecurityMagazine.com](https://www.CyberSecurityMagazine.com). *Millions of monthly readers and new platforms coming...starting with www.cyberdefenseconferences.com this month...*

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefenseemagazine.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



**ALWAYS FREE
NO STRINGS ATTACHED**

DIB Contractors:

**Nation-state and
ransomware actors are
targeting your data.**

We can help protect it.

**Get started -
nsa.gov/ccc**



FREE CYBERSECURITY SERVICES ARE AVAILABLE TO THE DIB
NSA CYBERSECURITY COLLABORATION CENTER



UNKNOWN
CYBER

"70% of Malware Infections Go Undetected by Antivirus..."

Not by us. We detect the unknowns.

www.unknowncyber.com



CYBER DEFENSE

MAGAZINE



www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefensenewswire.com
www.cyberdefensewebinars.com
www.cyberdefenseemagazine.com
www.cyberdefenseconferences.com



Together we secure. Join us at RSAC 2025 Conference!

Cybersecurity's greatest challenges demand more than one perspective. That's why RSAC 2025 unites thousands of voices from around the world to collaborate, innovate, and secure our digital future.

From April 28 – May 1 you'll hear groundbreaking Keynotes, explore hands-on sessions, and participate in exclusive networking opportunities, this is where the global cybersecurity community connects to share insights and find solutions.

Why Attend?

- Hear from top experts tackling today's toughest challenges in cybersecurity.
- Experience cutting-edge solutions at the expo that will drive your strategies forward.
- Collaborate with peers to unlock innovative solutions and gain fresh perspectives.
- Expand your network with professionals from every corner of the globe, forging connections that last a lifetime.

Be a part of something bigger. RSAC 2025: **Many Voices. One Community.**



*** with help from writers
and friends all over the Globe.**