CYBER DEFENSE
MAGAZINE

eMAGAZINE

NOVEMBER
2021

In This Edition

MORE INSIDE!

CONTENTS

@MILIEFSKY

From the

Publisher…

GLOBAL INFOSEC AWARDS NOW OPEN CYBER DEFENSE MAGAZINE 2022

We'll be celebrating our 10th Year in business and of our Global InfoSec Awards and as a Platinum Media Partner of RSA Conference on Feb 7 – 10, 2022 – See You There!

Dear Friends,

From my hawkeye view at the head of Cyber Defense Media Group (CDMG), every day I see the emergence of many trends and fact patterns. This month is no exception. But with these challenges, including Active Directory becoming the major target vector of exploiters, we see solutions like Attivo Networks and Cion Systems among others focusing on the proactive defense and hardening of Active Directory.

Suggestion: get a budget for "AD SECURITY" like your job and security posture depends on it. IAM is a target. Identities are GOLD to cybercriminals – like a golden ticket attack.

Among the opportunities CDMG offers is our currently active 10th Global Infosec Awards 2022, happening during the RSA Conference for 2022. It's our 10th year in business as well and we feel blessed and are so thankful to our partners, to the winners, leaders, vendors, product and service buyers, customers all whom share our belief that yes, we can get one step ahead of the next threat.

As always, among the valuable resources we rely on to respond to cyber threats are the providers of cybersecurity solutions; we commend your attention to the excellent group of articles in this month's Cyber Defense Magazine.

Wishing you all success in your own cyber endeavors.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS

CEO, Cyber Defense Media Group

Publisher, Cyber Defense Magazine

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

InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.

From the International Editor-in-Chief…

On the international front, we continue to see developments involving privacy regulations, ransomware developments, and criminals operating within jurisdictions which either deny their existence or refuse their extradition.

Unfortunately, the continuation of diverse and sometimes conflicting initiatives tends to drive us farther away from creating and adopting common solutions, and often sets up dynamics more favorable to threat actors than the societies and nations we seek to protect.

To some degree, the private sector may be encouraged to take the lead in breaking out of this impasse. As has been observed many times before, the imperatives of government differ fundamentally from those of industry. At the same time, it's interesting to note that some of the wider concerns for society appear to be gaining greater influence with private sector entities.

Some of those influences are positive and in the ordinary course of business; some are better understood as risk-averse, as in avoiding civil liability for lapses in cybersecurity practices.

The message remains clear, however, that the international implications for both government and business participants cannot ignore the importance of cybersecurity.

To our faithful readers, we thank you,

Pierluigi Paganini
International Editor-in-Chief

Pierluigi

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

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

INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

US EDITOR-IN-CHIEF
Yan Ross, JD
Yan.Ross@cyberdefensemediagroup.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

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

http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

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

9+ YEARS OF EXCELLENCE!

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

CYBERDEFENSEMEDIAGROUP.COM
MAGAZINE TV RADIO AWARDS
PROFESSIONALS VENTURES WEBINARS
CYBERSECURITYMAGAZINE (FOR CONSUMERS)

Welcome to CDM’s November 2021 Issue

From the U.S. Editor-in-Chief

As always, in this month’s issue of Cyber Defense Magazine, we are pleased to include a broad variety of excellent articles with actionable intelligence from highly knowledgeable cyber professionals.

Risk identification, attack prevention, and incident response form the bulk of this month’s articles, with contributions coming from domestic and international sources, as well as from public and private sector writers.

Not only do we see solutions to today’s recognized threats, but also projections of responses to attacks our expert writers perceive to be coming down the pike.

We continue to draw your attention to the 16 elements of our critical infrastructure, which are fast becoming the most targeted areas for cyber criminals. In my role as editor, I would reiterate my call to our readers to become familiar with the 16 areas of critical infrastructure designated by the Department of Homeland Security, found at www.dhs.gov . Going forward, activities in these areas will become more and more important in the world of cybersecurity.

In this November 2021 issue, we continue our tradition of making Cyber Defense Magazine most valuable to our readers by keeping current on emerging trends and solutions in the world of cybersecurity.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

Yan Ross
US Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

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

SPONSORS

THETA432™

Prepare Against Cyber Attacks!

With Dynamically Defined Defense™ (3D).

See If I Need Cyber Defense

Cyber Defense

Best-in-Class Cyber Defense Services, operated 24 / 7 by Industry-Leading Professionals from around the world.

IRAAS + TRU-A™

Incident Response as a Service provided by our dedicated world class Threat Operation Center.

Digital Forensics

You need answers into what happened and how to fix it. You want to know who accessed what, when and how.

Remote Monitoring

Our Threat Operation Center Provides Remote Monitoring and Response Services with dedicated Analysts at your side.

As seen in

THE WALL STREET JOURNAL.

abc NEWS

CIOReview

I.R.I.S.™
INCIDENT RESPONSE INVESTIGATION SYSTEMS

TRU-A
THREAT RESEARCH UNIT ALPHA

AI acquisition international
the voice of modern business - est. 2010

INFOSEC AWARDS
CYBER DEFENSE MAGAZINE
2020
THETA432™
BEYOND VISIBILITY™
Next Gen
Managed Prevention, Detection And Response Services (MPDRS)

INFOSEC AWARDS
CYBER DEFENSE MAGAZINE
2020
THETA432™
BEYOND VISIBILITY™
Cutting Edge
Cyber Defense Services

INFOSEC AWARDS
CYBER DEFENSE MAGAZINE
2020
THETA432™
BEYOND VISIBILITY™
Hot Company
Cyber Security Services

INFOSEC AWARDS
CYBER DEFENSE MAGAZINE
2020
THETA432™
BEYOND VISIBILITY™
Publisher's Choice
Cyber Threat Services

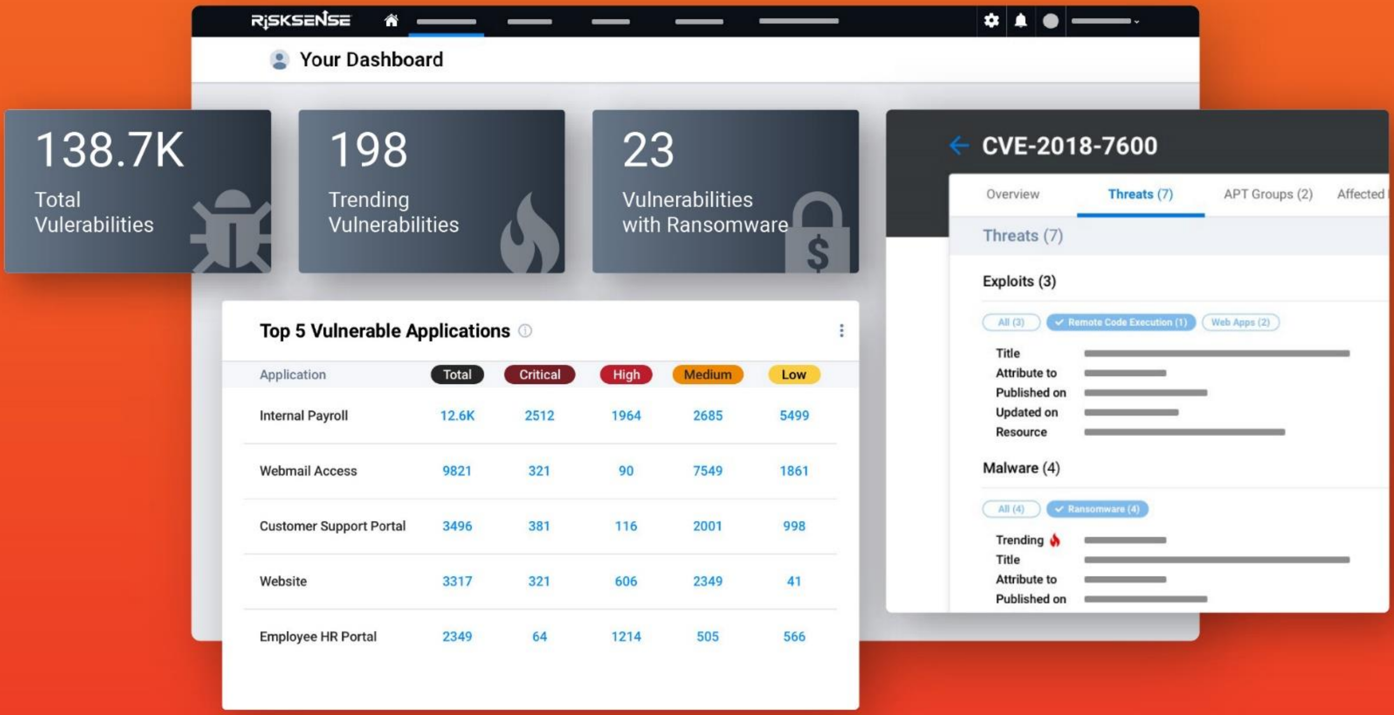
Your Fastest Response to Vulnerability Exposure

Full Spectrum Risk-Based Vulnerability Management

Vulnerability Intelligence
Active threats & ransomware

Vulnerability Prioritization
Clear directions for actions

Full-Stack Application Security
Code visiblity to risk



138.7K
Total Vulerabilities

198
Trending Vulnerabilities

23
Vulnerabilities with Ransomware

Top 5 Vulnerable Applications

Application	Total	Critical	High	Medium	Low
Internal Payroll	12.6K	2512	1964	2685	5499
Webmail Access	9821	321	90	7549	1861
Customer Support Portal	3496	381	116	2001	998
Website	3317	321	606	2349	41
Employee HR Portal	2349	64	1214	505	566

CVE-2018-7600

Threats (7)

Exploits (3)

Title
Attribute to
Published on
Updated on
Resource

Malware (4)

Trending
Title
Attribute to
Published on

Take a Proactive Stand Against Adversarial Risk

RiSKSENSE®

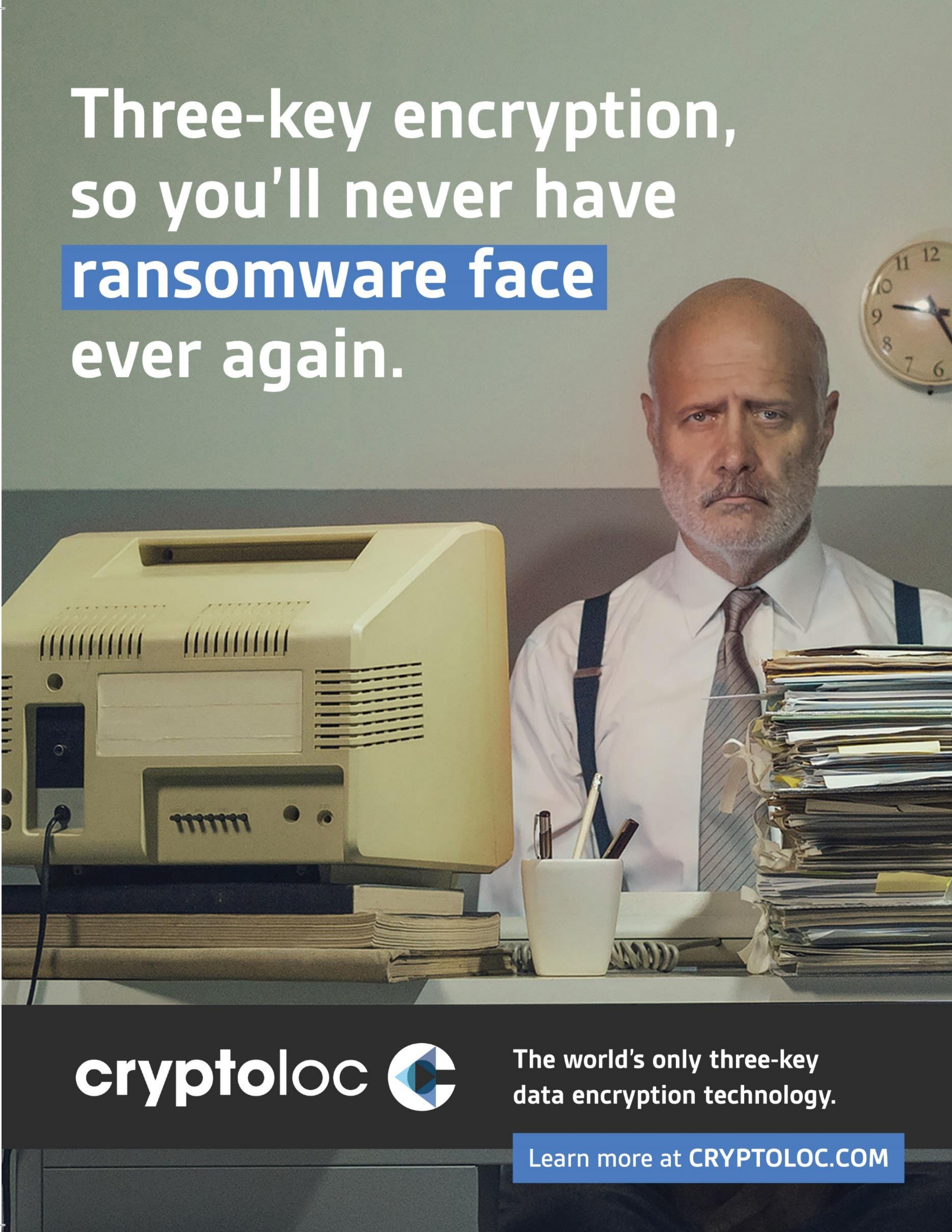
www.risksense.com

axiad

Passwordless Anywhere with **SMARTidentity**

Secure digital interactions for users and machines to keep your business moving forward

axiad.com

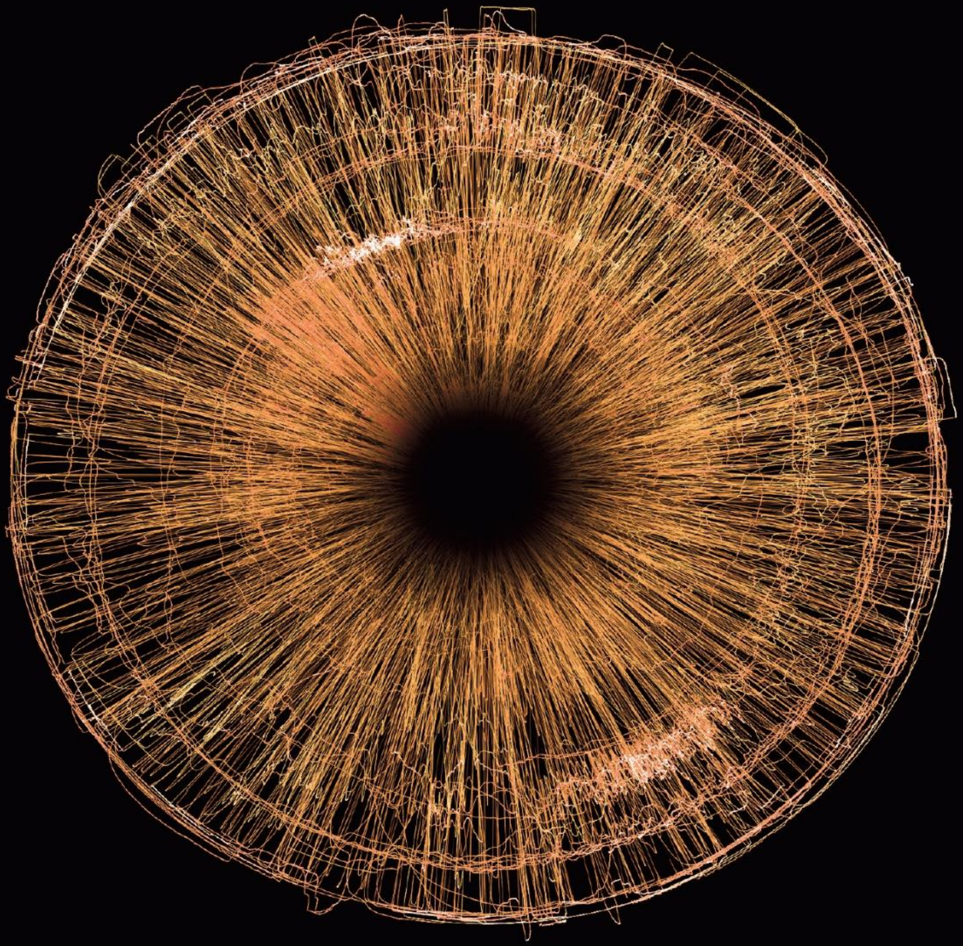

Three-key encryption, so you'll never have ransomware face ever again.
cryptoloc
The world's only three-key data encryption technology.
Learn more at CRYPTOLOC.COM
12
11
10
9
8
7
6

Things have changed. Difenda will help maximize your Microsoft security investments through technology consolidation and provide a modular approach to provide a clear view of your cybersecurity landscape through a single pane of glass.

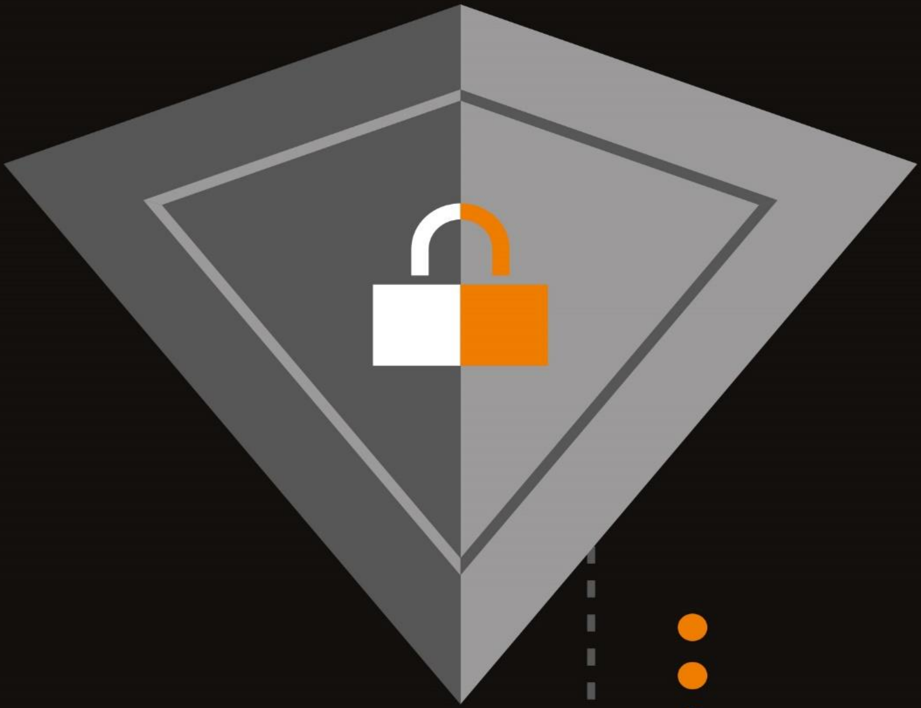
See the difference a personalized approach to cybersecurity makes work with a partner thats focused on you.

DIFENDA

CONTACT A DIFENDA SECURITY EXPERT TODAY



A NEW WAY TO KEEP YOUR SECRETS SAFE
CONTACTLESS
SECURE SHARING
IN YOUR POCKET
www.freemindtronic.com



FOCUS ON YOUR BUSINESS, NOT YOUR EMPLOYEES' CYBER HABITS.
CYBERSECURITY DONE RIGHT.
FluencySecurity.com
Fluency®

Do you check the boxes with your cybersecurity?

- ☑ **Leadership Prioritizes Cybersecurity**
- □ Assessments
- □ Plans
- □ Policies
- □ Procedures
- □ Training
- □ Education
- □ Testing
- □ Scanning
- □ Monitoring
- □ Response

Antivirus

Protects devices against known infections

Firewalls

Protects networks against unauthorized access

DEFENDIFY®

Cybersecurity. *Simplified.*

Protects organizations against diverse threat landscape

What's Your Cybersecurity Strength?

A+ A A- B+ B B- [✓ C+] C C- D+ D D- F

Find out in 3 minutes

www.defendify.io/mygrade

WORK ON THE FRONT LINES PROTECTING AMERICAN INTERESTS

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working to safeguard Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll find a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.

AFCivilianCareers.com/CYBER | #ItsACivilianThing

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.

AIR FORCE CIVILIAN SERVICE

Forces. Joined.

cythereal

Predictive Cyber Defense

Lucio Frega, Threat Researcher
Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

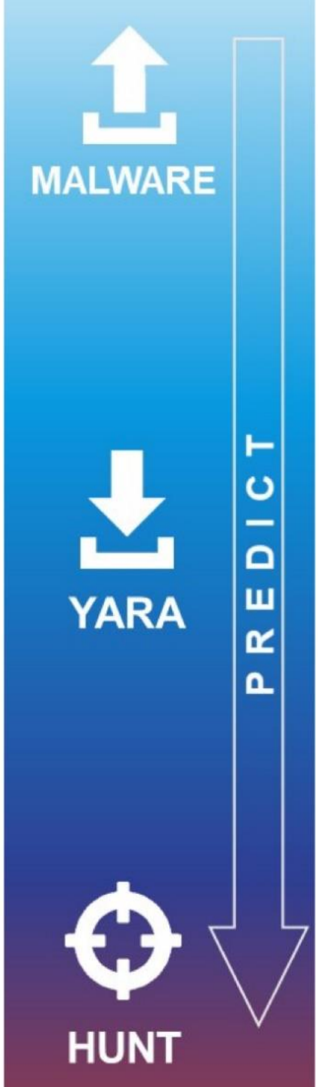
This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

About the Author/Disclosure

Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.



cythereal.com

Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011

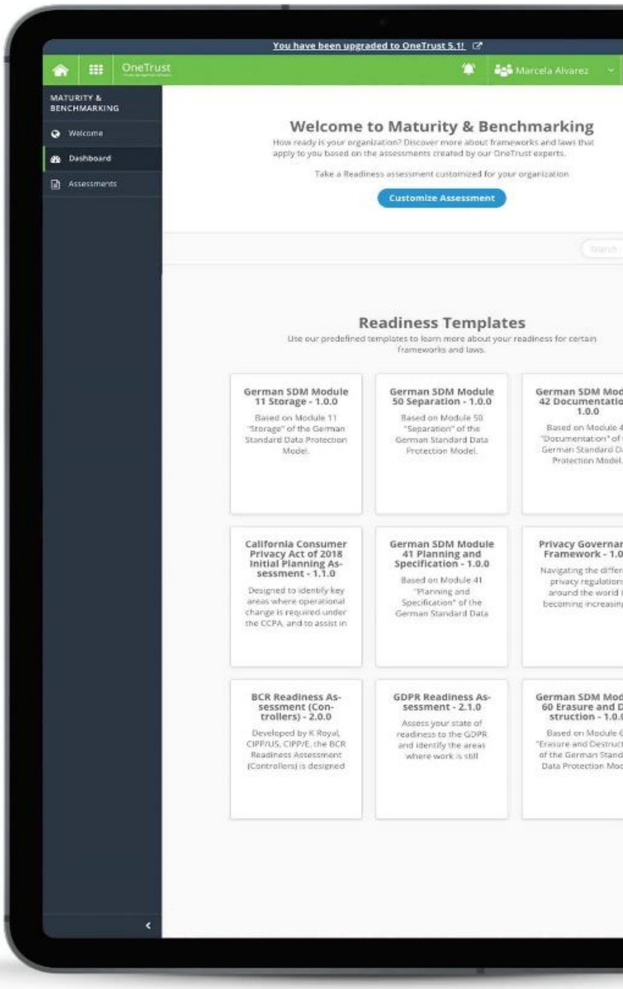
Founder & Managing Partner

SEAN DRAKE

***“At** Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. “*

Sean Drake
Managing Partner
Stony Lonesome Group LLC
203-247-2479 ☎
www.stonylonesomegroupllc.com 🌐

CISCO
Networking Academy



Welcome to Maturity & Benchmarking

How ready is your organization? Discover more about frameworks and laws that apply to you based on the assessments created by our OneTrust experts.

Take a Readiness assessment customized for your organization

Readiness Templates

Use our predefined templates to learn more about your readiness for certain frameworks and laws.

German SDM Module 11 Storage - 1.0.0
Based on Module 11 "Storage" of the German Standard Data Protection Model.

German SDM Module 50 Separation - 1.0.0
Based on Module 50 "Separation" of the German Standard Data Protection Model.

German SDM Mod 42 Documentatio 1.0.0
Based on Module 4 "Documentation" of German Standard D Protection Model.

California Consumer Privacy Act of 2018 Initial Planning Assessment - 1.1.0
Designed to identify key areas where operational change is required under the CCPA, and to assist in

German SDM Module 41 Planning and Specification - 1.0.0
Based on Module 41 "Planning and Specification" of the German Standard Data

Privacy Governan Framework - 1.0
Navigating the differ privacy regulation around the world becoming increasin

BCR Readiness Assessment (Controllers) - 2.0.0
Developed by K Royal, CIPP/US, CIPP/E, the BCR Readiness Assessment (Controllers) is designed

GDPR Readiness Assessment - 2.1.0
Assess your state of readiness to the GDPR and identify the areas where work is still

German SDM Mod 60 Erasure and D struction - 1.0.0
Based on Module 6 "Erasure and Destruct of the German Stand Data Protection Mod

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

ARTICLES

The Top 3 Cyber Security Mistakes and How to Avoid Them

As hacks become more common, organizations have no room for cybersecurity mistakes.

By Ivan Paynter, National Cybersecurity Specialist at ScanSource

Ransomware cost Americans an estimated $1.4 billion last year, and beyond high-profile hacks like the Kaseya and Colonial Pipeline breaches, cyber threats are more common than ever. As a result, businesses of all sizes are scrambling to learn more about cyber security and ensure that they have the proper measures in place to protect their operations. These are the top three considerations organizations must take into account when implementing or upgrading their cyber security approach.

1. People and Training

First and foremost, there is a significant lack of cybersecurity education among employees. The human firewall is the most important defense, but it is also the most vulnerable. That means security training has to be a top priority when it comes to an organization’s cyber security. Organizations should implement a security awareness training platform which trains, tests and scores all employees. It’s important to teach employees how to identify cyber security threats and remain vigilant toward anything suspicious, such as scams, fraudulent emails, or even physical threats. It’s also important to consider implementing some sort of email gateway filter. With the rise of remote working, additional problems emerge as more people go mobile. For example, it is much easier on mobile to mix company and private mail and people tend to click quickly, which leads to errors. We all need to slow down, verify incoming requests and be cognizant of what we are clicking on so that we do not fall victim to a cyber security threat.

2. Technology and System

It is also paramount that organizations ensure systems are fully patched, inclusive of their OS, firmware and applications. They must ensure each endpoint detection and response application is installed on each device, with all systems reporting back to a central location or Security Operation Center, where all notifications, events, and alarms can be correlated. A quality Detection and Response application is not only going to defend against malware and other malicious activity, but it will also identify possible insider threats by monitoring lateral traffic. Utilizing such Security SaaS should be part of the overarching security platform which will provide a level of behavioral analytics with the ability to determine what is standard for that user and/or system. Therefore, this allows organizations to identify unusual activity, even if the user has the rights to the systems being accessed.
Additionally, I would suggest V-LANs and least privilege access or even zero trust as a greater security play. For example, IoT devices should not cohabitate on the same V-LAN as the accounting or human resources department. This type of network segmentation allows for greater risk reduction.

3. Staffing and Security Operations

Many organizations forgo the managed services model to create an in-house security operation center, believing they can do it themselves. There are many cyber security tools available; however, there are very few trained and certified security engineers, and these tools often rely upon alarms, event notifications, or automated messaging to provide alerts. However, this begs the question, who will be monitoring and mitigating the environment at 3 a.m. on New Year's Eve? Effective cyber security infrastructure requires extensive resources to reduce the total volume of alerts, alarms and events to an actionable notification which requires mitigation. Vacation, training, sick time, education and retention programs are all factors to consider when creating a security operator center. There is a deficit of security analysts, engineers and architects throughout the cyber security space today. Even if you can hire a strong team of cyber security specialists, security operation centers require at least five to six people to ensure 24/7 coverage.

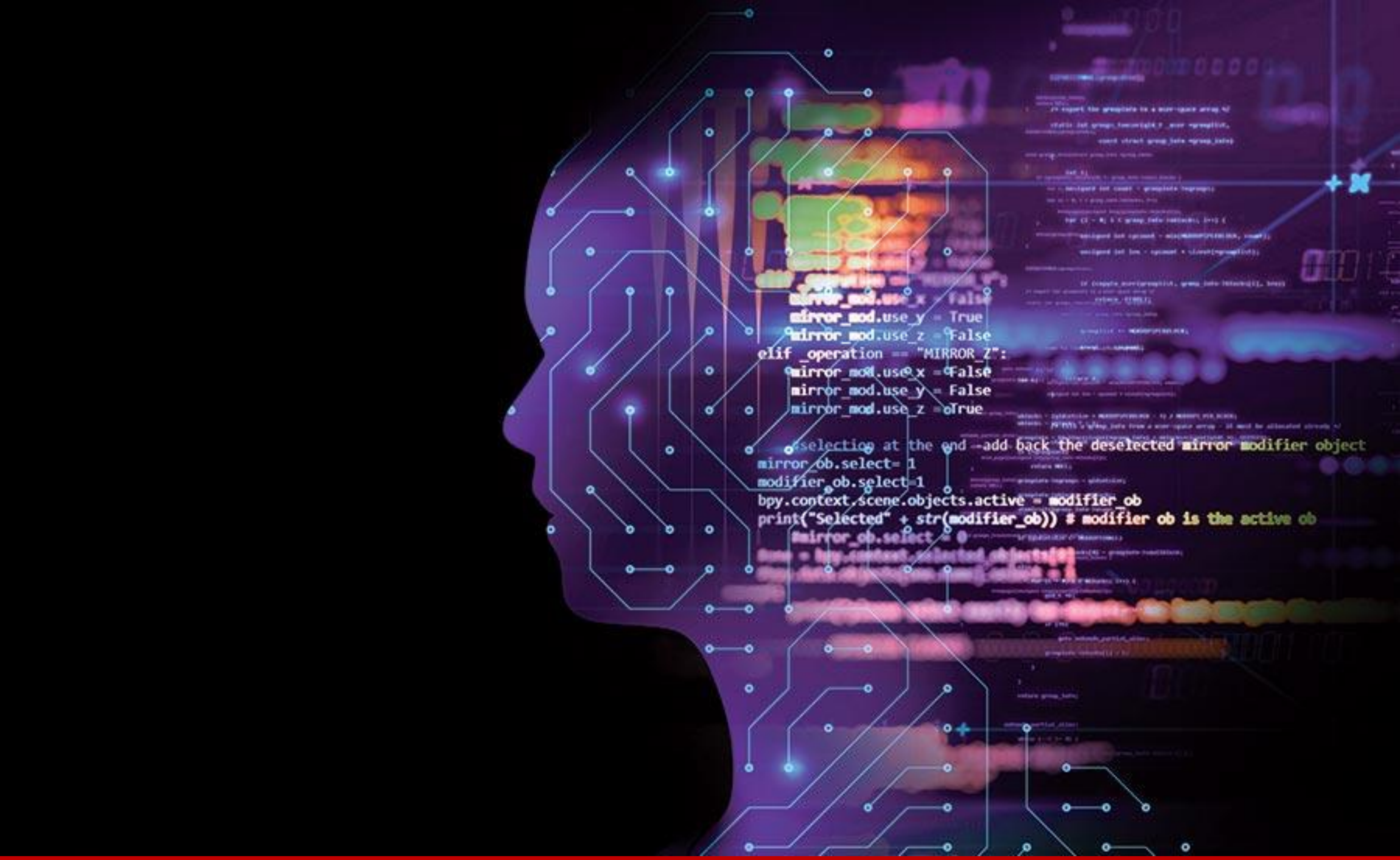
In addition to the personnel issues, there are also equipment, software updates and proper configuration to consider. True quality deployment will require multiple layers, and the systems will have to be integrated, monitored and managed. In comparison, an organization that outsources its cyber security needs can depend upon systems being maintained and a team of experts to support them. Simply put, organizations should secure their environment through a third-party managed security service. These services are inclusive of EDRs, patching systems, a security information event manager, behavioral analytics and east/west traffic monitoring. At best, with the current staffing shortage, an in-house SOC is an ineffective method to detect, quarantine and/or remediate an infected device and/or network.

Hackers are only becoming more sophisticated and, big or small, no organization can afford to go unprotected. Being aware of these three points is critical in protecting your organization from cyber threats. In the current cyber security environment, there is no room for mistakes.

About the Author

Ivan Paynter is the National Cyber Security Specialist of ScanSource and has over 30 years of experience in cyber security, working at Verizon and Masergy before coming to ScanSource in 2019.

Ivan can be reached online on LinkedIn and through ScanSource's company website https://www.scansource.com/


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob

NetOps Enhances Security

Growing numbers of network engineers turn to this IT mindset to address mounting concerns of network safety in an age of hybrid work and edge commuting

By Simon Pincus, VP of Engineering, Opengear

Today, NetOps (network operations) utilizes a combination of automation, virtualization and orchestration, to make networking operations and functions faster and more accessible. While the potential for greater productivity may seem to be the main pull for engineers to adopt the current NetOps iteration, more than four in ten (41%) network managers, network engineers and network architects say their organizations use NetOps to enhance network security. In fact, the top use for NetOps overall, according to new research spanning the U.K., the U.S., France and Germany is network security. The research also revealed that a growing number of network engineers are turning to NetOps, specifically, to bolster their network security.

Why Security?

Network engineers understand that without the network, conducting business isn't possible. A survey of 500 senior IT decision-makers found that security is key to avoiding network downtime. Although the shift to remote work and virtualization are partly to blame for the rise in costlier and more common network outages, the primary culprit for network downtime is that networks are becoming more layered, and as a result, more vulnerable. Software stacks must be updated more regularly, creating more opportunities for cyber-criminals to compromise systems. Moreover, with bad actors and external bots constantly probing corporate networks for weaknesses, there was a recent rise in unassuming employees falling victim to phishing attacks resulting in breaches and downtime.

Customers today expect uninterrupted network experiences, and because everything from leisure to work-related activities is dependent on a stable network connection, it is not an unreasonable expectation. The health of networks directly correlates to the health of businesses. Increasingly, organizations consider network resilience to be a necessity rather than an insurance policy. Security is a critical aspect of network resilience, or the ability to keep a network running during issues, ensuring business continuity. Whether at the core or on the edge of infrastructure, network resilience prevents disruptions to the customer experience from cyber-attacks.

The True Cost of a Poor Security Posture

Network engineers are leveraging NetOps because they know the true cost of a network outage is much more than the loss of revenue. According to the same survey of the 500 senior IT decision-makers, the three greatest impacts network outages have on their organizations included clear drops in customer satisfaction (41%), data loss (34%) and financial loss (31%). Additionally, 39% of companies revealed that it took more than a full day to restore network functions after an outage. Likewise, in 2020 alone, 31% of companies lost at least one million USD due to downtime. Downtime consequences are so severe that they could lead to an untimely disaster for a business.

Unsurprisingly, due to the heightened risk of outages and increases in cyber-attacks, 83% of network engineers put network resilience as their number one priority. And because network outages from cyber-attacks are a matter of when and not if – businesses can deploy NetOps to minimize the most damaging effects.

NetOps and Network Management

Network engineers use NetOps for its various benefits, from the standard day-to-day processes of keeping the network running to providing an alternative route to remediate the network when it goes down. Increasingly, NetOps is used to build and maintain a network that is automated, agile and available. Having this type of network is vital to protecting the production network from accidental misconfiguration or, more importantly, cyberattacks. Furthermore, all network configuration and management should be restricted to the core network operations team through an independent management plane, including an out-of-band network; this has led to the management plane being referred to as the network for network engineers.

Those organizations who use an independent secure management plane separate from the production network, such as an out-of-band network, noticed significant improvements to their security. Similarly, the businesses utilizing an independent management plane experienced fast remediation of devices and the heightened monitoring of their remote network. As stated early, security was central to reducing network downtime. For instance, 39% of respondents using an SD-WAN deployment from the same survey that observed the increase in adoption of NetOps amongst network engineers said that they use multi-layer security to avoid downtime. One in five (18%) of those surveyed indicated that they use end-to-end micro-segmentation and security zoning.

NetOps for Network Engineers

NetOps is fundamentally changing the role of the network engineer. With network teams having more locations to look after, more equipment to manage and more flowing data to oversee, the purpose of the network engineer had to grow exponentially to keep up. Now, using the tools and capabilities of NetOps, IT personal have evolved their role from one that was reliant upon manual process to a fully automated approach. Through automation, businesses can enhance their security and network monitoring while also accelerating their cloud adoption. As a result, organizations will decrease unwanted downtime and safeguard themselves financially and reputationally.

About the Author

Simon Pincus is responsible for the Opengear Engineering team, developing, releasing and maintaining all Opengear software and hardware products. He has over 28 years of experience in product management and product development roles. Prior to joining Opengear, Simon held senior management roles at CSG, Intec and ADC. He has worked in technology companies serving a variety of industries including Telecommunications and Customer Communication Centres. His passion is building engineering teams that develop products that delight customers, with the highest quality, usability and responsiveness to changing business needs. Simon holds a BSc (Hons) degree in Computer Science from the University of Queensland. Simon can be reached online at LinkedIn and at our company website https://opengear.com/.

Guntrader Data Breach: Victims Concerned Over Impact

By Aman Johal, Lawyer and Director, Your Lawyers

In July 2021, the details of over 111,000 Guntrader users – which included registered firearm owners - were leaked online after a cybersecurity breach affecting the Guntrader.co.uk website.

Guntrader, an online platform that allows farmers, landowners and shooting enthusiasts to buy or sell firearms online, reportedly attracts more than 350,000 visitors each month. Given the volume of visitors and the nature of the information they store and process, strong cybersecurity ought to be at the forefront of the company's mind.

Unfortunately, a wealth of sensitive information has been exposed. The personal information affected was incredibly detailed in some cases, including names, home addresses, postcodes, phone numbers, email addresses, IP addresses, and ID numbers, as well as details of the users' account creation date, last login dates and times, last login browser details, and even latitude and longitude coordinates of their last login.

Alarmingly, it has since been reported that victims' details have been published in a Google Earth-compatible format, specifically pinpointing their locations.

Sensitive data exposure and the serious and long-term impact

The information exposure could pose a serious, prolonged and direct risk for the victims. These individuals could now be targeted, and firearms owners affected by the breach, or anyone who has recently moved to an address previously linked to a gun owner, could also be at risk of being targeted by criminals.

Organised crime groups could target data breach victims, and affected firearm owners have been advised to be wary and ensure that they have sufficient home security deployed. However, individuals living in the previous addresses of gun owners may be unaware that they are even at risk, which is a further cause for concern.

The implications of this threat could have a significant and long term impact on the victims. It is common for data breach victims to suffer from distress caused by the loss of control of their personal information, and ruminating over risks and worries can lead to recognised and diagnosable conditions, such as anxiety and depression. Your Lawyers represents thousands of data breach victims, and many have required medical help to manage the impact of a data breach.

Serious data breaches like this are becoming increasingly frequent, and cybercriminals do target data controllers in charge of particularly sensitive information. It is clear to see how badly victims can be affected when such sensitive information is exposed.

In another recent example from September, the Ministry of Defence accidentally leaked the personal information of Afghan interpreters, with the email addresses of more than 250 Afghan interpreters who worked for British forces being erroneously shared. This group is already at heightened risk due to the political climate in Afghanistan, and the timing of this leak is alarming given the volatile situation there. Organisations need to take their data protection responsibilities seriously and understand, at all times, the real-life repercussions of information exposure.

Victims must demand accountability

People should not allow data breaches to go unpunished. Victims can take action with data breach compensation claims and by joining class action cases against the organisations responsible for large data breach incidents. Holding companies accountable is an important way to ensure best practice cybersecurity becomes commonplace in the future.

Given the severity of an incident like the Guntrader data breach, settlement pay-outs could be substantial. If enough people come forward to join the Your Lawyers Claimant Group, a Group Litigation Order (GLO) may be initiated unless the Defendant agrees to settle cases

Victims can be eligible to claim compensation on a No Win, No Fee basis by contacting Your Lawyers via its Data Leak Lawyers website here: https://www.dataleaklawyers.co.uk/start-your-claim

About the Author

Aman founded consumer action law firm Your Lawyers in 2006, and over the last decade he has grown Your Lawyers into a highly profitable litigation firm.

Your Lawyers is a firm which is determined to fight on behalf of Claimants and to pursue cases until the best possible outcomes are reached. They have been appointed Steering Committee positions by the High Court of Justice against big corporations like British Airways - the first GDPR GLO - as well as the Volkswagen diesel emissions scandal, which is set to be the biggest consumer action ever seen in England and Wales.

Aman has also has successfully recovered millions of pounds for a number of complex personal injury and clinical negligence claims through to settlement, including over £1.2m in damages for claimants in the PIP Breast Implant scandal. Aman has also been at the forefront of the new and developing area of law of compensation claims for breaches of the Data Protection Act, including the 56 Dean Street Clinic data leak and the Ticketmaster breach.

Aman can be reached via our company website https://www.dataleaklawyers.co.uk/start-your-claim

You've Been Attacked by Ransomware. How Will You Respond?

By Steve Schwartz, director of security, ECI

Earlier this year, a ransomware attack on the Colonial Pipeline led to a shutdown of 45% of the East Coast's fuel supply, 12,000 gas stations running dry and the highest gas costs in years. Five days and $4.4 million later, the pipeline was back up, with the CEO of the company acknowledging he authorized the ransom payment because executives weren't sure of the extent of the breach and how long it would take to restore operations.

He noted, “I will admit that I wasn't comfortable seeing money go out the door to people like this.”

Yet, it was all about business, and eerily, that's what it was for the perpetrators. Hackers from DarkSide were quick to make this point clear; the attack had nothing to do with a political agenda or social causes -- it was about money. Period. DarkSide not only carries out such attacks, it offers Ransomware-as-a-Service so aspiring cybercriminals can profit from doing the same. In fact, DarkSide provided assurance that moving forward they'd “check each company that our partners want to encrypt to avoid social consequences in the future.”

Sounds fairly professional, right? You bet it is. And that should worry a chief information officer (CIO), whether they're in investing, insurance or any industry where identifying, assessing and quantifying risk to the organization is essential. Businesses produce a wealth of data, and not only can downtime take a devastating financial toll and result in missed opportunities, a breach can ruin a corporate reputation and send customers for the door.

CIOs don't want that and hackers know it. Further, their perception is organizations must have the resources to pay huge demands, quickly, and their cybersecurity efforts are probably underfunded because corporate emphasis is placed on generating profit.

In their eyes, this all makes *your* company a prime target.

First things first

Yes, hackers know when they have a company over a barrel. So, how should you respond to a ransomware attack? What actions should you immediately take or avoid?

The immediate question for many leaders is should they pay the ransom at all? The knee jerk reaction is "no" in order to discourage extortion. But, the reality is, the pros and cons needs to be examined on a case by case basis. Operations must get back up and running ASAP, so nine times out of 10, paying a ransom is a straight business decision. After all, inaccessible data equals loss, and in a worst-case scenario, perhaps even the end of a company

There are two mistakes that often occur during response. Failure of personnel to immediately report the initial signs of an attack can enable ransomware to spread across systems and do even greater damage. This can be caused by an employee lacking understanding about what's happening, thinking they can rectify the situation and getting in over their heads or simply not wanting to admit there's an issue out of fear. The other mistake is turning off systems and possibly losing the ability to recover keys or thoroughly conduct a forensic investigation.

Some companies wonder if they should take matters into their own hands and look for decryption keys online. Once you've contained the malware, then you can search online or even try to get them directly from the locked system. With limited ransomware applications being written, there isn't a huge volume of keys out there, so it's possible to find them. Some groups use static keys, which are easily decrypted, others use asymmetric ones and key pairs, which are more difficult to crack. But it helps that hackers often re-use the same underlying code.

What are you going to do about it?

Today, it's not a matter of if you're going to be attacked, it's a matter of when. But there's plenty you can do to mitigate risk, including the following:

- Stop the bleeding: Segregate the system or systems from the networks so you can reduce the damage and keep other parts of your business running.

- Maintain backups: Be sure you regularly review backups of your data so that you can recover with as little loss as possible. If a full restore will take longer than you can tolerate, prioritize the data and applications to be restored in order of importance.

- Create and update response plans: These strategies should include such things as immediate containment tasks, chain of command, disaster recovery processes and more. Update these regularly whereas new threats are constantly emerging, personnel can leave key posts and infrastructure changes.

- Assess and test: Perform risk assessments and network penetration tests. This includes conducting table-top exercises so IT and executives can define and refine the response plan.

- Go phishing: Employees are often the way into a company's network, particularly now whereas remote workers often have lax security. Test them with fake phishing attempts and be sure to regularly conduct preventative training.

Fuel for thought

Some attacks I've seen have been investigated internally, but typically, these efforts don't include a forensic chain of custody that provides the chronological electronic evidence needed for a court of law. I make this distinction because I believe it's very difficult for a company to get all the data that they need in order to take legal action that may result from a ransomware or other type of attack.

If an organization uses a managed services provider (MSP) to get the cloud-based services they need, they likely won't need to hire a forensic investigator to delve deeper. For that matter, an MSP can defray a lot of costs, concerns and aggravation, particularly if they cater to industries that deal with financial and sensitive data. MSPs tend to have the best security in place, constantly invest in new technology and have experts versed in best practices and fast recovery. And, it doesn't hurt to have a team that can take a calm, collected approach during chaos.

The Colonial Pipeline attack has indeed given CIOs "fuel for thought." In a way, that's good, after all, the frequency of ransomware and other threats is on the rise. Your organization could be next – so be sure you're ready.

About the Author

Steve Schwartz, director of security, ECI.

Steve has spent more than 15 years in the cybersecurity industry with the past five at ECI. At ECI he helps clients understand the shifting cybersecurity landscape and to plan, prepare and respond for cyber-related events. Steve also works to bridge the gap between the business and the security priorities, helping organizations make sense of their investments.

Prior to joining ECI, Steve spent five years in the U.S. Navy onboard a submarine and has worked with several boutique consulting organizations in addition to S&P Global Markets and PwC. Steve's experiences primarily revolve around penetration testing and security assessments. He has worked with a variety of different security standards and frameworks and has multiple industry recognized certifications.

Steve can be reached online at Sschwartz@eci.com and at our company website ECI: Cloud, Digital Services and Cybersecurity Solutions

Digital Transformation Security: Guidelines for Success

By Yehudah Sunshine, Head of PR, odix

With the workforce going remote and IP existing almost exclusively in the digital domain enterprises, local and federal agencies, and SMBs alike are all striving to find the right digital blend to meet their industry transformation needs.

Supercharged by the Covid-19 pandemic, businesses in all sectors have been increasingly demanded to 'digital transform' and somehow mitigate all the evolving risks and regulatory expectations they face in the cyber battlefield. While the drive towards digital transformations has now become commonplace, its tangible achievements may be difficult to be seen.

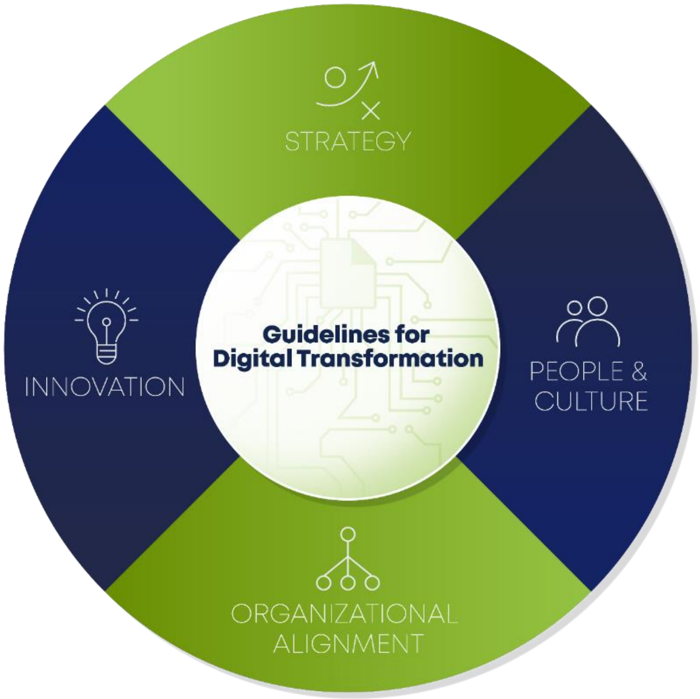
From incorporating innovative technology and security protocols to protect their assets, digital transformation is the process of optimizing new and existing technologies, fluid ways of thinking, and automation heavy processes to mitigate human error and cyber risk.

What is a Digital Transformation?

For many, digital transformations mark a critical readdress of how their organization manages technology, process, and most importantly the individuals responsible for integrating new business models and new revenue streams. The end goal of all of these is drastically alter driven customer expectations around products and services, changing brand image and technical capacity in the process.

For those who operate in traditional goods, this transformation entails building digital products, such as a mobile application or an e-commerce platform.

What does it take to reach digital transformation?



According to McKinsey, regardless of the public push towards digital transformation very few have achieved this goal. “Years of research on transformations has shown that the success rate for these efforts is consistently low: less than 30 percent succeed. This year’s results suggest that digital transformations are even more difficult with Only 16 percent of respondents say their organizations’ digital transformations have successfully improved performance and equip them to sustain changes in the long term.”

Talk is cheap. In practice, top-down directives only achieve their aims if the process is well defined, and the objectives are clear. In the case of digital transformation, this means compartmentalizing which segments stand to gain the most through digitalization and defining the core technologies and vendors whose implementation meets a strategic need.

When the partners and solutions have been identified, the organization are then positioned to set realistic short-term and long-term goals to determine success based on predefined KPI.

Importance of security layers within Digital Transformation

Ingraining security capabilities at every step of the digital transformation is the key to mitigating cyber risks in the future. Just like you wouldn't build a house and then add the plumbing and electrical after the fact when building towards digital transformation, organizations must focus on the technologies, cybersecurity education, and industry best IT practices that lay the groundwork for cybersecurity from square one.

From implementing encryption and mandatory policies on prohibited email attachments to offering regular training sessions and focusing on skills-based approaches vs fear-mongering, the digital transformation process can result in a higher level of security systemwide.

Metrics for success?

Effectively integrating new technologies, innovative processes, and industry best protocols takes time, money and a qualified staff of well-trained employees to do it right.

Digital transformation is not like a boxing match. While they both are hard-fought battles, only one gets the privilege of being judged by an outside panel of experts with a clear winner crowned at the end.

For digital transformation, measures of success may not be as clear cut as a knockdown, but they can be as straightforward as:

- Ensuring HR is attracting and hiring top technical talent
- Identifying % of processes designed for the cloud
- Comparing year on year operational improvements

The name of the game in analyzing your KPI is to keep them simple, easy to gauge on a year-to-year basis, and directly linked to business productivity.

Guidelines for success

Realizing an effective digital transformation strategy involves tough choices, and long hours implementing new technology but more importantly ensuring buy-in from strategic partners across the organization.

Through clear vision and careful planning, the digital transformation process will be difficult to implement but more than pay dividends in the value it achieves and security it assures to organizations of any size.

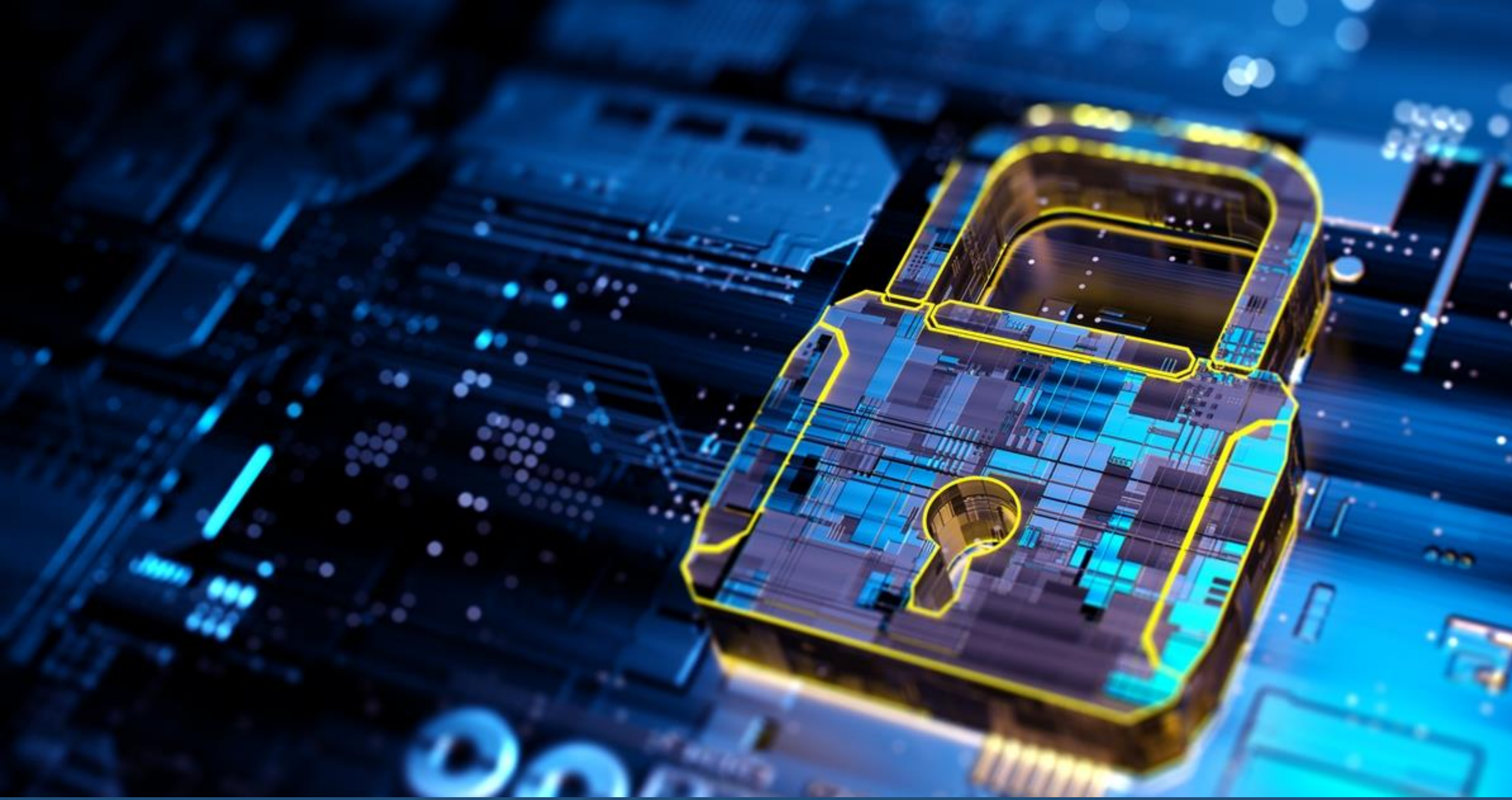
Ensuring a secure digital transformation can most directly be tied to:

- Capacity building for the future workforce
- Implementing and updating day to day tools and processes
- Investing in staff education to manage and optimize new technology
- Demanding leadership prioritize and implement best-in-class technology to streamlines workflows and decrease human error.

About the Author

Yehudah Sunshine Head of PR at Odix

Bringing together his diverse professional cyber know-how, intellectual fascination with history and culture, and eclectic academic background focusing on diplomacy and the cultures of Central Asia, Yehudah Sunshine keenly blends his deep understanding of the global tech ecosystem with a nuanced worldview of the underlying socio-economic and political forces which drive policy and impact innovation in the cyber sectors. Yehudah's current work focuses on how to create and enhance marketing strategies and cyber driven thought leadership for odix (www.odi-x.com), an Israel-based cybersecurity start-up. Sunshine has written and researched extensively within cybersecurity, the service sectors, international criminal accountability, Israel's economy, Israeli diplomatic inroads, Israeli innovation and technology, and Chinese economic policy.



Why The Integration of Netops And Secops Is Here To Stay

By Eileen Haggerty, Sr. Director, Enterprise Business Operations, NETSCOUT

The pandemic accelerated digital transformation and increased organizations' reliance on cloud services, VPNs, and other solutions designed to support remote work. These changes have redefined, if not destroyed, the idea of the traditional security perimeter.

At the same time, the pandemic led to a massive increase in DDoS attacks and ransomware attacks. Globally, 2020 saw more than 10 million DDoS attacks, the most ever, with a record-setting 929,000 attacks in a single month that year. Furthermore, attacks against remote workers have increased through the pandemic as employees have left the safety of their corporate networks, leaving security teams stretched thin.

In another survey, three fourths of financial institutions reported greater cybercrime during the pandemic, with many (42%) expressing concern that the work from home model made them less secure. Survey analysis showed that education institutions also faced 80 million assaults in the first half of 2021. And bad actors frequently targeted hospitals and healthcare organizations, through Internet of Things devices like tablets and smart beds, as well as via wholesale network shutdowns with malware and ransomware attacks.

At many organizations, these events served as a catalyst to closer cooperation between the network operations (NetOps) and security operations (SecOps) teams, deepening collaborative relationships that had already been formalized, and initiating collaborations where silos had existed in the past.

Now, many IT executives are considering how these teams could be structured to work more closely together for the long-term.

A Historical Failure to Collaborate

To understand the benefits of closer collaboration, let's start by examining the state of NetOps and SecOps collaboration just before the beginning of the pandemic.

In EMA's Network Management Megatrends 2020 survey, although 78% of companies reported formal collaborations, only 47% reported that they fully converged to the extent of sharing tools and processes. At 31% of companies, the collaboration involved some integration of tools, but at 16% of companies, the collaboration was strictly ad-hoc. Small and mid-sized companies were the most likely to report high levels of integration.

In practice, 35% percent of network operations teams said security system problems, such as bad policies and device failures, had led to complex and difficult-to-troubleshoot service performance issues. Another 35% reported incidents that originally presented themselves as complex service performance problems that later required cross-silo collaboration.

Add a pandemic to that recipe and it's easy to see why so many organizations struggled with supporting and securing millions of remote workers early in the pandemic. Given that network performance and security issues often go hand-in-hand, organizations with low levels of collaboration had fewer avenues to communicate and diagnose the root causes of issues, which likely led to longer than necessary disruptions.

In response, with security teams stretched thin, it was often networking professionals who filled the void to manage the complex challenges introduced by organization-wide extended remote work. After all, they already understood much of the underlying infrastructure -- and brought their own perspective to play when collaborating with security teams.

By working together, NetOps and SecOps teams gained increased visibility, quickened time to remediation of network and security issues, and reduced security risk.

Fostering Cooperation for the Long Haul

The conditions — a faster pace of digital transformation, the continuation of the hybrid workforce, and an expanded threat environment — will endure for the foreseeable future. So how can IT executives foster and maintain better collaboration and (hopefully) integration? The answer is especially important at large organizations, where siloed operations are likely to persist. There are a few steps to put in practice, specifically:

- **Begin at the design stage:** NetSecOps collaboration tends to center on infrastructure and deployment, while incident monitoring and response are secondary. As digital transformation continues to introduce new features into the IT environment, it's critical that communications between the teams are delivered early and natively.
- **Find a single source for truth:** Collaboration demands that everyone has equal access to current, relevant network data. Too often, this isn't the case because information shared across silos is outdated or irrelevant. If one team has too many blind spots, they can't partner effectively.
- **Establish a common toolset:** Performance management tools can help analysts understand how a security incident affects performance and vice-versa. Network automation and orchestration tools also benefit from collaboration as they allow enterprises to make quick changes to the network in response to a security event.
- **Formalize the collaboration:** Cooperation between NetOps and SecOps requires ongoing management that documents processes, identifies challenges, improves where necessary and borrows from best practices where relevant. Executive input needs to make sure the teams don't drift apart and recreate silos again.

Building on Pandemic Successes

The successes of collaboration over the past year have proven the advantages of having NetOps and SecOps teams work more closely together. In short, the more integrated the tools and processes used between them, the more successful they can be. But if left to stray apart, organizational silos can pop right back up. For closer collaboration between NetOps and SecOps teams to stick, IT managers must be vigilant in ensuring collaboration remains a priority even after the pandemic subsides.

The current environment, and the future one, will require these integrations to expand. Working together, an integrated NetSecOps team can achieve results greater than the sum of their parts: better network performance, increased security, and faster incident response.

About the Author

As Senior Director of Enterprise Business Operations, Eileen is responsible for working with enterprise customers to ensure that NETSCOUT's service assurance and cybersecurity solutions are meeting the needs of NETSCOUT's customers and the market. Eileen has worked for NETSCOUT for nearly 20 years, where she has held several product management and marketing roles. Prior to joining NETSCOUT, Eileen leveraged her MBA from Boston College working in a variety of technical marketing roles at Motorola Codex, Racal Data Group and Celox Networks. Our company website https://www.netscout.com/

What To Know to Fight Against Cyber Attacks

By Gergo Varga, Senior Content Manager / Evangelist at SEON

Cyber attacks have become a part of our reality, not only that we are all constantly getting phishing emails, but you can read about some cyber attack or data breach happening on a daily basis. Some of the attacks are concentrated on large businesses like Volkswagen & Audi or tech giants like Twitch, Facebook, Linkedin, but the truth is that nobody is safe. By October of 2021, according to Fortune's research, there had been nearly 281.5 million people affected by some sort of data breach. That means that there is a high chance that you and your business will be affected by some type of cyber attack, unless you start being proactive and fight against it.

How to protect yourself from cyber attacks?

The only way to effectively fight back against cyber attacks is by implementing a cyber security plan which includes various tools and policies that make it impenetrable. Let us introduce you to everything you need to know to fight against cyber attacks and how to implement it in your cyber security plan.

Implement device fingerprinting

One of the tools that should be added to any security is device fingerprinting. In short, device fingerprinting is a process of collecting and analysing different variables of users' devices like its software and hardware configurations to create a unique user profile. SEON's view on device fingerprinting, shows us how crucial it can be in fighting against cyber attacks. By creating a unique profile or device fingerprint for each user you can recognize when some of the variables change and confirm if it is a legitimate change in user details or suspicious behaviour. This way you can stop the fraud attempt before it even happens.Use multi-factor authentication

This is a great tool to use to provide an extra layer of security, especially when used together with device fingerprinting. It asks users to provide extra verification before giving them access to their accounts, like a special code being sent to the user's device. This can come especially handy if there is a difference in users device fingerprint, as it can confirm if they are legitimate users or if they are attempting an account takeover.

Train your employees

Your employees are the most important element of your business, and also its biggest security risk. Most of the cyber attacks will try to use the human element of the business in order to get access to confidential data like their credentials, bank account details, or even intellectual property. This is why it is extremely important to educate your employees about what are the cyber threats and risks, how to recognize them, and how to fight against them. Report to cyber threats from Netwrix, explains that 58% of all organizations claimed that their employees do not follow cyber security guidelines. Truth is that if you are not proactive about the fight against cyber attacks, neither will your employees be, regardless of your guidelines, especially if nobody is enforcing them. This is why it is extremely important to have a clear and easy to understand cyber security policy and to keep your employees informed about emerging threats.

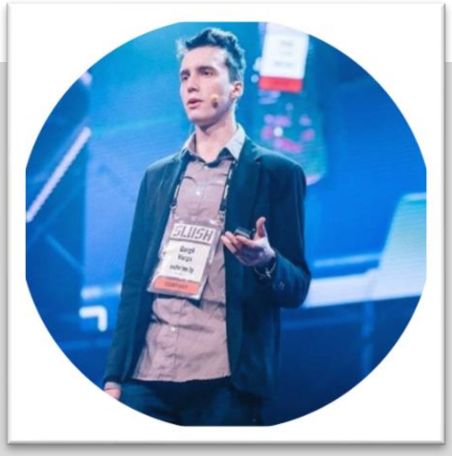
Introduce the password policy

This step might seem small, but it can make an enormous difference in your cyber security plan. Did you know that 81% of hacking-related breaches happened due to stolen and/or weak passwords? Considering that a large number of people use either the same or similar passwords for all of their accounts, one breach can cause a domino effect and put all of the other accounts in danger. Introducing password policy for your employees and also your users can significantly reduce the risk of data breach.

Update software and systems regularly

Cyber criminals will exploit all the weaknesses they can to gain access to your confidential data, and by not updating software and systems you are opening doors wide open for them. This is at the same time the easiest and one of the most important elements of your cyber security plan as it stops cyber criminals before they can even access your network.

It is difficult to know where to start when it comes to fighting against cyber attacks, especially because new threats are emerging every day. By implementing these steps into your cyber security plan, you will set your business on the right path in the fight against cyber attacks.



About the Author

Gergo Varga, Senior Content Manager / Evangelist at SEON. He has been fighting online fraud since 2009 at various companies - even co-founding his own one, enbrite.ly. He's the author of the Fraud Prevention Guide for Dummies - SEON Special edition. He currently works as the Senior Content Manager / Evangelist at SEON, using his industry knowledge to keep marketing sharp, communicating between the different departments to understand what's happening on the frontlines of fraud detection. He lives in Budapest, Hungary, and is an avid reader of philosophy and history.

Gergo can be reached via Our company website https://seon.io/

Five Cloud Telephony Security Vulnerabilities that Can Threaten Your Business

Five Cloud Telephony Security Vulnerabilities That Can Threaten Your Business

The Flip Side of Using Cloud Telephony Services

By Sujan Thapaliya, CEO and Co-Founder, KrispCall

It is evident that VoIP will be the future of business communications. Historically, it has been difficult to predict whether a call would be reliably forwarded over the internet, but that problem is mostly gone now.

The versatility and adaptability of today's VoIP platforms allow them to beat traditional landlines in competition. Additionally, they can be configured within minutes, and they come at a significantly lower cost than typical phone setup and maintenance. It's not surprising that more than 60% of businesses have already migrated to VoIP from landlines.

There are many benefits associated with VoIP phone systems. From affordability to increased functionality, VoIP systems have become more popular because they make businesses run more smoothly and efficiently than traditional phone systems, which is why they have gained such popularity.

While all of these benefits are important, one of the biggest downfalls of the technology is its lack of security.

It's like a phone setup with calls not connected via a traditional phone line but rather over the internet. All internet-connected devices are exposed to hacking, which leaves them at least somewhat vulnerable. Therefore, your VoIP system is less important than your internet network when it comes to security.

Importance of VoIP Security

Are VoIP security concerns really as important as you think they are? The reality is that security breaches via phone systems present a pretty serious threat to everyone, even if you've never been a victim yourself.

More than half of businesses in 2018 had their phone numbers hacked through social engineering, a type of scam that disguises itself as a real call to obtain valuable information. In the year 2020, several well-known Twitter accounts were used to promote a cryptocurrency scam that amassed hundreds of thousands of dollars. Among the users were Barack Obama, Kim Kardashian, and Bill Gates.

VoIP security is crucial and cannot be overstated. Furthermore, VoIP technology relies on the web to make calls, so it is susceptible to attacks that target the web. A lax VoIP provider could leave your business open to serious security risks since 24% of Wi-Fi networks in the world lack encryption.

The situation actually deteriorates. The US is not ahead of the worldwide average when it comes to Wi-Fi networks without encryption, as 25% of all networks lack encryption worldwide. Especially if your business is based in Europe, the chances are very high (34% - 44%) that your network is not encrypted, so you should really pick a VoIP company like Krispcall that follows best practices.

Cloud Telephony Security Vulnerabilities

1. Packet Sniffing and Black Hole Attacks

As the name suggests, packet sniffing is one of the most common VoIP attacks. With this attack, hackers may steal and log the information included in voice data packets as they travel.

Sniffers attempt to steal information by using packet drop attacks (often called black hole attacks) to prevent voice data packets from reaching their destinations, causing packet loss. By taking control of your router, packet sniffers deliberately drop packets into data streams, causing your network service to be much slower or to stop working completely.

Using packet sniffing, hackers can also collect sensitive data such as usernames, passwords, and credit card numbers.

Use a trusted VPN to send information over the internet to help make your lines more secure. Getting started and getting the system up and running takes some time, but it ensures the safety of information.

By encrypting all data end-to-end and monitoring their networks consistently, users can protect themselves against packet sniffing and black hole attacks. This alerts them to suspected login attempts, unusual devices, and so on.

2. DDoS Attacks

According to a survey by Corero, approximately 70% of companies experience at least 20-50 DDoS (distributed denial-of-service) attacks per month.

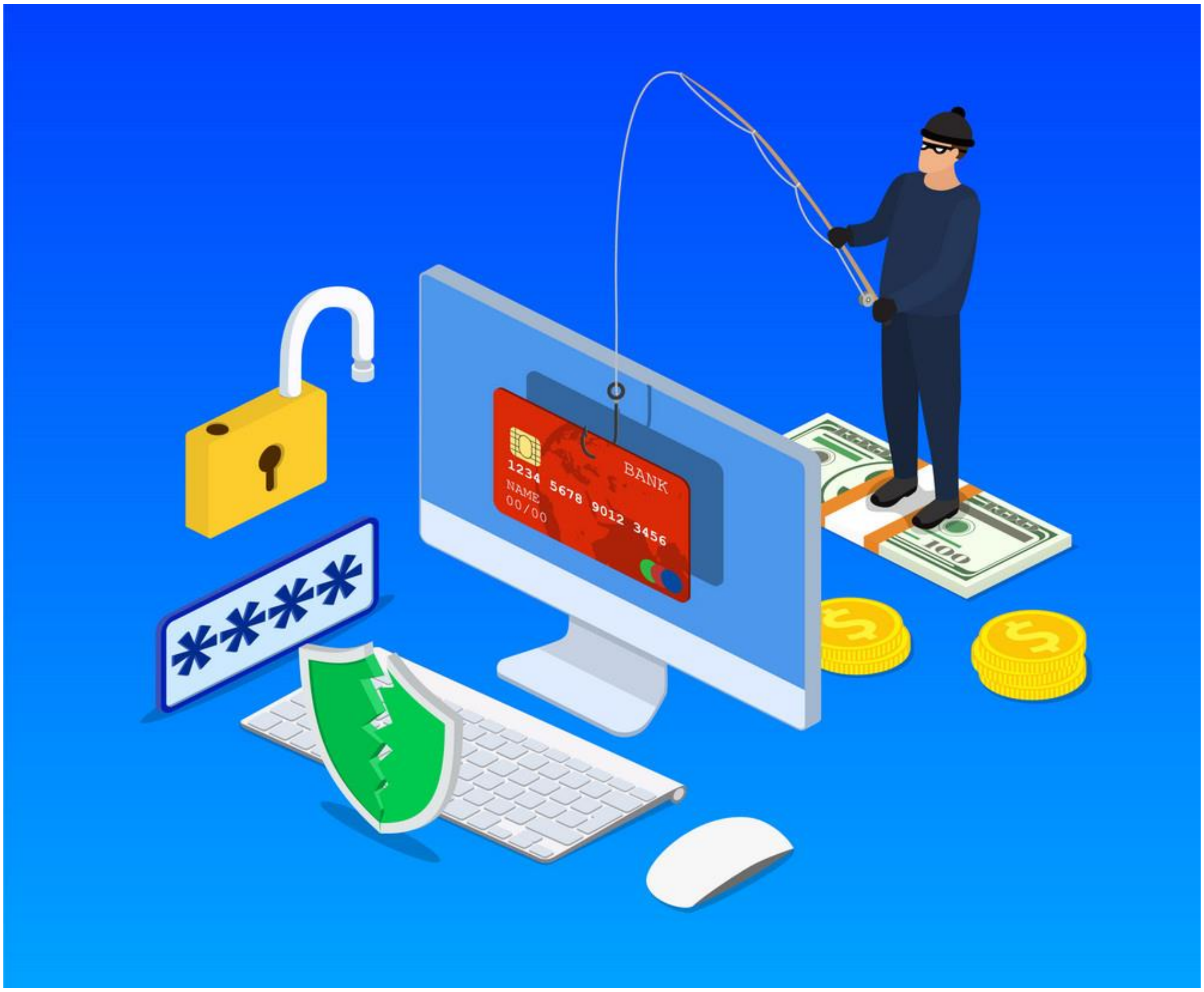
Despite the fact that they are mostly unsuccessful, the main issue is that cybercriminals are now able to launch DDoS attacks much faster and cheaper with highly capable machines, special tools, and much higher bandwidth than they were previously. This puts businesses of all types and sizes at risk, including large institutions (like banks or enterprises).

During a DDoS attack, criminals use all the bandwidth of a server and overwhelm it with data. This allows hackers to temporarily or permanently interrupt a machine or network so that its users can no longer access it. The VoIP system cannot make or receive calls when that occurs.

However, that's not all - in the worst-case scenario, the attacker might even gain access to the server's admin controls.

3. Vishing

Vishing uses VoIP to lure your attention, meaning that hackers pretend to be someone or something trusted in order to get sensitive information from you. Credit card numbers, passwords, and more are typically stolen.



Vishing hackers use caller ID spoofing to deliberately confuse potential victims, making their phone number and name appear legitimate. Your bank's phone number may appear to be the number they call from, claiming your account has been compromised. They can also ask you to do a thing or two, promising to secure your account.

The IT department of the targeted agency should verify all phone requests, regardless of whether they look like they came from within the department. Additionally, agents need to be trained to refrain from disclosing sensitive information unless authorized by their supervisor.

The following signs may indicate a vishing attack:

- There is a great deal of urgency coming from the other end of the line.
- The hacker continuously requests that you provide the information to verify it.
- A call from a known number or an established company that you weren't expecting
- On Caller ID displays, you may see short and unusual phone numbers.

4. Weak Encryption Tools

Obviously, data packets carrying voice data must be encrypted from beginning to end in order to ensure that they cannot be intercepted during transmission. You might encounter this at your network, your ISP, or anywhere in between.

Due to the complexities of voice encryption and the fact that it varies depending on factors like the sensitivity of the voice data you send, this is not something that's easy to understand. For this reason, Cisco has recommended some basic encryption best practices for its customers, including:

- Balance encryption costs with business-specific requirements while keeping costs low.
- SIP over TLS implementations in your switch fabric should be enabled by your vendor.
- Encrypting mobile device calls with VPNs when packet encryption protocols are not available (e.g., SRTP).
- A secure voice channel protected against eavesdropping during the transmission of packets over public networks.

Cloud security is threatened by APIs by their very nature. You can customize the features of the cloud to match your business needs. They also authenticate users, provide access, and take steps to encrypt data. A comprehensive protection strategy can provide you with all these benefits.

Using encryption is one way in which you can protect your data. Due to this, having a holistic approach to end-to-end encryption is important instead of focusing on both your vendor and network separately. You will be better prepared to handle any potential threats this way.

5. VOMIT and SPIT

It may sound like a gross acronym, but VOMIT describes a serious threat to any business. Criminals can steal sensitive information and voice packets straight from calls by using a tool called "Voice over Misconfigured Internet Telephones." In addition, they can also find out where the call originated, which they can use later in order to intercept everything you say.

The SPIT method consists of sending voicemails or automated calls several times a week. Because spammers have access to so many different tools, they can easily send many messages at once to several IP addresses or pretend to be local businesses when they are actually foreign companies.

If the call is answered, the recipient may end up being redirected to a very expensive phone number from another country, or the messages may contain viruses or spyware.

Is VoIP Secure to Use Then?

You might feel anxious to make internet calls for your business after reading about the risks and dangers of VoIP. The good news is that by learning some basic cybersecurity methods, you can ensure that your calls and data are secure.

- The most effective way to avoid hackers accessing your sensitive info is by encrypting it. Data or messages can still be intercepted, but they will be worthless to hackers with strong encryption.
- Make sure your VoIP platform's various devices have strong, varied passwords.
- Maintain a security vulnerability testing program.
- Ensure that your tools are always up-to-date.
- Prepare your employees on what to do in the event of phishing attacks.

Conclusion

Currently, VoIP appears to be in a state of evolution, as no widely accepted general security solution seems to be available to address all the challenges it faces. So many methods have been suggested and evolved over the years; VPNs, for example, are good security options, though they sometimes have some shortfalls, such as affecting performance.

Even though VoIP has been the subject of huge amounts of research, more research is needed to identify ways to combat the numerous attacks without drastically decreasing the performance. VoIP over VPN and other already suggested approaches should also be considered.

About the Author

Sujan Thapaliya is the CEO and Co-founder of KrispCall. He has a wealth of computer, communications, and security experience. As well as years of experience in the industry, Sujan has also conducted investigative research into issues such as privacy and fraud. Through KrispCall, he aspires to make business communication safer, reliable, and more affordable. Sujan can be reached online at (sujan@krispcall.com and https://www.linkedin.com/in/sujanthapaliya) and at our company website https://krispcall.com/

The 5 Most Common Cyber-Attacks on Mobile Devices In 2021

By Nicole Allen, Marketing Executive, Salt Communications.

Many companies are prioritising mobile efforts these days with research suggesting that increased mobility helps businesses enhance their operations and efficiency. Verizon's 2021 Mobile Security Index Report demonstrates, there are many pre-existing and new hazards when it comes to mobile security that businesses must consider in order to stay safe.

Traditionally the increases in organisational mobility often resulted in a rise in the number of mobile devices accessing your systems from afar. With COVID-19 impacting business operations globally in 2020 there are much higher numbers of mobile users accessing internal systems from home. For your security staff, this implies an increasing number of endpoints and risks to secure in order to prevent a data breach at your company.

Before we get into the top attacks of 2021 here are four different types of mobile security threats that businesses need to continue to look out for:

Most people think of mobile security risks as a single, all-encompassing issue. However, there are four major forms of mobile security concerns that businesses must be aware of in order to defend themselves.

- Web-Based Mobile Security Threats

Web-based attacks constitute an ongoing challenge for mobile devices since they are continually linked to the Internet and regularly used to access web-based services. These threats can be carried out through phishing scams, drive-by downloads and browser exploits.

- Mobile Network Security Threats

Cellular and local wireless networks are usually supported by mobile devices (WiFi, Bluetooth). Different forms of risks can be found on each of these types of networks through threats such as network exploits and wi-fi sniffing.

- Mobile Device Security Threats

Theft or loss of a device are the most common physical hazards to mobile devices. This threat is especially dangerous for businesses because hackers have direct access to the hardware where confidential data is housed.

- Mobile Application Security Threats

Mobile application security threats, like all other sorts of security threats, are continually evolving. Security threats to mobile applications, on the other hand, are of particular concern because they receive less security attention than other forms of software and technology. Some of the top mobile application threats are through malware, insecure coding, ransomware and crytojacking.

5 Most Common cyber attacks on mobile devices this year:

1. Social engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. When unscrupulous actors send bogus emails (phishing attacks) or text messages (smishing attacks) to your employees, they are attempting to deceive them into giving over personal information such as passwords or downloading malware onto their devices. According to reports from cybersecurity firm Lookout and Verizon, workplace mobile phishing assaults have increased by 37%, and phishing attacks will be the leading source of data breaches globally by the end of 2021.

The best protection against phishing and other social engineering threats is to teach employees how to recognise suspicious phishing emails and SMS messages so they don't fall for them. Reducing the amount of employees with access to sensitive data or systems can also help protect your company from social engineering attacks by reducing the number of ways attackers can obtain access to key systems or information.

2. Data breach via malicious apps

The millions of freely available apps on employees' devices pose a significantly greater threat to businesses than mobile malware. Since 85% of today's mobile apps are essentially insecure, this is the case. Hackers may now simply locate an unprotected mobile app and exploit it to plan broader assaults or steal data, digital wallets, backend details, and other lucrative information directly from the app.

When your employees go to Google Play or the App Store to download apps that appear to be harmless, the apps will ask for a list of permissions before they can be downloaded. These permissions typically demand access to files or folders on the mobile device, and most individuals simply scan over the list of permissions and agree without thoroughly evaluating them.

This lack of oversight, on the other hand, might leave devices and businesses susceptible. Even if the software performs as expected, it has the potential to mine corporate data and distribute it to a third party, such as a rival, exposing critical product or business data.

3. Unsecured public & home WiFi Networks

Since there's no way of knowing who set up the network, how (or if) it's secured with encryption, or who's now accessing or watching it, public WiFi networks are inherently less secure than private networks. Furthermore, as more firms provide remote work choices, the public WiFi networks your employees use to access your servers (for example, from coffee shops or cafés) may pose a security risk to your organisation. Cybercriminals, for example, frequently set up WiFi networks that appear legitimate but are actually a front for capturing data that travels through their system - a "man in the middle" attack.

Requiring employees to utilise a VPN to access corporate systems or data is the greatest approach to safeguard your firm from dangers over public WiFi networks, this can also be carried out for those working from home wifi’s. This ensures that their session remains private and safe, even if they access your systems via a public network.

4. End-to-end encryption gaps

A hole in an encryption gap is similar to a hole in a water pipe. While the point where the water enters the pipe (your users' mobile devices) and exits the pipe (your systems) may be secure, the hole in the middle allows bad actors to gain access to the water flow.

One of the most common examples of an encryption gap is unencrypted public WiFi networks (which is why they pose such a significant risk to businesses). Since the network isn't secured, fraudsters can gain access to the information your employees share between their devices and your systems. WiFi networks, however, aren't the only thing that may be exploited; any application or service that isn't protected might provide attackers access to important company data. Any unencrypted mobile messaging apps that your employees use to communicate work-related information, for example, could provide an entry point for a bad actor to intercept important business communications and documents.

End-to-end encryption is required for any sensitive work data. This means ensuring that any service providers you interact with encrypt their services to prevent illegal access, as well as encrypting your users' devices and systems.

5. Internet of Things (IoT) devices

Mobile devices that access your company's systems are expanding beyond smartphones and tablets to include wearable technology (such as the Apple Watch) and physical hardware (like Google Home or Amazon Alexa). Since many of the latest IoT mobile devices have IP addresses, bad actors can exploit them to acquire internet access to your organization's network if those devices are connected to the internet that are connected to your systems.

It is the responsibility of each organisation to implement the necessary technological and regulatory regulations to ensure that their systems are secure. According to statistics, you probably have more IoT devices connected to your networks than you think. In a research conducted by Infoblox, 78% of IT leaders from four countries indicated that over 1,000 shadow IoT devices accessed their networks every day.

What can your company do today?

Seeing the destruction that cyber attacks can do should be enough to convince your organisation to take the necessary measures as soon as possible. So, there are some steps you can do to improve your company's cybersecurity and protect it from cyber threats.

Mobile security should be at the forefront of a company’s cybersecurity agenda, especially in an era where remote working is the new norm, and not something that will be going away anytime soon. Many companies and organisations that Salt Communications work closely with have seen an increase in mobile usage for communications and day-to-day work requirements. Often firms will look at developing a mobile security guide for what users should and should not be doing while operating from their mobile devices. Other companies have deployed MDM/UEM systems to lock down devices and provide an extra layer of security to workplace issued devices which employees are utilising from home.

At Salt we understand the requirement for a secure communications system to be utilised in an era where mobile interception is rife. With the ever increasing requirement for sensitive communications to take place remotely, organisations need to be able to deploy a system that they have complete assurance that everything they are disclosing remains confidential. This may be law enforcement events, or lawyer-client communications; effectively any form of communications that needs complete security. Salt Communications works with clients all around the world that understand the importance of having complete control over their private communications. Leaks to the public tarnish their organisation's reputation and, in some cases, jeopardise the safety of their employees and the broader public. You will be able to govern your communications and feel safe in whatever situation you may experience throughout your everyday operations by utilising a secure communication platform such as Salt Communications.

At Salt Communications we work with businesses of all sizes all around the world to enable them to have secure, confidential discussions wherever they are, at any time.

To discuss this article in greater detail with the team, or to sign up for a free trial of Salt Communications contact us on info@saltcommunications.com or visit our website at saltcommunications.com.

About Salt Communications

Salt Communications is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. Salt Communications offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. Salt is headquartered in Belfast, N. Ireland, for more information visit Salt Communications.

About the Author

Nicole Allen, Marketing Executive at Salt Communications. Nicole has been working within the Salt Communications Marketing team for several years and has played a crucial role in building Salt Communications reputation. Nicole implements many of Salt Communications digital efforts as well as managing Salt Communications presence at events, both virtual and in person events for the company. Nicole can be reached online at (LINKEDIN, TWITTER or by emailing nicole.allen@saltcommunications.com) and at our company website https://saltcommunications.com/

Why Email Archiving Builds Cyber Resilience

Plus 3 Email Archiving Solutions

By Adnan A. Olia, Chief Operating Officer, Intradyn

As innovations in technology continue to create new uses across an array of industries, cyber safety has become more important than ever before. Technological advancements have made cyber security a top concern for small businesses, global enterprises, educational institutions and government agencies alike, all of whom must keep cyber resilience a top priority.

While cyberattacks can be difficult to predict, building a cyber resilience strategy can help combat any potential issues that might arise. This is where email archiving becomes of paramount importance for businesses across nearly every industry.

With an email archiving solution, you can have peace of mind knowing that your emails are safe, secure and easily searchable. Read on to learn how email archiving can support cyber resilience, including tips on how to build a comprehensive cyber resilience plan for your organization.

What is Cyber Resilience?

According to the National Institute of Standards and Technology (NIST), cyber resilience is “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.” Cyber resiliency addresses all threats that can reach any form of a cyber resource. Therefore, a cyber resiliency plan is an all-encompassing strategy that should be applied across an entire organization or operation. A cyber resilience strategy helps to protect critical systems, applications and data and enables faster reaction times in the event of a disruptive cyber incident such as a data breach.

Cyber resilience plays both a preventative and a reactive role. By putting the necessary measures in place, such as email archiving, you are mitigating significant risks for your organization. In the event of an attack, cyber resilience is important for analyzing, managing and recovering efficiently.

What is Email Archiving?

Email archiving refers to the ability to completely move an electronically stored message from one data store to another. The ultimate goal of email archiving is to preserve and make all emails searchable.

Businesses and organizations need to archive electronic communications and information for a number of reasons, including business continuity and disaster recovery. With email archiving, businesses can preserve such communications in a safer, more accessible way.

Not only is an email archiving solution vital to an organization’s protection, but it can also aid in saving on storage, reducing storage load, eliminating PSTs and improving productivity.

Email Archiving Solutions

Spending in the cybersecurity industry reached around 40.8 billion U.S. dollars in 2019 and is only continuing to grow as the use of technology increases. It is important that organizations today place a strong focus on investing in cyber security and following best practices in cyber security risk management, such as continuous data monitoring and record-keeping.

When building a cyber resilience strategy, it is important to work with an email archiving consultant that has the necessary expertise to meet your unique cyber resilience requirements. It is also critical to find an email archiving solution provider that maintains a high standard of security and reliability.

3 Ways Email Archiving Builds Cyber Resilience

So, how exactly does email archiving build cyber resilience? Here are some of the ways that email archiving supports a strong cyber resilience strategy:

- **Combat Phishing Attacks**
  Phishing is the fraudulent practice of sending out malicious emails to acquire sensitive data, steal information or gain access to a system. Such attacks are one of the most common threats to businesses and individuals in 2021.

  It is of the utmost importance to act quickly when combatting any form of cyberattack. If your systems are compromised, an email archiving solution both ensures that important data is not lost, and that private information remains private. If a data breach were to occur without an email archiving solution, an organization could face a hurdle so major that the damage could ultimately be irreversible.

- **Email Security**

  There is no doubt that storing emails in your inbox is no longer as safe as it once was. Today's hackers are so advanced that they can get in and gain access to anything that they want in a matter of minutes.

  Fortunately, an email archiving solution will maintain the data in a manner that cannot be changed or deleted. This guarantees that an organization can present any information needed should they be faced with litigation or record requests and quickly get back online following a malicious cyberattack.

- **Protect Data**

  There are various types of archiving solutions that can be used to protect data contained within an email archive, such as encryption, role-based permissions, multi-factor authentication and redaction tools. Data protection is one of the many reasons why having a secure electronic information archiving platform is an essential part of a cyber resilience strategy.

- **Recoverability & Compliance**

  With email archiving, an organization can recover company-wide inboxes back quickly and correctly. The best way to maintain compliance in regulatory industries while maintaining cybersecurity is to use an independent archiving solution.

  An archiving solution stores emails in the most resilient manner because it moves and secures only one copy of the email immediately after it is sent or received. This subsequently enables an organization to collect, secure and store incredibly large amounts of email into a single central location that can be easily searched or audited. Moreover, the metadata within the message will not be duplicated again, regardless of how many more times the information is passed along through various accounts.

Additional Benefits of Email Archiving

Aside from the notable benefits that relate to building cyber resilience, there are numerous other advantages that come with email archiving. Some of these advantages include:

- Reduced storage costs
- Reduced stress on servers
- Faster restoration
- Reduced costs for email backups
- Instantaneous access to email records
- Faster disaster recovery
- Increased productivity
- Regulatory and legislative compliance

As technology continues to evolve, building cyber resilience will continue to be crucial. With the right email archiving solution, your data can be preserved and protected using consistent backup and disaster recovery capabilities.

About the Author

Adnan A. Olia is a senior member of the Intradyn team and is responsible for keeping an eye on the regulatory and technological marketplaces. Adnan provides thought leadership in the archiving and compliance sector to help Intradyn understand the latest trends in business innovation.

Adnan can be reached online at our company website https://www.intradyn.com/.

Overcoming the Limitations of VPN, NAC, and Firewalls with Zero Trust Access

During 2020 and 2021, we've seen ransomware-as-a-service wreak havoc in the IT supply chain and critical infrastructure. Below we explore how technologies and approaches to help protect organizations from these types of attacks.

By Burjiz Pithawala, CPO & Co-Founder, Elisity

We live in a world that is making a transformational leap into uncharted territory out of necessity. The pandemic has challenged us both at home and at work. We now live and work differently than a couple of years ago. What was called the "new normal" has become the "now normal": the hybrid workspace, with users working alternatively from home and on campus. This rapid change is still in progress and challenges networking and information security teams in many novel ways. This article focuses at a high level on some of the problems and solutions derived from the need to secure remote access to enterprise resources, the sprawl of IoT, the growth of shadow IT, and the acceleration of the migration to cloud infrastructure.

Trends making implicit trust security controls obsolete

As a result of the pandemic-driven changes in the workspace and IT environments, bad actors have adapted rapidly to tap into a growing attack surface. During 2020 and 2021, we’ve seen ransomware-as-a-service wreak havoc in the IT supply chain and critical infrastructure just at a time when IT organizations were migrating infrastructure and applications to the cloud and trying to secure access for an all the sudden majority of remote workers. It’s been a rollercoaster across all industries for organizations of all sizes, to say the least.

Users, devices, applications, and data have for the most part left the traditional perimeter, and as a result, traditional security controls are failing to secure them. The enterprise networks have become more challenging than ever before to secure against these ever-growing cyber threats from outside and inside the new perimeter. Rogue applications, unmanaged IoT devices, and overlap of IT and Operational Technology (OT) networks add more to these difficulties, with growing risks as the attack vectors multiply. In the end, network availability and productivity are suffering too due to the lack of scalability of traditional cyber defenses.

These trends resulted in a re-definition of the enterprise perimeter which is now centered around the identities of users, devices, applications, and data. It is being said that identity is the new perimeter. By now, you should have read about the Zero Trust model enough to be confused by the sheer amount of spin around this information security concept. To make it simple, short, and sweet, let’s stick to the fact that Zero Trust is not a product, but a premise from which to derive a ubiquitous information security strategy and the controls that help operationalize it. Zero Trust is based on the assumption that all network communications are compromised and therefore should be untrusted regardless if these occur within or outside a network’s boundaries. The solution to minimizing risk under that premise demands for identities to be continuously verified and access authorized regardless of location in the network.

Zero Trust is essentially a journey towards the aspirational elimination of the attack surface. In this regard, identity has a central role. But identity alone is not enough. It’s behavioral intelligence that should deliver the power of end-to-end protection for all of your assets, regardless of location. There is a pressing need to contextualize three things: identity, environment, and behavior. This new fluid perimeter is a combination to be managed by organizations with a simple business logic policy to securely connect all of the assets across every domain: campus, branches, data center, cloud, and remote.

Although the concept of Zero Trust has been here for a decade or so, it was always challenging to operationalize it because the traditional security controls, designed under the premise of Implicit Trust, are inefficient and ineffective to enable it at scale. Let’s list some of the limitations of these legacy security controls.

Virtual Private Networks (VPN)

User-to-application access from outside the traditional network perimeter has been traditionally secured with VPN, but:

- VPN cannot limit access control after authentication and can’t provide continuous verification that would prevent the ability to traverse the network unhindered (East-West/North-South movement).
- It’s inefficient to drag all user traffic back to the corporate data center, and split-tunneling brings loss of visibility and control.
- VPN provides an inefficient traffic path for SaaS and cloud applications or services, delivering a bad end-user experience.
- No policy can be defined when a user is within the network perimeter, and not using VPN.
- VPN concentrators are expensive and complex to deploy and manage.

Network Access Control (NAC)

NAC technology has been around for a while but it is showing its age vis-à-vis of the evolving threat landscape.

- NAC provides binary network access (either on or off) and has limited granular control and segmentation capabilities.
- It typically has no supplicants for wired users or unmanaged devices such as IoT and OT, and provides limited access control for such devices.
- With NAC, there is no continuous verification of authorization. User identity is verified at the point of authentication, limiting the ability to monitor for threats post-authentication, changes to permissions, and abnormal behavior.
- Typical NAC solutions cannot manage and deploy NAC policies to cloud infrastructure.
- Most NAC solutions have separate policy management systems for remote access VPN and firewall configuration.
- As with most security controls designed under the old Implicit Trust model, traditional NAC solutions can be highly complex and expensive to deploy and maintain.

Firewalls

Deploying and managing firewalls across an SD-WAN is quite an undertaking, and firewall policy drift is a common ailment. This is why:

- IP-based policies are hard to manage and do not provide micro and nano-segmentation capabilities.
- Firewalls policies are statically configured and cumbersome to manage and update, and are often based on traditional networking constructs.
- True micro-segmentation to limit lateral movement within the network requires a proliferation of firewalls, which is costly and resource-intensive to deploy and manage.
- Access is based on location, i.e., inside or outside the moat: the network perimeter. Once a user is inside the network perimeter, they are inherently trusted and free to roam the network.
- It is challenging to unify policies for on-prem and remote users (i.e., behind the firewall and outside remote users).

Solving for the long run

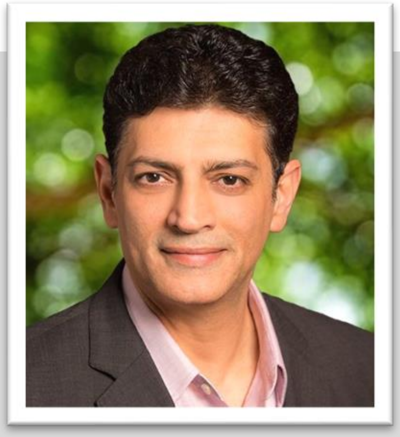
All these limitations drive the requirements for the transformation of network security and how information security is approached altogether. Some of this transformation was in progress before the pandemic, but it accelerated rapidly out of necessity when it struck. Zero Trust is still riding the hype curve, and many fragmented point solutions exist that address specific use cases without accounting for the bigger picture. This bigger picture is the need to decouple security from the underlying network construct to avoid the traditional cybersecurity vs. networking trade-offs that either cripple network availability or the security posture.

There is also a need for ubiquitous access policy management (across all domains) and simplification via automation of cybersecurity operations to accelerate detection and response times. An ideal Zero Trust Access (ZTA) platform should deliver full visibility about what's flowing through the network (users, devices, apps) by integrating with existing identity providers (IDP). The solution should also provide a unified policy management plane across multiple domains that would address the need for ubiquity and agility.

It's just then, through a single pane of glass across all domains, that the never-ending Zero Trust journey to eliminate the attack surface can start. Organizations can begin by securing the crown jewels first, or by piloting Zero Trust Network Access (ZTNA) to secure access for the hybrid workforce. Alternatively, Network Security Architects may choose to learn the ropes of Zero Trust network security by addressing the sprawl of IoT in the workplace. Whatever the most pressing use case may be, the worst they can do is to lose sight of the long game: that the same solution should address all use cases and avoid network chokepoints that prevent scalability.

The ideal end game is a distributed architecture where multi-domain policies are managed centrally but distributed and enforced as close to the resources as possible, with continuous identity verification via integration with any flavor of IDP, including those providing telemetry about health status and other contextual attributes alongside identity. By making identity, context, and behavior the new (and now dynamic) enterprise perimeter, it becomes easier to manage risk and implement a potent cyber defense system that works under the Zero Trust paradigm.

About the Author



Burjiz Pithawala is the CPO and co-founder of Elisity. Burjiz's experience as a leader and technology visionary spans 23 years with deep roots in networking, cloud transformation, and enterprise software. Prior to Elisity, Burjiz led many of Cisco's best-recognized routing and switching product groups with teams of 15 to 300 people. Burjiz is an Internet Task Force (IETF) author and patent holder for technologies ranging from routing, switching, and predictive cloud management.

Burjiz co-founded Elisity, now a series A start-up, to address the challenges depicted in this article. Elisity offers an identity-driven control plane for corporate networking and remote access without tying customers to a particular network or network security technology. Its Cognitive Trust platform, delivered as a cloud-based service, is deployed as an overlay or underlay on whatever WAN and/or SD-WAN infrastructure an enterprise prefers to protect data, users, devices, and applications in the data center, the cloud, at home, and everywhere. Based in San Jose, Elisity is backed by Two Bear Capital, AllegisCyber Capital, and Atlantic Bridge. Burjiz can be reached online at LinkedIn and at our company website: www.elisity.com

Multicloud Rolls In: Federal IT Professionals Share Insights and Challenges

By Rick Rosenburg, Vice President and General Manager, Rackspace Government Solutions, Rackspace Technology

Federal agencies kicked into IT modernization overdrive during the pandemic and, as 2022 approaches, agencies are looking for ways to capitalize on investments and continue to accelerate transformation. One of the key investments has been in the cloud technologies that largely enabled operations across the government during the past year. And now, agencies are looking to expand capabilities, shore up security and optimize their investments in both cloud infrastructure and solutions.

To achieve these goals, agencies need to invest in a comprehensive multicloud strategy to address the complexities and challenges inherent to managing and optimizing cloud investments and capabilities while emphasizing security, workforce optimization, and resource availability. While using multiple cloud vendors is not new, crafting a multicloud strategy is – and it is complex, especially when it comes to addressing security and compliance, so Federal agencies seek a clear path forward.

A Work in Progress

The Advanced Technology Academic Research Center (ATARC), in partnership with Rackspace Technology, AWS, VMware, and Carahsoft, recently surveyed Federal IT professionals to take the pulse of the Federal multicloud world to better understand the current landscape, the most significant challenges, and how agencies can move faster on the path to implementing a multicloud strategy.

First, it is encouraging to see that many organizations are utilizing the capabilities of multiple cloud vendors and thinking about optimizing their investments. Thirty-seven percent of respondents report their agency uses multiple clouds (infrastructure and solutions), and 60 percent have started on a cloud strategy journey. Federal IT professionals understand that it is necessary and critical to their operations. Thirty percent of respondents rank business agility as the number one benefit of cloud adoption – followed closely by legacy modernization, improved citizen experience, and optimizing IT investments.

And while agencies are taking steps in the right direction to utilize vendor-provided cloud solutions and services, budget is reported as the most significant barrier in making that shift, followed closely by workforce skillset and procurement challenges.

Another significant barrier holding agencies back is understanding cloud security and compliance requirements. Nearly one-third of respondents report their agency struggles with a basic understanding of their annual security and compliance requirements – where only 40 percent of responders give a strong rating on their agency's understanding, whether they are procured or developed in-house.

FedRAMP – A Mixed Bag

One of the most important programs for ensuring cloud solutions meet Federal security and compliance procedures is the Federal Risk and Authorization Management Program (FedRAMP). Survey responses showed that most Federal agencies understand FedRAMP's significance, with 62 percent agreeing that FedRAMP helps streamline the procurement of secure, trusted cloud solutions. However, FedRAMP authorization levels vary widely, with 43 percent of agencies reporting that their highest FedRAMP impact level implemented is moderate, while 32 percent noted high FedRAMP.

Even though Federal IT leaders see the benefits of FedRAMP, 41 percent say that the program hinders modernization through a slow ATO process. Respondents agree there is room for greater collaboration between government and industry to accelerate FedRAMP authorization and avoid the pressure and risk of alternative or shadow IT procurement.

Multicloud as a "Business" Model

Cloud modernization is critical in government agencies' lowering their cybersecurity risks and improving Cyber posture, optimizing operations, and maximizing the potential in leveraging other emerging technology applications (e.g., artificial intelligence and machine learning). Choosing cloud does not actually mean choosing a vendor; it is a business model. Rather than thinking of cloud (and multicloud) as a destination, agencies should think of cloud as a great strategy requiring planning for the complete lifecycle and utilizing multiple vendors to maximize their capabilities and outcomes.

Using multiple cloud technologies brings new challenges and complexities to every phase of that lifecycle – design, build, secure, manage, and optimize – because agencies have to manage multiple public, private, and hybrid clouds. So, it's vital to know what, where, and when to migrate for workloads, data, and applications – and the security and compliance required to maximize value and reduce risk and cost associated with missteps that necessitate multiple moves. For example, buying AWS does not mean that all of your cloud security comes along with it. AWS protects the perimeter of the cloud, but everything else inside the permitter needs to be secured on top of that. It means understanding all the data applications and workloads and what goes where and at what level of security.

The complexity that comes along with multicloud can be overcome. The key is a fully baked multicloud strategy that puts security first, optimizes internal resources, and utilizes the right industry partners, services, and solutions. When done right, agencies realize all the benefits of streamlined operations and optimized cloud environments with unified governance and security.

About the Author

Rick Rosenburg is the vice president and general manager of Rackspace Government Solutions at Rackspace Technology. He oversees services in support of government agencies and holds 35 years of leadership experience across companies that have supported the Federal government's technology needs. Prior to Rackspace, the government services vet held leadership roles at NTT Data Services, Seros, and Dell Services Federal Government.

Rick Rosenburg can be reached online at rick.rosenburg@rackspace.com and at our company website https://www.rackspace.com/industry/government.

SOAR Into More Integrated Cybersecurity

By Josh Magady, Section Manager, Senior Cybersecurity Consultant, and Practice Technical Lead, 1898 & Co.

Why is being cybersecurity compliant not the same as preparedness for threats? Shouldn't compliance mean full coverage against all current and future threats? Compliancy builds in a checklist mentality. A company measures their compliance compared to certain standards like NERC CIP and HIPAA for example but, they can't account for a company's environment. They are intended as a starting point. The problem for organizations is when they stop with just meeting compliance standards and don't look for avenues to bolster their cybersecurity efforts. They might follow the best practices of the CIS Top 20, but they need a more comprehensive approach. They require a suite of tools and policies that allow them to handle the challenges of remote working and access, nation state-sponsored attacks, and broader digital transformation.

An ideal counterpoint to various threats and digitization is a SOAR platform. SOAR stands for Security Orchestration, Automation, and Response. Orchestration means coordinated devices and software applications. Automation involves security processes and protocols happen based on pre-set rules, and Response relates to a collection of information and rapid actions taken against threats in real time. It's an ideal solution for protecting critical infrastructure against an ever-increasing number of threats.

Threats for OT, Industrial Control Systems, and SCADA Environments

The threats for OT, ICS and SCADA vary by sector. Nation states are a consistent threat which are targeting municipalities, electrical grids, and other similar entities. They're looking to destabilize these systems and, in some cases, they're fronting the efforts of ransomware gangs.

For industrial control systems (ICS), the challenge comes when security experts are asking engineers and system operators to think about cybersecurity. These people often feel the data produced by their ICSs is not valuable and might not warrant strong cybersecurity. However, bad actors have interest in control over these systems, not the data.

The push towards remote work and broad digitization of services complicates the cybersecurity responses. Within OT, ICS and SCADA environments, there's a range of related threats, including the risk of human error and usage of old and outdated legacy systems. With spreading digitization, there's also an increased need for connectivity for information sharing and insights. Further digitization means additional endpoints and transits that expose data to bad actors. Within all three of these environments there's also some networks and systems that are not secure by design, so there is deep inherent flaws. Adding to all these flaws are a market with too many vendors and not enough integrated systems that enable continuity.

With remote work, firms are reliant on their employees to maintain security over their home networks but, traditionally these staff don't have the training or the background to understand the risks and threats facing their home networks. People remain the vector for threats. Firms need robust hardened endpoints and implement technologies that can provide endpoint detection response (EDR) as well as adopt zero trust architectures (ZTA). Managing all these threat exposures at scale proves challenging for any business unless it brings onboard a SOAR platform to unify its infrastructure and automate various processes.

SOAR Adds Efficiency to Cybersecurity Efforts

SOAR uses automation to extend the ability of security teams to manage multiple systems. It integrates across various platforms and efficiently codifies existing workflows to expand the work of understaffed teams. It's an operations platform, one that blends technology and operational processes. In the hands of an experienced practitioner, SOAR can improve various processes.

SOAR platforms provide almost infinite capabilities because at heart, they are application platforms. This means if a user can think it, it can most likely be implemented in a SOAR platform. Since it's only limited by one's imagination, sometimes SOAR platforms can intimidate teams. However, when used properly SOAR functions as an integrative platform that saves time and gives cyber teams a deeper reach. It automates vital processes and integrates various systems within a single platform, which creates streamlined actions and familiarity over time.

With SOAR, organizations can orchestrate existing resources together with automation. It enables a more proactive response model, with UI standardization, improved data gathering, and workflow analysis that work together to manage today's complex threats.

For example, a firm might spend several hours performing an indicators of compromise (IOC) investigation. They might receive a notification from E-ISAC about checking certain domains or IP addresses or even a specific hash of a file. This creates a significant amount of work, as the analyst will need more information than what's provided in the alert. For example, if a file hash alert comes in, the analyst requires more data to really understand what it’s doing. They might reach out to AlienVault or Virus Total and lookup that hash and get all the details, such as what things it usually changes, attack vectors, and other details that build a forensic case. Once this information has been collected, a search of a systems endpoints is required to check if that IOC is present in the environment. With the tasks already programmed into SOAR, along with an email parser that recognizes the E-ISAC alert, a company can tackle the investigation in minutes. The SOAR platform produces a report, so the team can take further actions as needed.

This dynamic cuts through the noise for optimal efficiency and accuracy. So, the cybersecurity team can focus on dealing with present threats that are in the network, while automating threat identification and investigations. It also limits analyst burnout from responding to the hundreds of thousands of threat alerts that come across their desks nearly every hour. Going through these manually and determining which ones are actionable is not a reasonable task.

One caveat for SOAR is before a significant implementation, an organization needs to review and improve its documentation. Especially if the company expects the full SOAR capabilities of incidence response, endpoint detection, phishing management, and asset management. A quality SOAR platform can manage all of this, but it requires a mature organization that has its policies in place with documentation. It doesn’t work with “tribal knowledge” that differs based on staff’s opinions because it cannot automate unknown processes. Before diving into a SOAR platform, it’s worthwhile for organizations to take any undocumented processes and put them on paper and then perform smoke testing to insure they are indeed the right processes.

SOAR provides an operations platform that enables threat investigation at scale and can streamline existing processes. It addresses staffing shortages and the need for leaner operations by automating mundane tasks. Through integration of different systems, SOAR drives efficiency for the benefit of overworked cybersecurity teams who now have time and energy to conquer other operational issues.

About the Author

Joshua Magady is a proven security professional and leader of security teams and programs within a variety of markets. For the past 5 years he has been working to secure our nations critical infrastructure with 1898 & Co. For the 10 years prior to that, he was leading the charge in the DoD helping to keep the systems our warfighters rely on safe and secure. He has many initials after his name, including CISSP, OSCP, and GICSP. He has a passion for helping the average person and new security professionals understand the why, what, when and how of security.

Joshua can be reached online at https://www.linkedin.com/in/joshuamagady/ and at our company website: https://1898andco.burnsmcd.com/.

Analyzing The Security Challenge of Hybrid and Remote Working Models

By Mike East, VP EMEA, Menlo Security

The pandemic has shifted the balance in many arenas, not least in relation to cybersecurity.

Where COVID-19 has continued to have a drastic influence over economies, societies and governments globally, cybercriminals have been able to piggyback on a perfect storm of uncertainty and confusion, tapping into fears and capitalizing on new vulnerabilities.

One of the most significant indirect impacts of the pandemic has been the uptick in remote and hybrid working models.

Indeed, such models deliver a variety of benefits, from improved work life balances for employees to the ability to access wider talent pools for employers who are no longer restricted by geographies and offices.

However, with remote and hybrid operations have come distinct changes in relation to IT, revealing a host of security vulnerabilities in those organizations that have failed to adapt appropriately.

Menlo Security recently surveyed over 500 IT decision makers in the US and the UK to gain insight into the attitudes surrounding securing remote access to applications and resources and potential methods of doing so.

Critically, this survey found that while 83 percent of organizations are confident in their ability to control access to applications for remote users, 75 percent are still opting to err on the side of caution and conduct additional evaluations of their security strategy to gauge suitability in the ‘new normal’.

While a quarter of organizations are opting not to do so, the fact that three in every four companies are is a promising sign.

Critically, security protocols in relation to on-premise models and hybrid cloud-based models differ wildly. Both require different approaches, and therefore those companies that have made the shift to cloud-based operations since the pandemic first emerged must update in order to be secure.

At the same time, however, it is vital that those organizations conducting such reviews come to the right conclusions.

Our survey also found that three in every four organizations still rely on virtual private networks (VPNs) for controlling remote access to applications – this ratio rising to more than four in five for organizations with over 10,000 employees.

With traditional security tools such as VPNs being inherently insecure in the modern day, this is a challenge – yet there is significant opportunity to address this, and organizations are showing willing.

Achieving holistic protection in the hybrid era

So, what improvements should organizations be considering in order to bolster their security within an environment dominated by remote and hybrid business models that are plagued by rising cybercriminal activity?

Enter zero trust – the perfect starting point for transforming security.

Unlike traditional protocols that take a somewhat outdated ‘castle and moat’ approach to security, only working to defend the external perimeter of an organization, zero trust takes an approach rooted in three key principles:

- That all available data points must be continually authenticated.
- That user access must be limited to specific applications.
- That a breach must always be assumed to be imminent.

In simple terms, zero trust is about viewing trust as vulnerability.

While defending the perimeter once worked, today’s hyperconnected world, underpinned by the cloud and the integration of a sea of external applications, the perimeter no longer exists. As a result, the threat landscape has become increasingly exacerbated, and therefore it is critically important to limit risks and exposure.

Many of the most harmful cyberattacks in recent times have largely been the result of a lack of proper security protocols beyond the perimeter. After hackers have gained initial access to a company’s network, they have been able to move laterally to access data and elevate privileges without any meaningful resistance.

For this very reason, zero trust ensures that all external and internal traffic – be it emails, websites, videos, documents or other files that originate from either inside or outside an organization – must be verified.

Implementing zero trust: Isolation technologies

Indeed, many organizations agree that the inherent connectivity that comes with hybrid and remote working models is creating additional areas of security consideration.

Some 75 percent of Menlo's survey respondents stated that they believe hybrid and remote workers accessing applications on unmanaged devices pose a significant threat to their organization's security.

Further, almost four in five agreed that remote access by third parties is a cause for concern with more than half planning to reduce or limit third party/contractor access to internal systems and resources over the next year or two.

Yet such concerns could easily be addressed by the implementation of zero trust policies – given the intensity of today's threat environment, controlling internal and external user access has never been more important.

That said, it can be difficult to know where to start.

What does zero trust look like? What technologies and tools are required? How can I implement it throughout my entire organization? Here, a security specialist can be a highly valuable partner, helping to answer many key questions and implement a zero-trust architecture that suits the specific needs and functions of any one individual organization.

Isolation technology, for example, is one tool available that can achieve zero trust in its truest sense.

Isolation essentially moves the browsing process from the endpoint – be it a desktop, mobile device, tablet or other – and executes it in the cloud. In this process, a form of digital air gap is created between the internet and endpoint where all content can be rendered safely to always deliver holistic peace of mind.

Isolation-centric zero trust therefore does not leave any room for error. Indeed, it can halt threat actors in their path 100 percent of the time.

About the Author

Mike East is Vice President EMEA, Menlo Security Mike East is Vice President EMEA Sales. In this role, he is helping to grow the business across the region and develop and manage the EMEA sales team. Mike has worked in the IT industry for 30 years, in technical and sales leadership roles, focusing on security for the last 15 years, building and restructuring the UK and EMEA businesses for vendors, including Symantec, Mandiant, FireEye, CrowdStrike and Duo Security.

Passionate about solving the ever-increasing cybersecurity issues that companies and governments face on a daily basis, Mike has experience of presenting at industry events and participating on panels and webinars talking about web isolation, network security, malware and cybersecurity resilience.

Mike can be reached at mike.east@menlosecurity.com or via https://www.linkedin.com/in/mike-east/ and at our company website http://www.menlosecurity.com/

How To Effectively Secure Connected Devices

By Gnanaprakasam Pandian, Chief Product Officer and Co-Founder, Ordr

As connected devices, including Internet of Things (IoT), Internet of Medical Things (IoMT) and Operational Technology (OT) continue to explode in growth, they introduce a new attack surface. In fact, an astonishing 46% of all connected devices are vulnerable to medium and high severity attacks. This is just one of the key findings of a new report released by connected device security company Ordr, in its 2nd annual Rise of the Machines 2021 Report "State of Connected devices -- IT, IoT, IoMT and OT report.

The report analyzed connected device security risk and adoption between June 2020 and June 2021, across more than 500 customer deployments in healthcare, manufacturing, financial services organizations and more. According to the report, the following are the key security issues that should be on the radar of every network security professional.

Extending security to agentless or un-agentable devices

The report found that 42% of connected devices were agentless or un-agentable devices – meaning that they cannot support endpoint security agents. This represents a 32% increase since 2020, further confirming that a security strategy focused only on agent-based endpoint security is insufficient. A complete security strategy should include solutions that can identify and secure these devices **via the network** to complement endpoint security solutions.

Adopting a “whole organization” approach to connected security

To ensure connected device security, it is vital that **all** devices and assets on a network be identified and profiled. The Colonial Pipeline attack showed us that when IT and IoT systems are hit by a cyberattack, business is impacted even if the OT environment continues to function. For example, in a hospital environment, a cyberattack impacting an elevator control system will similarly bring down the entire healthcare operations if patients cannot be transported, even if medical devices are unaffected.

Understanding the Risks posed by “Shadow IoT” and personal devices

Reflecting current times, the report found that the number of Pelotons, Sonos, Alexas and Teslas in customer networks have almost doubled since 2020. Many of these devices (with the exception of Teslas) are being used for actual business operations. In fact, many of “Smart Hospitals” have deployed Alexas in their rooms for their pediatric patients. Alexas were used for “nurse call functions,” to switch channels on TVs, and to dim or change the smart lighting in the rooms. Pelotons are being used for physical therapy in hospitals, deployed in gyms in hospitality verticals and enterprises.

Not only do these devices have vulnerabilities (for example leaky APIs within Pelotons) that threat actors can take advantage of, but there is also an overwhelming amount of data stored that could be used to target users within the organization. Threat actors are already targeting disgruntled employees to get them to unleash ransomware. Data from personal devices could present a whole new range of threats.

Gauging the level of security risk posed by devices

It is important to be aware that outdated operating systems present the greatest security risks for most organizations. According to the report, about 19% of deployments include devices running outdated operating systems Windows 7 and older, and almost 34% of deployments have devices running Windows 8 and Windows 10, which are expected to end-of-life in 2023 and 2025, respectively.

Within healthcare, 15% of medical devices and 32% of medical imaging devices run on outdated operating systems. This is because many medical devices remain in operation for many years and cannot be easily replaced for cost reasons. Segmentation is the only way to ensure security of these devices, keep them in operation and avoid the costs of replacing devices early.

Managing user access to devices and appropriate offboarding when status changes

A particularly interesting finding of the report was that about 55% of organizations examined had devices with orphaned users. These are most often devices that were the responsibility of users that have left an organization or changed roles. Devices with orphan accounts retain the same access rights as when they were associated with an active user. These orphaned user accounts provide a gateway to privilege escalation and lateral movement. Therefore, as part of a robust and complete Zero Trust strategy for connected devices, security teams need to ensure that all devices are being utilized only by current users.

This latest Rise of the Machines report identified a substantial number of vulnerabilities and risks in connected devices, which is a crucial reminder that organizations must have comprehensive visibility as well as security for everything connecting to their networks. The number of network-connected devices is only going to increase and the number and sophistication of attacks targeting them will continue to grow in parallel.

About the Author

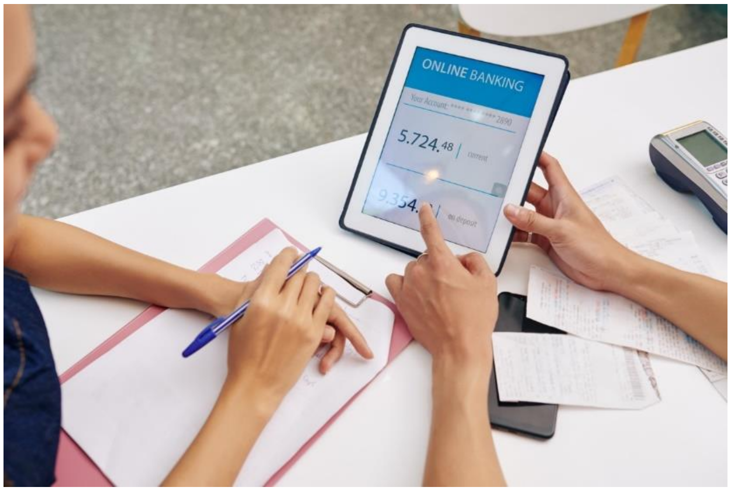
Gnanaprakasam Pandian, Chief Product Officer and Co-Founder of Ordr. Pandian has more than 20 years of product and engineering leadership experience and is also a serial entrepreneur. Before founding Ordr, he was the Chief Development Officer at Aruba, responsible for all of engineering and product management functions. Aruba, an enterprise mobile wireless company, was acquired by HPE for $3 Billion in March 2015. Before Aruba, Pandian served as the head of engineering for Cisco's multi-billion-dollar Wi-Fi business unit and before that as VP of engineering for low-end switching product lines. He graduated with a master's degree in Electrical Engineering from IIT, Chennai, India and holds several patents to his credit in various networking technologies.

He can be reached online at GPandian@ordr.net, on Twitter at @ordrofthings, and on LinkedIn at https://www.linkedin.com/in/gpandian/, and at our company website is www.ordr.net.

Financial Institutions Leveraging CIAM Benefits to Scale Customer Experience and Brand Equity

By Balraj Dhillon, Director – Engagement & Delivery, Simeio

Financial Services is one of the best-known use cases of IAM. With ever-increasing regulations, protocols, and complexities surrounding the industry, adopting the latest and the best tools to manage Customer Identity and Access Management (CIAM) has become critical for businesses. New report from TransUnion has found an alarming spike in fraud attempts targeting the financial services industry. Compared to the last four months of 2020, suspected digital fraud attempts increased by 149% in 2021 in financial services. For financial services organizations, in such a scenario, there is constantly tremendous pressure to ensure their customers are safe from such identity theft attempts. As part of digital revamps that financial institutions are engaged in, scaling their CIAM programs becomes mandatory to keep up with changing security briefs and trends and protect their brand equity. Whether it is a large or mid-size financial services organization, customer expectations from their digital experience have changed. And with Covid, the digitized world has become more relevant than ever before, driving significant investments. The increase in demand for self-service tools has led to customer identity and access management becoming a top priority. So, some digital features and access that were "nice to haves" are now an absolute necessity for increased brand loyalty and trust. According to Forrester analysts (reported in Gauge Your Identity and Access Management (IAM) Program Maturity, August 2nd, 2021), *"Without effective CIAM strategy customers and prospects will take their business elsewhere and cost you revenue."*



Customers want financial institutions to prioritize great user experiences. They also want brands and organizations to protect them from fraud, breaches, and privacy violations. CIAM enables this functionality by bringing features such as customer registration, service account management, consent, single sign-on (SSO), multi-factor authentication (MFA), and data access governance. One of the leading financial services organizations has implemented customer-focused, digital transformation programs and prioritized CIAM.

Coastal Capital Savings, the largest member-owned financial cooperative in Canada with more than 500,000 members, is aiming to enable digital interactions, driving seamless customer experiences, and onboard users in a digital capacity safely and securely. According to **Stephen Pedersen, Director, Information Security, Coastal Capital, "***Customer needs have changed where simplicity, transparency, and security is critical for them, when interacting with a financial service provider. The question is how do we ensure that these are addressed, and customers access applications efficiently and seamlessly? Customer identity and access management (CIAM) thus became integral in the modernization and transformation of our applications to ensure accessing applications for customers remain effortless without compromising security. Our legacy services needed to modernize its interfaces and integration patterns into CIAM which was a priority to offer the best experience for our customers***."**

When talking about customer data security and financial transactions, a strong CIAM program must provide the highest level of security and a seamless customer experience no matter which channel (web, mobile, etc.). In terms of investments, financial institutions are not wary of the fact that significant investments are required to achieve the desired digital experience for their customers. Canadian financial institutions have reportedly spent over C$100 billion on technology to provide customers digital banking platforms. In a Forrester research, (reported in The Top Trends Shaping Identity and Access Management, July 12th, 2021) 62% of respondents comprising of senior decision-makers, indicated increasing their budget by at least 1% in Customer Identity and Access Management. 31% of respondents said they would increase the same by at least 5%, and 72% of organizations either already adopted it or will have it between 2025. Undoubtedly, CIAM is an area that is increasingly becoming a focus to achieve a robust, and seamless customer experience that significantly impacts brand equity. CIAM adoption and customer experience are increasingly becoming a basis for competition. It will not be an exaggeration to say that to offer the best and an end-to-end customer experience, a robust CIAM investment will form a critical part of the overall technology spent.

About the Author

Balraj Dhillon is a Director, Engagement & Delivery at Simeio. As a cyber security leader, he leads customer engagements, technology delivery, and product advocacy across IAM deployments. Prior to joining Simeio he co-founded a patient engagement healthcare startup, that delivered natural processing (NLP) experiences to solve patient engagement using voice and chat-based interfaces. He also served as Director of Product at Ontario Health, where he led multiple cyber-security and identity modernization initiatives focused on consent, privacy, healthcare provider identity and API gateway for a system that aggregated over 7 billion electronic health records. Balraj has a robust background in developing, deploying, and positioning products/solutions across multiple domains.

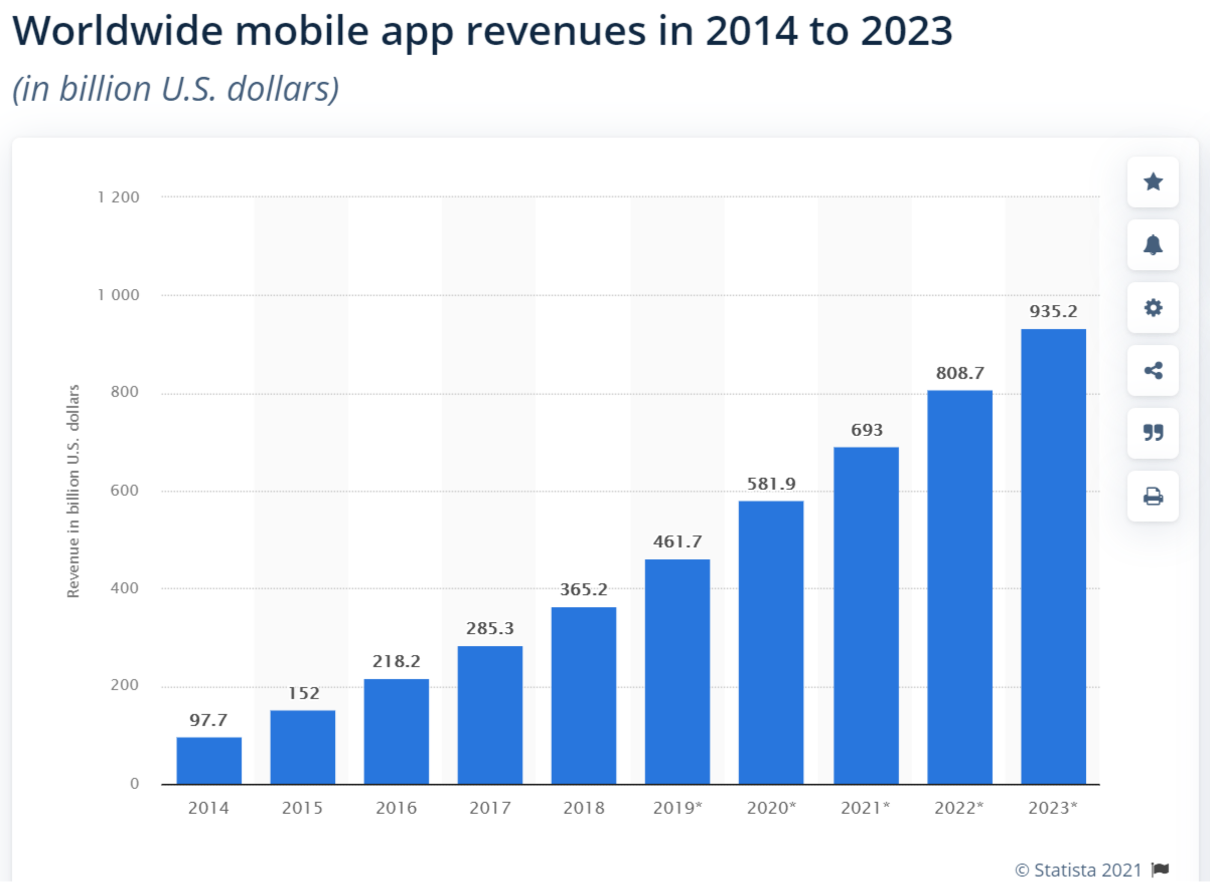
First Name can be reached online at bdhillon@simeio.com and at our company website http://www.simeio.com/

How Certificate Pinning Helps Thwart Mobile MitM Attacks

By David Stewart, CEO, Approov

The massive deployment of mobile apps is presenting new attack surfaces to bad actors and the API channel between the apps and backend services is one of the 5 defined attack surfaces in the ecosystem. In this article we will explore the challenges of defending this channel and outline some practical steps you can take to put immediate protection in place.

Mobile app usage has been increasing year on year and that seems unlikely to change. As shown in the chart below, direct revenue derived from mobile apps is also showing impressive growth. Most consumer facing enterprises now have a mobile app since it is the preferred touchpoint for their customers and even if those apps don't generate revenue directly for the company, trust in the mobile app platform is vital for brand reputation.



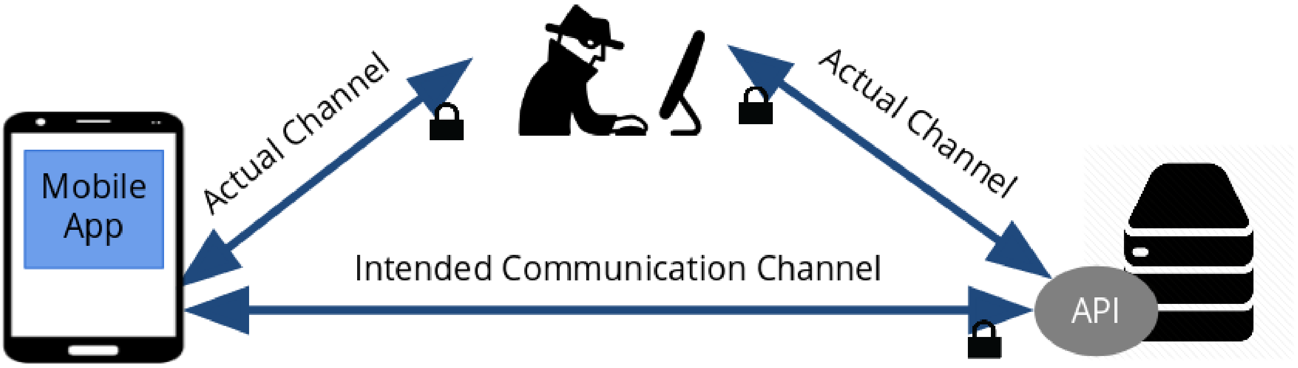
(Image source: Statista)

Attacking the API channel between mobile apps and their backend servers through Man-in-the-Middle (MitM) attacks are a growing threat for mobile users. The ability to intercept and manipulate communications between mobile devices and servers is an issue that has been known for some time and, backed by the explosive growth in mobile app usage, it has become commonplace. In spite of this, many enterprises are not clear on effective and efficient ways to combat these attacks.

In the following sections, we'll look at how certificate pinning can help thwart mobile MitM attacks, as well as the pros and cons involved with static versus dynamic pinning, and what else you could do to protect your organization's data and revenue from these types of exploits.

Man-in-the-Middle Attacks - A Brief Explainer

Man-in-the-middle attacks are when an attacker intercepts or manipulates mobile device communications to gain access to sensitive information. The bottom line is that they give attackers the ability to see any communications, modify messages using the channel, steal login details or certificates from encrypted traffic, intercept sensitive commercial/personal data, or even launch a denial of service attack against the service being accessed via a mobile app with ease.

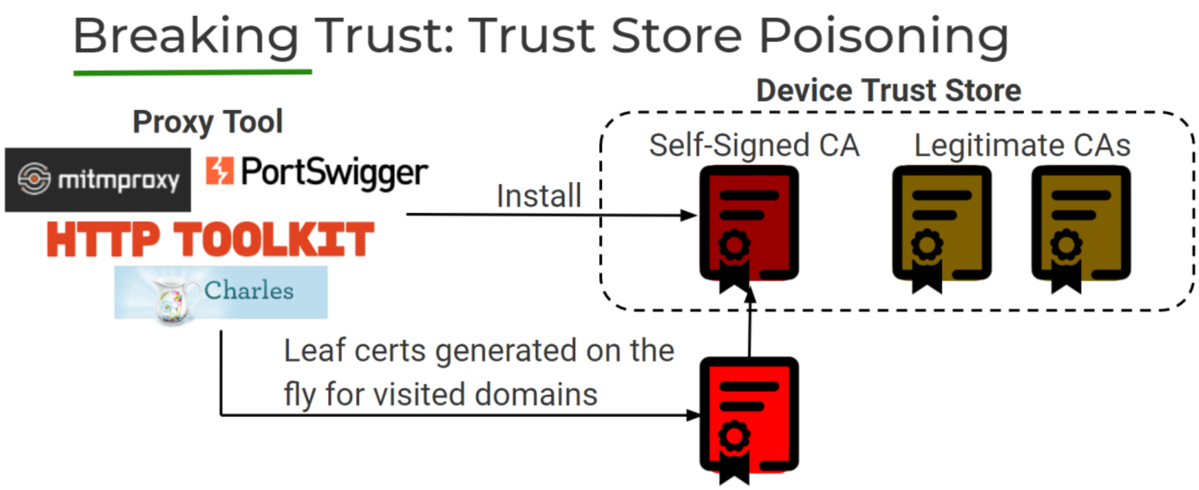


(Image source: Approov)

You might be wondering about the fact that API traffic is normally encrypted using TLS (Transport Level Security). You are right and in TLS there's a whole protocol around ensuring that the mobile app thinks it's talking to a legitimate backend server. However, a MitM can insert themselves into the channel such that the mobile app ends up talking to the MitM actor over an encrypted channel thinking that it's actually the backend server. Thus, the MitM can see all the traffic, potentially modify the traffic, and then transmit that on, again over an encrypted channel back to the backend service. Let’s look at how TLS is supposed to work and how it can be manipulated.

When a communication is made from the app to the backend service, there is a certificate that is on your server that's part of an overall trust chain that proves the legitimacy of that particular server and that it actually belongs to the person you say it belongs to. This uses public key infrastructure (PKI) and during the negotiation, a number of different certificates are presented and are checked by the client to prove that they are correct, and this follows a trust chain that ultimately needs to lead to a root certificate authority. The anchor point in terms of trust is the fact that there are a number of certificates which are essentially pre-installed and updated on the mobile device itself from certificate authorities and you only accept the traffic if you have a chain of trust leading there.

Now, there are a couple of ways that this trust chain can be subverted. One way is to use a MitM tool, of which there are many, such as mitmproxy. In such cases you’ll be analyzing traffic from a mobile app and you're also controlling the device. Tools such as mitmproxy create a certificate that is installed onto the end user device. Rather than being a certificate from a root certificate authority, it is actually a self-signed certificate that the tool has made up. You install it into the trust store on the device and then when the tool intercepts traffic, on the fly it will create leaf certificates for the particular domains that you are visiting, which have a chain of trust back to the self-signed certificate authority that you have put on the device. Thus, everything will check out on the trust side and the traffic is redirected to the MitM rather than actually going to the server. From there the MitM will then connect to the real server, allowing the traffic to continue but actually there's this proxy in the middle that's seeing all the traffic. You can replay the traffic and you can now modify the traffic if you want.



(Image source: Approov)

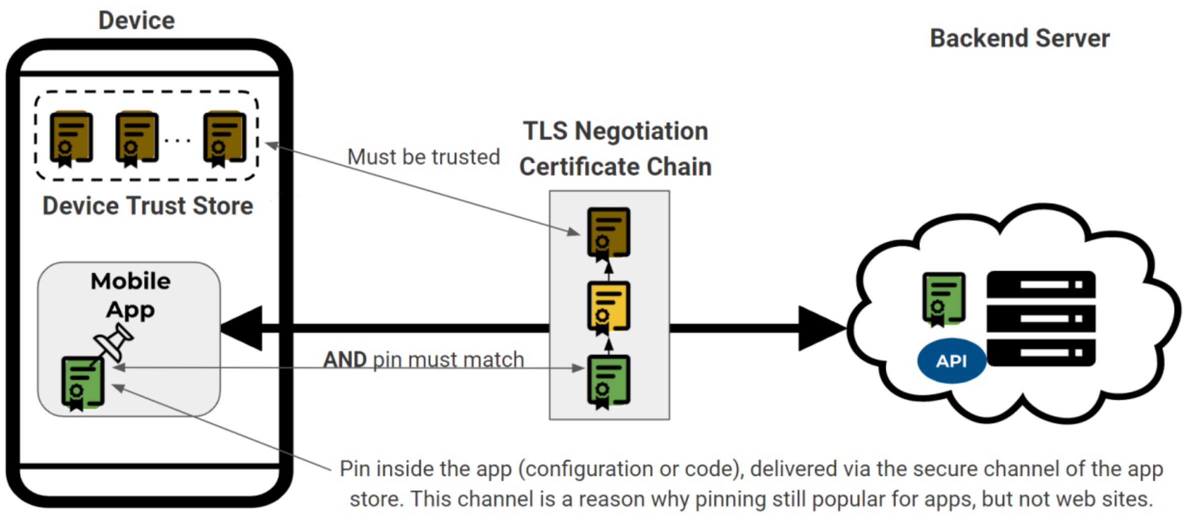
The other way that you can break the trust is if there has been a breach of a certificate authority or a bad issuance of a certificate. One of the weaknesses of the PKI architecture is the fact that there are a large number of root certificate authorities that are installed on the device and if there's a breach in any of those then that could lead to a situation in which a certificate for a domain that you're connecting to you could have an attacker certificate incorrectly issued.

So the trust is only as strong as the weakest link.

The Benefits of Certificate Pinning

Certificate pinning helps mobile app developers protect mobile apps from the MitM attacks described above. However, despite its usefulness, it isn't widely used.

Certificate pinning allows mobile applications to restrict communication only to servers with a valid certificate matching the expected value (pin). The connection is terminated immediately if communication is attempted with any server that doesn't match this "expected" value.


Device
Backend Server
TLS Negotiation
Certificate Chain
Must be trusted
Device Trust Store
Mobile App
AND pin must match
API
Pin inside the app (configuration or code), delivered via the secure channel of the app store. This channel is a reason why pinning still popular for apps, but not web sites.

(Image source: Approov)

In the past, certificate pinning has been challenging to implement and highly reliant on the networking stack in use. DataTheorem's TrustKit, as always, has been a fantastic tool for putting it into action. However, Google and Apple have recently enhanced their platforms to simplify the process, removing any dependency on the network stack.

Since Android 7, Google has supported pinning. Developers simply define pins in the file's particular XML syntax. Apple has lately followed suit and added NSPinnedDomains support with iOS 14. Developers may add Pins by entering them in the Info.plist file for the app in the correct format.

There's now some solid platform support, but the configuration part is tricky, especially if you're not familiar with PKI and certificate management. The majority of the setup is based on issuing numerous complex OpenSSL commands and managing certificate files in various formats.

If you want to get started with understanding and implementing certificate pinning, this free Pinning Generator Tool makes it simple to generate and maintain pinning configurations for mobile apps, ensuring that they are kept up to date on Android and iOS.

Static Pinning Risks

Unfortunately, certificate pinning isn't quite the panacea for preventing MiTM attacks, particular for mobile. There are certain risks where a certificate pin is set statically as described above. For example, when you hardcode the pins into an app before releasing it, there are a few things to consider:

- If somebody with malicious intent gains access to one of your private keys that have been used in production, they could then use this key on any other server linked to your mobile application and have complete control over all communications from users' devices, without them knowing anything was amiss;

- If you make changes (for instance, by changing encryption algorithms), old versions of the code using static pinning will break;
- If there is a problem with the pins in your mobile app and you release an updated app, users will remain vulnerable until they get around to updating it.

A good example of a situation where static pinning was disastrous is the 2016 Barclays Bank UK incident. The bank's mobile application had been pinning an obsolete intermediate certificate in the mobile application - making transaction authentication impossible. Hundreds of thousands of consumer payment transactions were affected due to the outage, which prevented many small and medium-sized enterprises from conducting important transactions. As a result, many companies had to close their doors at 8:30 am on 25th November 2016 (Black Friday) and for the rest of the festive period leading to immense financial losses. In addition, it had a significant negative impact on Barclays' reputation and its business customers.

The Need for an Alternative Pinning Approach

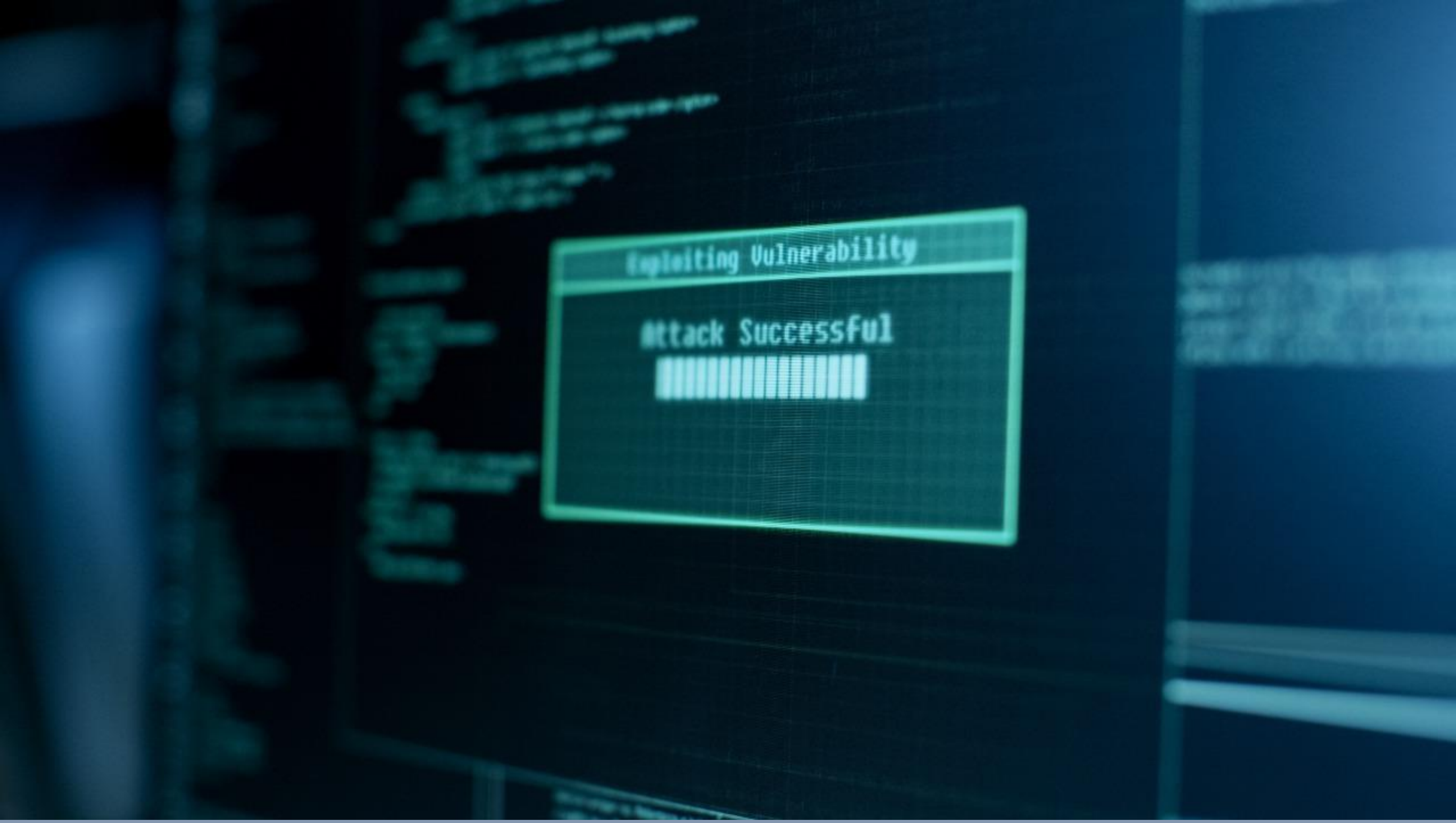
What mobile app developers need is a way to pin certificates that don't require static pins. Instead, mobile applications should have access to dynamic or live pinned certificates from an online service so they can be updated automatically on the fly - without having users download and install updates for their apps every time there's a change in security infrastructure.

Essentially, this approach allows mobile application developers to stay one step ahead of hackers by keeping up with changes in certificate authorities' keys over time while minimizing downtime due to misconfiguration, avoiding any potential reputational damage among consumers that could lead them away from using your business' mobile offering altogether.

This would allow developers and DevOps teams to avoid further incidents like Barclays' and improve customer experience over mobile. Certificate pinning must be implemented for all APIs that service mobile apps in industries which handle commercially or personally sensitive data. Trust is a major factor in mobile security, and app developers need to do everything they can to protect their customers from cyber-attacks while also maintaining trust among their users that the mobile application has been designed with privacy and data protection as top priorities.

About the Author

David Stewart is CEO of Approov. He has 30+ years' experience in software security, mobile apps/APIs, embedded software tools, design services, chip design, design automation tools, technical support, marketing, sales, fundraising, executive management & board advisory roles. Current focus is growing a business delivering revenue assurance for enterprises reliant on mobile channels to reach their customers. Approov is a SaaS security solution preventing APIs being accessed by anything other than genuine instances of your mobile apps running in a safe environment. David can be reached at @approov_io and https://approov.io/



What Do Spear Phishing Attacks Look Like In 2021?

Understanding the Threat Landscape in 2021

By Tim Sadler, Co-Founder & CEO, Tessian

You don’t need to tell me that the security threat landscape has changed a lot over the last two years. Fuelled by global pandemic and a widespread shift to online operations, cybercriminals have changed their tactics once again to target businesses and their remote workers.

And one of the top ways to target employees has been phishing attacks. Not the bulk spam and phishing attacks that have become easier to spot, though. We have seen a rise in highly targeted spear phishing emails, which are designed to bypass existing email security defences and manipulate people into complying with cybercriminals’ malicious requests.

In fact, Tessian’s recent ‘Spear Phishing Threat Landscape 2021’, revealed that two million malicious emails landed in employees’ inboxes, having slipped past defences like Secure Email Gateways (SEGs) and native tools between July 2020 and July 2021. This rendered people as a company’s last line of defence and, consequently, left organisations vulnerable to costly cyberattacks like business email compromise or ransomware.

It's not that people aren't smart enough to spot a scam when they see one. The problem is that today's advanced phishing attacks are difficult to detect, given that they don't contain the tell-tale signs that employees are told to look out for. When you then add in the fact that cybersecurity is rarely front of mind for all employees and that many are distracted by their overwhelming to-do lists, you can hardly expect on every employee to spot every malicious email that they receive – even with training. For example, in a previous report, we revealed that 45% of people had clicked on a phishing email at work because they were distracted.

So how are these emails bypassing existing security solutions and which employees are most likely to be targeted?

Who is being targeted?

According to our data, an average employee receives 14 malicious emails a year and cybercriminals aren't picky when it comes to company size, with our researchers finding that SMBs and enterprises are targeted in equal measures.

However, employees in the retail industry were prime targets, with the average worker receiving 49 emails per year – making retail the most targeted industry during this time. People working in manufacturing received the second most at 31 emails per employee, per year. To put this into context, an employee in the retail industry would have to successfully identify up to 50 carefully crafted emails a year to avoid causing a serious security incident.

That's not so easy when the emails are crafted using sophisticated techniques to avoid detection. These include display name spoofing, whereby the attacker changes the sender's name to someone the target recognises; domain impersonation whereby the attacker sets up an email address that looks like a legitimate one, and account takeover attacks where a bad actor poses as a legitimate customer or employee, gains control of an account and then makes unauthorised transactions.

When are they being targeted?

We're often told that bad actors borrow best practice from marketers. If that's the case, most phishing attacks would land in employees' inboxes around 10AM on Wednesdays, but our research revealed a different story.

The most malicious emails are delivered between 2PM and 6PM, with very little fluctuation day-to-day (except over the weekend). This isn't an accident. Since employees are more likely to make mistakes when they're stressed, tired, and distracted, the second half of the working day is likely a bad actor's best bet.

Our report also suggests that employees need to keep an eye out key calendar events in the year, as cybercriminals jump on key trends or holidays as lures in their attacks. For example, last year, the most malicious emails were received on the days surrounding Black Friday, one of the busiest days for online shopping.

How are they evading detection?

Employees – and the traditional security defences in place to protect them – typically rely on a set of guidelines and rules to determine whether something is malicious. For instance, does the email have a suspicious attachment or link? Does the message contain certain words that signal a threat? Does the sender's domain contain incorrect characters?

Cybercriminals are aware of these rules - and they are doing everything they can to reverse engineer the rules and remove these tell-tale signs from their campaigns to evade detection.

In our report, for example, 75% of the malicious emails we detected and analysed didn't contain an attachment.

Zero payload attacks, which don't rely on a malicious payloads like attachments or links, were used instead – a technique whereby the attacker builds a rapport with victims over time and persuades them to action a request once trust is established. Zero payload attacks can be as devastating as malicious payload attacks, and traditional antivirus and anti-phishing software – which often rely solely on keyword detection and deny/allow lists – struggle to detect them every time.

What's more, our researchers also found examples of account takeover – a type of attack whereby a cybercriminal sends an email to their victim using a legitimate account that they hacked into previously. To all intents and purposes, the sender's email looks like the real deal. There would be no reason to flag it as malicious – if you're relying on rules to detect threats.

To sophisticate cyber defence policies, then, business decision makers must ensure employees are trained and made aware of the types of threats they could be exposed to. The training must be delivered regularly, if they are to keep up to date with the evolving threat scape.

But it's unrealistic to expect your employees to spot every threat, every time. Regardless of training, employees are prone to mistakes and can be tricked. So, businesses must also consider how to bolster their defences to keep the bad guys out of the inbox. Rules are not enough. For advanced threats, you need advanced machine intelligent security solutions which can detect, and flag, potentially malicious emails based on people's behaviours on email and alert employees before it's too late.

This advanced and layered approach to email security is critical as cybercriminals continue to evolve their techniques to bypass detection and deceive people using phishing attacks.

About the Author

Tim Sadler is the CEO and co-founder of Human Layer Security company Tessian. He leads the company to achieve its mission of securing the human layer and empowering people to do their best work, without security getting in the way. Since starting the company in 2013, Tim has raised $127m from leading VC funds and he has grown the company across the UK and US.

Tessian can be contacted via tessian@centropypr.com, or at our company website https://www.tessian.com/

Keeping Your Guard Up: Protecting Against Inherent Trust Risks

Important steps to identify inherent trust in the risk management process

By Zubaid Kazmi, a managing director in MorganFranklin Consulting's cybersecurity practice

Trust is a huge problem in cybersecurity. Whether gaining access to a building or infiltrating a computer network, anything can be breached with the right credentials. While implementing multiple identity zones is a good measure in the zero-trust playbook, a bad actor that can get through a first checkpoint, can certainly make it through the second. This is why implementing a second checkpoint that requires biometric verification or requests information only the real employee would know is vital for security. Meanwhile, most organizations still inherently trust the strength of their verification processes, and this trust extends to what happens once an intruder is inside the organization.

The Risks of Inherent Trust

In a world where it is increasingly difficult to trust that an identity is true and not compromised, models like "zero-trust" are catching interest and frequently being implemented. The best way to approach zero-trust within an organization is by being **intentional** about trust. This goes beyond traditional authentication and access governance use-cases. It extends to the supply chain of identities, organizations, and services. It also goes beyond just third-party risk management and starts delving into fourth-party risk management. Truly protecting an organization means thinking about zero-trust as an assessment of where there is inherent trust across business processes, contractual agreements, systems integrations, and (yes) identity and access controls.

When designing and implementing systems, policies, and processes, organizations commonly make assumptions about the security and trustworthiness of the applications, systems, partners, and other entities that they work with. A billing application logically needs access to customer data to do its job. However, this doesn't mean that this is all the application does with this data.

An application may be created by a reputable manufacturer, but this does not ensure it is secure. As incidents like the SolarWinds and Syniverse hacks have demonstrated, supply chain and third-party risk are major security threats. Simply by using a particular application and granting it the access and permissions necessary to do its job, an organization inherently places trust in that software, its manufacturer, the manufacturer's suppliers and partners, and so on.

These inherent risks are not limited to external supply chains and third-party risks. Employees and systems within the organization can be inherent risks as well. For example, access to a company's financial records may be explicitly granted to members of the finance department. However, these records are stored, processed, and transmitted on infrastructure managed by the IT department. By using computer systems, organizations inherently place trust in their IT department, its processes, and its security against cyber threats.

Syniverse: A Case Study in Inherent Trust

The recently reported Syniverse hack is a prime example of the risks of inherent trust. Syniverse is an SMS routing company that transfers SMS messages between the networks of major carriers (T-Mobile, AT&T, and Verizon). On October 6, 2021, the company reported in an SEC filing that it discovered in May 2021 that an attacker has had access to its systems since May 2016.

Syniverse has access to the contents of all text messages sent via its platform, and, while there is "no indication" that the attacker had access to these messages, it is certainly a possibility. Companies using SMS for business communications are not only trusting their own carrier to protect the confidentiality of their communications. They are also inherently placing trust in companies like Syniverse often without even knowing it.

How Security Initiatives Fall Short

Security initiatives are commonly designed to address a specific issue. Initiatives can be reactive, addressing regulatory compliance failures or vulnerabilities that lead to cybersecurity incidents, or proactive such as an attempt to implement a zero-trust security model.

In most cases, these security initiatives boil down to deploying a solution to solve a problem, such as using encryption solutions to improve data privacy and security. However, without the necessary context and a holistic approach to the problem, these solutions may not actually fix the issue they intend to solve and could potentially make things worse.

Often, inherent trust and its associated risks are a vital missing piece during this decision process. A failure to appropriately assess an organization's inherent trust and take appropriate precautions can create significant security risks that undermine the effectiveness of the original solution. Encryption provides no benefit if an attacker can access the decryption keys.

Effectively Managing the Risks of Trust

Inherent trust – and its associated security risks – are inescapable. It is impossible to do business without placing trust in some systems, applications, users, etc.

However, this is not to say that organizations should blindly extend this trust. The risks of inherent trust should be a core part of corporate risk management calculations and categorized, addressed, or accepted just like any other type of risk.

Gaining the visibility into the corporate supply chain needed for effective management of inherent trust can be difficult. Many companies struggle to manage their third-party risks, let alone fourth-party and beyond.

Acknowledging and attempting to identify inherent trust when it occurs is an important first step in the risk management process. By examining security initiatives in context – looking at both upstream and downstream effects – and attempting to limit and manage inherent trust when possible, an organization can dramatically reduce the impact that inherent trust poses to its overall level of risk.

About the Author

Zubaid Kazmi is the Managing Director for Identity and Access Management at MorganFranklin Consulting. Prior to joining MorganFranklin, Zubaid held managing director and director positions at large and boutique consulting firms with a specific focus on Identity & Access Management and Digital Identity governance. Combined with over 20 years in professional service, Zubaid brings his experience advising clients on how to realize their IAM transformation objectives while advancing their compliance, security, and business initiatives.

Zubaid can be reached online on LinkedIn and at our company website https://www.morganfranklin.com/services/cybersecurity/

Empowering Your Employees To Prevent Cyberattacks In A Remote Work Era

By Bill DeLisi, CEO of GOFBA – a leading secure search engine and communication platform

Cybercrime's business impacts reached $1 trillion in 2020. This staggering sum represented around one percent of global GDP. It reflected the total costs incurred with implementing security measures, lost productivity and profits, ransomware payments, and other considerations. Cybercrime is a global problem that impacts companies big and small. An August 2021 survey from CNBC found 56 percent of small business owners were concerned about an attack, and 59 percent of those surveyed were majorly confident they could quickly handle any attack. However, only 28 percent had a plan in place to combat cybercrime, and many of those plans would likely prove insufficient against a sophisticated hacker group.

For small business owners and managers, overconfidence about preparations and capabilities, and a lack of concern are a troublesome mix. To fix this dynamic, they need to focus efforts on preventing cyber intrusions. The best place to start is by focusing on staff members actions, as *people* are often the conduit for hackers through phishing schemes, malware, and personal devices.

Stop Phishing in its Tracks

The Delta variant COVID-19 surge prompted cybercriminals to develop fake “vaccination requirement” emails. These phishing schemes were sent to millions of workers, with official looking forms and links asking for recipients to confirm their vaccination status while providing valuable personal information. It is a common tactic for phishing schemes to prey on people’s fear and uncertainty along with a message of urgency and possible consequences.

Hackers enjoy phishing schemes because they are easy to deploy and can provide fast access into networks. The recipient clicks a link or opens an email or an attachment, and that launches malware which can infect a computer and give the hacker administrative control. And, once they have control, they encrypt the data and hold it for ransom.

Preventing phishing schemes requires staff training. They need to understand the risks of opening emails and downloading attachments from unrecognized senders. Be sure to conduct training sessions with images of phishing emails, pointing out common tricks like misspelled URLs, poorly constructed sentences, and other signs of non-genuine emails.

Here are some other signs of phishing emails employees should be aware of:

- URLs do not match the purported business. Users can hover over the URL (place your curser over the URL or email address) to see the *real* destination or address
- Emails asking for Social Security Numbers, bank account information, and other personal data are always fake
- Emails that attempt to elicit panic and suggest the recipient ‘must act’ are always suspicious
- Phishing schemes often change to reflect current events, such as vaccination, political decisions, COVID “cures”, and other hot topic issues

For employees, deletion is *always* the answer. If there is any doubt about the veracity of an email, they can simply contact the organization or individual that sent the message. Institute a policy that no worker will be in trouble if they delete a genuine email if they thought it came from a shady sender.

Managing Remote Workers: Flexibility vs. Safety

It is obvious remote work is here to stay. For new hires it is now considered a standard condition of employment, instead of a rare sought-after benefit. With remote work comes inherent hazards for businesses to manage devices and employee actions as they relate to cybercrime risks. Ideally, business owners will provide employees with dedicated laptops and phones for work. These will come preloaded with malware protection, firewalls, and strict access points for reaching company data. It is a better route than ”BYOD” as workers tend to use their own devices for riskier behaviors that can offer convenient entry points for bad actors.

There is also privacy and support benefits with corporate-provided devices. IT can control company property without worrying about stumbling across an employee’s photos or their Facebook posts.

Corporate devices enable uniformity in terms of software updates and patches as well as phone and computer OS versions.

Remote workers should also utilize encryption software for all their data production. This protects them and the company against loss or theft, either virtual or physical. They can also leverage encrypted internet connections, with end-to-end encrypted email and file sharing that protects data in transit when it is most vulnerable.

Business owners and managers offering remote work need to construct clear policies for all electronic activities. Give them examples of why policies are needed, including how hackers can use devices, Wi-Fi, and other conduits that may cause harm. The policies should include devices, VPN access procedures, and password creation and usage. Utilizing secure communication and file sharing platforms (such as GOFBA) within the office can help mitigate threats and other phishing schemes within the company. Consider making two-factor authentication mandatory to reduce password-related exposures and require employees to change passwords on a regular schedule. Within policy documents, you can include context for why stringent controls are needed. Detail how ignoring or "going around" these controls could mean an end to the remote work benefit and irreparable harm to the company's future.

About the Author

Bill DeLisi is one of the world's most authoritative experts on cybersecurity. He is currently the Chief Executive Officer, Chief Technology Officer and a founding member of the Board of Directors for GOFBA, Inc. DeLisi has more than 30 years of experience in the computer industry, including holding the position of Chief Technology Officer at several companies. He has worked closely with Microsoft Gold Certified Partners, helping pioneer "cloud" computing and creating security infrastructures that are still in use today. DeLisi is responsible for the development of proprietary technology that serves as the backbone of GOFBA's platform and has over 30 certifications with Microsoft, Cisco, Apple, and others, which includes the coveted Systems Engineer with Advanced Security certification, as well as expert status in Cloud Design and Implementation.

Bill can be reached online at www.GOFBA.com.

Lateral Movement – The Key Element in Advanced Attacks

Understanding lateral movement techniques in advanced cyberattacks and how to fight back

By Jon Murchison, founder and CEO, Blackpoint Cyber

Advanced Attacks on the Rise

When the pandemic made its impact around the globe early last year, it simultaneously ushered in an exponential surge in cybersecurity attacks. In the scramble to mass-migrate businesses to virtual work environments, many did not have the time nor resources to implement strong cybersecurity policies and processes. This climate has allowed attacks in particular to boom in nearly all industry verticals, impacting critical infrastructure, utilities, transport, food supplies, healthcare, education, and the US economy at federal, state, and municipal levels.

Advanced cyberattacks are now considered a risk to national security following the sweeping uptick in cyberattacks. Once targeting small companies or individuals, threat actors are now making headlines by growing their attack radius to include major infrastructure companies and even leading security firms. What's more is that threat actors are quickly evolving their tactics and targets when it comes to deploying their cyber assaults.

Understanding Lateral Movement in APTs

Advanced persistent threats (APTs) are seeing increased success due to lateral movement techniques. When threat actors infiltrate a network, the initial, vertical entry seldom causes damage. Actors are likely to break in through low-level web servers, compromised email accounts, or a poorly protected endpoint device. The real damage begins once the actors secure their foothold and start to pivot laterally through the rest of the environment to find and reach their targeted assets. Examples of lateral movement techniques include:

- Exploiting remote services
- Remote service session hijacking
- Pass the Hash (PtH)
- Pass the Ticket (PtT)

By taking advantage of one vulnerability, threat actors use lateral movement techniques to access many systems within an IT environment, obtaining the privileges and access they need along the way to their target. While pivoting laterally, actors will utilize anything they come across that may help them access a targeted asset more efficiently. By leveraging built-in operating systems and other IT policies and support tools that your business already uses day-to-day, they can save their own resources and evade detection, appearing as anomalous network activity.

Lateral movement is a critical element in the execution of long term, advanced attacks. Rather than just compromising a single asset or target, threat actors use these techniques to establish a persistent, malicious presence in their victim's environment.

How to Fight Back Lateral Movement

Lateral movement attacks are extremely fast moving with many proving successful for the threat actor in less than one day. To fight back, live detection of privileged lateral movement is a must. In the last year alone, Blackpoint Cyber only saw next-gen anti-virus and EDR alerts in 14% of the attacks stopped – experts at defending must be able to quickly discern between normal IT operations and hijacked IT operations. Most companies are unable to detect lateral movement because it is lost among the regular traffic of daily network traffic and operations. Even platforms such as SIEMs (Security Information and Event Management), advanced analytics tools, anti-malware, and anti-virus solutions have proven inadequate at catching this phase in the attack lifecycle.

However, it is during the lateral movement phase that threat actors are most vulnerable to detection. Having the right tools and cybersecurity best practices in place can minimize the chance of infiltration and, in the case of a breach, detain the actors before they can take root and devastate your business. Below are the three core elements needed to prevent lateral movement:

Purpose-Built Managed Detection & Response (MDR) Platform

When an attack occurs, detection and response times often determine whether the actors succeed in their efforts. To combat the sophisticated attacks occurring in today's cyberthreat landscape, investing in an around-the-clock true Managed Detection and Response (MDR) service means that you can fight back within minutes and hours, not days and weeks. MDRs can help close the gap between the identification of an event and the actual response and remediation. By immediately shutting down or isolating endpoints, MDR analysts can terminate malicious processes, delete bad files, and stop the threat from moving laterally into other systems.

Combining both prevention and advanced tradecraft detection technologies means that you can monitor your account activity and behavior in real-time; a critical factor in staying ahead of threat actors. 24/7 active threat hunting and response service provided by experienced analysts can detect reconnaissance activities at their earliest stages. With monitoring, detection, and response executed in tandem, MDR analysts have unparalleled visibility into hacker tradecraft, lateral spread, and remote privileged activity.

Proactive Threat Hunting by Experienced Analysts

Threat hunting is the practice of being proactive in the search for cyberthreats within an organization's network. It is performed deep within the network to deliberately search for hidden actors and malware that may have found a way to exist undetected otherwise. Many organizations invest in various managed services and tools in defense, but MDR threat hunting is a crucial, offensive strategy. Threat hunting has three main components:

- Investigation through threat intelligence and hypothesis
- Analysis of Indicators of Compromise (IoC) / Indicators of Attack (IoA)
- Machine learning and advanced telemetry

Threat hunters are highly-specialized and trained specifically in hacking tradecraft. They always take an 'assume breach' stance and investigate thoroughly to find evidence of suspicious behavior or changes that may indicate the existence of threat. These threat hunters rely on security experience and human

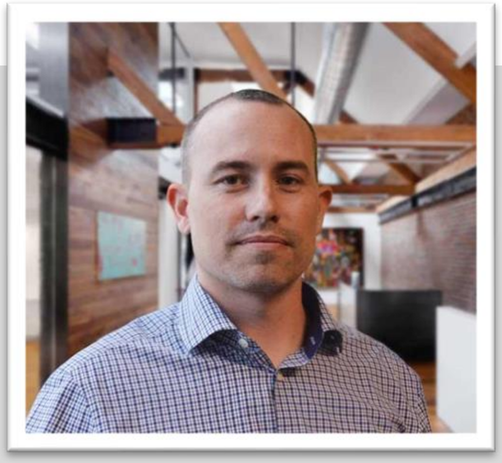
analysis of current threat tactics, techniques, and procedures (TTP) to instigate hypothesis-driven hunts. The human-powered element is a vital link that synchronizes collected threat intelligence, data logs, and advanced security technology towards safeguarding your business.

Strict Cybersecurity Hygiene & IT Best Practices

Set your business up for success by adopting tried and true cybersecurity hygiene practices. When consistently executed, they can help prevent breaches from occurring at all. This is especially true for the IT world as even one breach could be detrimental to your operations. Here are some examples of cyber hygiene best practices you can implement to strengthen your in-house security and fight back against lateral movement:

- Implement a principle of least privilege (PoLP) and zero trust model/architecture • Ensure networks are properly segmented
- Practice stringent password management including password complexity, rotation, and expiry • Establish app-based multi-factor authentication (MFA/2FA) for all devices and RMM tools • Keep your software up to date. Ensure that patching and upgrade activities are completed particularly for firewall and VPN appliances.
- Remove internet-exposed remote desktop services (RDP) services

- Run regular vulnerability assessments against all systems on your network



About the Author

Jon Murchison, founder and CEO of Blackpoint Cyber, started his career in network engineering and IT operations but quickly made the switch over to the covert world of the intelligence community. He has since spent more than 12 years planning, conducting, and executing high-priority national security missions. As a former NSA computer operations expert and IT professional, he brings a unique perspective to the mission of developing cyber defense software that effectively detects and detains purposeful cyber intrusions and insider threats. Jon has also helmed multiple cybersecurity assessments, including Fortune 500 enterprises and critical port infrastructures. Currently, Jon holds multiple patents in methods of network analysis, network defense, pattern analytics, and mobile platforms.

Jon can be reached online on LinkedIn, and on our company’s website https://blackpointcyber.com/

When Does a Vulnerability Become a Vulnerability?

If a vulnerability exists in a server forest and no one finds it, does it exist?

By Jason Kent, Hacker in Residence, Cequence Security

When I worked in vulnerability management, my role was to scan an organization's environment for network vulnerabilities. We would analyze the devices found and create a list of things that needed fixing. During one such engagement, I found something that made me stop and immediately report a vulnerability that needed to be fixed that day.

The manager didn't want to hear it. I tried to explain the machine was externally facing, had a flaw that was trivial to exploit, and I was cut off with, "If I know it is there, I am culpable to fix it. I'd prefer to not scan at all."

If a vulnerability exists in a server forest and no one finds it, does it exist?

A vulnerability is simply an exposure to a possible attack. The network manager I spoke about was placing all of his "if" on "possible": "If they don't attack, we are good." The problem with this type of "head-in-the-sand" approach is it rarely works.

As an example, BrewDog was recently notified that someone had figured out how to dump their entire customer database via their mobile application APIs. In addition to enabling customer account takeovers, the researcher figured out that they could generate unlimited free beer utilizing the entire customer base of coupons. BrewDog didn't believe the vulnerability existed and didn't acknowledge the report. The information was made public and BrewDog is dealing with significant fallout.

This year, I did some similar research on the well-known Lithium community forum platform, which is now owned by Khoros. Lithium is a multi-tenant SaaS architecture used by many organizations including Roku, DropBox and FitBit to host user forums. If you are logged in to FitBit, then you are using Lithium, configured as a public community, to share results, discuss workout regimens, and so on.

While logged into the FitBit Community I noticed a weird request being made by my browser:

```
GET
/xmnuz23762/api/2.0/search?q=SELECT+id,+login,+avatar.profile,+rank,+view_href+FROM+users+WHERE+id+%3D+%22REDACTED%22
```

My first thought was that it was strange to find SQL queries in the request, so I wondered if I could change them. My second thought was, "what the heck is xmnuz23762?"

I first tried changing the SELECT criteria and the WHERE information, yielding:

```
GET

/xmnuz23762/api/2.0/search?q=SELECT+*+FROM+users
```

This showed me all users. I found User 1, whose profile showed that they were the Lithium Admin. Now I knew what the FitBit community platform was based on.

Recall that a vulnerability is simply an exposure to a possible attack. So, is this an exposure to an attack? I believe so and here's why.

Exploiting the Flaw

I can change the query to get intended results. This means I can dump various parts of the database at will. Khoros disagrees, stating that what I had found is their API, called LiQL (Lithium Query Language) which uses a syntax similar to SQL. Occasionally, the similarity causes confusion with security experts concerned about SQL injection vulnerabilities. Okay, so it's not identical to a SQL injection, but I can still change it at will and get various pieces of data.

Let's turn our attention to the other oddity I saw: What is xmnuz23762? This alphanumeric sequence is available on every request so it must be related to FitBit. Since this data element was available in each request, I figured it was a domain ID. Querying the DNS entries for Lithium showed that xmnuz23762.lithium.com will redirect you to community.fitbit.com. Pulling a different ID from my DNS entries I found aempf32337.lithium.com, which redirects me to community.roku.com.

So, what if I change my query from:

```
GET

/xmnuz23762/api/2.0/search?q=SELECT+*+FROM+users
```

To:

```
GET

/aempf32337/api/2.0/search?q=SELECT+*+FROM+users
```

The answer is exactly what you think. I get the list of users from Roku. By the way, Roku requires authentication, but I didn't create an account. I just used all the authentication from FitBit to log into Roku and see the users there. This is commonly known as an authentication bypass.

I have now exploited the flaw in the request structure that allows for me to use my FitBit login credentials to bypass the Roku community authentication process. This means that I can observe the Roku forum without logging in, without accepting terms and conditions and I can read any public forum I wish by sending random requests and getting valid responses.

So What?

The question is, is this a vulnerability that enables me to execute an attack? The majority of the organizations that use this platform have requirements for use. FitBit requires you to register, establish a strong password and be over the age of 13. If I do not have to be logged in, then this requirement cannot be enforced. In this single use case alone, I am able to exploit this flaw to bypass terms and conditions. Is bypassing the terms and conditions an "attack"? Maybe or maybe not.

In a public community there is an assumption you are going to share information, but you are also afforded some level of privacy as most forums allow you to configure sharing permissions, yet my research showed that several scenarios were possible:

- A malicious actor could scrape the data off of all of Khoros' public tenants
- A competitor could easily uncover Khoros' customer names and contacts.
- A disgruntled user could use information from posts about product issues to execute a disparaging social media campaign.
- Given the lack of authentication and the ability to view data in the tables, we believe the platform may be susceptible to SQL injection attacks, despite their statements to the contrary.

If you are using a multi-tenant SaaS platform and assuming that platform is secure, but not testing the security of the platform, you might be surprised. Though we played it very safe here to ensure we didn't break anything, I am certain that bypassing authentication isn't the intended use of authentication on the platform.

Now, most security teams would say, “Yes, this is a vulnerability that Khoros should address.” They have insisted it works as designed. The reader can decide for themselves.

About the Author

Jason Kent is Hacker in Residence at Cequence Security. For over the last 20 years, Jason has been ethically peering into Client Behavior, Wireless Networks, Web Applications, APIs and Cloud Systems, helping organizations secure their assets and intellectual property from unauthorized access. As a consultant he's taken hundreds of organizations through difficult compliance mine fields, ensuring their safety. As a researcher he has found flaws in consumer IOT systems and assisted in hardening them against external attacks. At Cequence Security Jason does research, community outreach and supports efforts in identifying Automated Attacks against Web, Mobile, and API-based Applications to keep Cequence's customers safe. Jason can be reached online at jason.kent@cequence.ai and at our company website https://www.cequence.ai/.

How To Bring Your Own Key to Hybrid Cloud Without Losing Control Of Your Data

By Marcella P. Arthur, VP Global Marketing, Unbound Security

Amid the post-Covid increase in cloud spending, hybrid infrastructure remains the preferred option for many organizations. Cost-efficiency, scalability, agility and security are why many companies opt for this model, believing they can obtain the advantages of the cloud while protecting their most sensitive data and applications on-premise.

Research firm MarketsandMarkets predicts demand for hybrid cloud will increase at a compound annual growth rate of 17% into 2023. Meanwhile, analysts at IDC estimate more than 90% of enterprises worldwide will be relying on a mix of on-premise/dedicated private clouds, multiple public clouds, and legacy platforms to meet their infrastructure needs by next year (2022). The Flexera 2021 State of the Cloud Report also found that 82% of the 750 IT professionals surveyed now have a hybrid cloud strategy in place and that on average, respondents use 2.6 public and 2.7 private clouds.

But as companies distribute their data across these increasingly complex hybrid cloud infrastructures, they need to cast a wider security net as the volume of information exchanged continues to increase exponentially. The hybrid cloud model has significant security challenges in relation to the cryptographic keys that govern access and use of data and applications across and between existing infrastructure and perhaps multiple cloud environments. Keys are similar to the combination of a physical safe and the lock that secures it, and their poor management can easily compromise strong encryption algorithms.

Since keys offer access to plaintext data, the encrypted data in an organization is only as secure as the security of its key. Every enterprise should have the strongest encryption key security possible and a key management policy (KMP) that describes the goals, responsibilities, and overall requirements for managing cryptographic keying material. The policy should guide every employee accessing the keys, and include protection objectives, and what users can and cannot do with the keys. Responsibilities for the management of cryptographic keying material should be clear along with constraints that apply to the entire key lifecycle.

This sounds straightforward enough, but key management can be a complex task in any environment, because of the number of keys and processes involved and the sensitivity of the data they protect. In hybrid cloud this is especially problematic where each environment has its own requirements and effective oversight is difficult.

Two questions about hybrid cloud key security that must be answered

Cloud service providers (CSPs) provide a key management service (KMS) that generates encryption keys for customers and manages them throughout their lifecycle, from generation to storage, distribution, use and destruction.

This seems attractive for any enterprise, but two critical questions immediately arise in relation to key security, which organizations with hybrid infrastructure should address if they are to avoid exposing vulnerabilities or tying themselves up in complicated and time-consuming key management problems. The first is: “Who is responsible for encryption security – the CSP or the organization?” The second is: “Is the key management strategy compliant with government and industry-led regulations?”

Absence of sole control – is BYOK the solution?

The problem with this form of key management is that organizations lack sole control and ownership of the keys, resulting in confidentiality risks and failure to meet compliance or internal security requirements. Having the keys held by the same entity that holds the data is far from best practice. Whenever encrypted data is stolen it is because hackers have stolen the keys first.

This is where Bring Your Own Key (BYOK) in theory provides the solution. It is an encryption key management system that should allow organizations to generate their own encryption keys and retain control and management. It appears to be ideal for hybrid cloud infrastructure, but unfortunately, it still has significant drawbacks that enterprises should be aware of. Depending on the technology's deployment, businesses can still lose control of their cryptographic keys to the CSP.

How BYOK Works

BYOK typically allows cloud users to import their own key material. Users can generate keys using an on-premise physical or virtual hardware security module (HSM) then upload them to the CSP's KMS. The upload is usually protected using a public key provided by the CSP.

This customer-generated key is then used to encrypt data encryption keys (DEKs) – not the actual data – generated by the cloud KMS. From there, enterprise applications can use the key by connecting to the CSP's KMS.

Since this key is uploaded to the cloud, however, it gives the CSP full access and control and by extension, access to data. All other key management lifecycle processes are taken back to the CSP, meaning that the BYOK deployment has not brought control and management back to the enterprise despite the added complexity.

One of the potentially very adverse consequences is that the CSP's employees can compromise the data either through malice or incompetence. Even worse, the government can subpoena the cloud service for the encrypted data and the decryption key and prevent them from notifying the customer about it.

How enterprises can regain control

Enterprises considering using BYOK technology should determine the amount of control the deployment is going to bring. If an organization is subject to stringent data access requirements or needs to comply with complex regulation, that necessitates having the keys under its supervision throughout their lifecycle.

If an enterprise uses an external, third-party key controller, however, it will have greater control and is more likely to know whenever its data needs to be accessed. It can implement identity and access management (IAM) policies to control access to the key store, revoking CSP access to keys (for encryption and decryption) at any time.

And while BYOK ensures enterprises can migrate their encrypted data and its keys to the cloud, they should avoid refactoring applications to fit a specific CSP. Refactoring is highly time-consuming and very costly, requiring significant levels of skill. It hinders time-to-market, and if a cloud provider alters the way it runs its systems, an application must be refactored again.

Instead, enterprises should opt for an intermediary that can communicate with the CSP using a standard library or an easy-to-use RESTful API. The intermediary will handle all backend intricacies and ensure an enterprise can run its service or application on any cloud that makes the best business case for doing so. This also means avoiding cloud the HSMs provided by CSPs such as AWS, since organizations cannot migrate encryption keys that are managed there.

BYOK with cloud KMS versus external key management

Using BYOK in conjunction with a cloud KMS seems advantageous. Yet while it allows organizations to bring their own 'master' keys to the cloud, their data is still encrypted using the CSP's keys. This key management model does not require any specialized skilled resources and provides native integration with other services provided by the CSP. But the CSP remains in control of the encryption keys' lifecycle management.

External key management on the other hand, eliminates CSP control, and is implemented by using a supported external key management partner through services such as Google Cloud External Key Manager (Cloud EKM). This key management model allows organizations to store and manage keys outside the CSP's KMS, gaining total control over the location and distribution of the keys. Organizations can then regulate access to the keys and manage them from a centralized platform.

On-premise versus virtual HSMs

To bring keys under total control, an enterprise needs to store them in its own HSM, whether on-premise or virtual. An on-premise HSM provides complete control over keys and policies as there is no dependency on a vendor. However, it requires a substantial upfront investment in terms of hardware, skilled personnel, and management software. More fundamentally, it will not support the requirements of modern applications that drive digital services.

A virtual HSM, on the other hand, will offer flexible services while providing scalability and on-demand cryptographic services. Third-party virtual HSMs will also facilitate a multi-cloud infrastructure and are provide the flexibility needed for enterprises to meet modern business needs.

Enhancing BYOK security and control in the cloud

BYOK certainly brings benefits in terms of confidentiality, control, and compliance. However, organizations need to plan carefully to ensure that their BYOK deployment does not hand over management to their CSP. The point is that an external FIPS 140-2 Level 2 (and higher) certified key management service will store cryptographic keys outside the CSP KSM with a high degree of safety and ease-of-use.

Yet to maximize security and prevent a single point of failure, enterprises should use an external key management service that takes advantage of multiparty computation (MPC). This is a platform that application developers can write to, offering them flexibility and crypto agility. It will allow enterprises to override the need to refactor numerous applications to ensure their compatibility across each cloud environment.

Such a service will split keys into multiple random shares, enabling the enterprise to retain control as it chooses where the key shares are located. Since the CSP does not have the keys and no unauthorized party can access the full key, the enterprise can keep any data in the cloud no matter how sensitive it is while meeting compliance and governance guidelines. This allows enterprises to synchronize key management across many data environments and applications, eradicating the single point of failure. It creates a virtual mesh of key management and protection devices, wherever they are – in any datacenter and any cloud, both for management and consumption of cryptographic services.

If enterprises are to streamline their management and increase the security of the increasingly vast amounts of data held and used in the cloud, they must think much harder about how they use encryption keys. Cloud vendors' BYOK key management systems have much to recommend them in terms of utility but are not a route to either maximum security or a cost-effective use of resources. For that external, innovative new approaches, like MPC should be a consideration.

About the Author

Marcella Arthur, Vice President, Global Marketing of Unbound Security. During her career, Marcella spearheaded two successful IPOs and led the global marketing and channel strategy of several of the world's technology innovators and IT security vendors, including Sybari, Mimecast, and Microsoft.

Marcella can be reached online at https://www.linkedin.com/in/marcellaarthur , @sheknowsmktg and at our company website https://www.unboundsecurity.com/

Protect Data with Deep Packet Inspection or Be Breached

By Randy Reiter CEO of Don’t Be Breached

Recent Cyberattacks Have Been Brutal

A global surge in cyberattacks has resulted in organizations being hit with 490+ cyberattacks per week. This is 40% higher than pre March 2020. Government, military and healthcare followed by education and research organizations are targeted most often.

Recent High Profile Cyberattacks:

- Amazon Twitch 126 GB Data Breach. Hackers claim they stole 126 GB of data that included customer payment details in October, 2021. Twitch live streams video games and videos. The streaming service was acquired by Amazon in 2014 for nearly $1 billion.

- 70 GB of Data Stolen from Acer. Acer the Taiwanese tech giant was breached the 2nd time this year in October, 2021. The Hackers posted a link to the stolen data that included data from millions of customers. The stolen data included login credentials and financial documents.

- Hacker Group that Breaches Networks in 30 Minutes. The Hacking group SnapMC has been successful in exploiting vulnerabilities in webserver and VPN applications (October, 2021) to gain access to confidential data within 30 minutes of the start of a cyberattack. SnapMC has been observed exploiting remote execution flaws in .NET as well as SQL injection attacks.

Conventional approaches to cyber security are not preventing data breaches. In 2020 the DHS, Department of State, U.S. Marine Corps and the Missile Defense Agency recognized this and all issued requests for proposals (RFP) for network full packet data capture for deep packet analysis or Deep Packet Inspection analysis (DPI) of network traffic. This is an important step forward protecting confidential database data and organization information.

Zero-day vulnerabilities that allow Hackers to gain SYSTEM PRIVILEGES are a major threat to all organizations encrypted and unencrypted confidential data. Confidential data includes: credit card, tax ID, medical, social media, corporate, manufacturing, trade secrets, law enforcement, defense, homeland security, power grid and public utility data. This confidential data is almost always stored in DB2, Informix, MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL and SAP Sybase databases.

How to Stop the Theft of Data with Deep Packet Inspection

Protecting encrypted and unencrypted confidential database data is much more than securing databases, operating systems, applications and the network perimeter against Hackers, Rogue Insiders and Supply Chain Attacks.

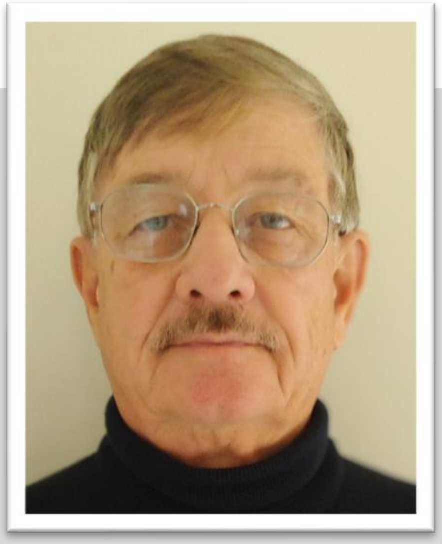
Non-intrusive network sniffing technology can perform a real-time full packet capture and Deep Packet Onspection (DPI) of 100% the database query and SQL activity in real-time from a network tap or proxy server with no impact on the database server. This SQL activity is very predictable. Database servers servicing 1,000 to 10,000 end-users typically process daily 2,000 to 10,000 unique query or SQL commands that run millions of times a day. Deep Packet Analysis does not require logging into the monitored networks, servers or databases. This approach can provide CISOs with what they can rarely achieve. Total visibility into the database activity 24x7 and 100% protection of confidential database data.

Advanced Behavioral Analysis from Deep Packet Inspection Prevents Data Breaches

Advanced SQL Behavioral Analysis of 100% of the real-time database SQL packets can learn what the normal database activity is. Now the database query and SQL activity can be non-intrusively monitored in real-time with DPI and non-normal SQL activity immediately pinpointed. This approach is inexpensive to setup, has a low cost of operation and disk space usage. Now non-normal database activity from Hackers, Rogue Insiders or and Supply Chain Attacks can be detected in a few milli seconds. The Security Team can be immediately notified and the Hacker session terminated so that confidential database data is NOT stolen, ransomed or sold on the Dark Web.

Advanced SQL Behavioral Analysis of the query activity can go even further and learn the maximum amount of data queried plus the IP addresses all queries were submitted from for each of the 2,000 to 10,000 unique SQL queries that run on a database server.

This type of Data Breach Prevention can detect never before observed Hacker database query activity, queries sent from a never observed IP address and queries sending more data to an IP address than the respective query has ever sent before. This allows real-time detection of Hackers, Rogue Insiders and Supply Chain Attacks attempting to steal confidential database data. Now an embarrassing and costly Data Breach can be prevented.



About the Author

Randy Reiter is the CEO of Don’t Be Breached a Sql Power Tools company. He is the architect of the Database Cyber Security Guard product, a database Data Breach prevention product for Informix, MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL, and SAP Sybase databases. He has a Master’s Degree in Computer Science and has worked extensively over the past 25 years with real-time network sniffing and database security. Randy can be reached online at rreiter@DontBeBreached.com, www.DontBeBreached.com and www.SqlPower.com/Cyber-Attacks.

Can Netflix Save Cybersecurity?

The CSaaS membership model offers a new paradigm for successful protection from today's advanced cyber attacks by pairing skilled security practitioners with proven processes and best-of-breed technologies

By Corey White, co-founder, and CEO of **Cyvatar**

Hacked. Breached. Compromised. Attacked.

Call it by any name you like, but there's no denying that cyber threats, incidents, and events continue to outpace our ability to protect against them.

Increasingly sophisticated relentless attacks and high-profile breaches spur the purchase of more and more security tools, but companies rarely (if ever) have the right people and processes in place to ensure the solutions they buy are installed correctly, not to mention the ongoing assessments, remediation, and maintenance needed to achieve cyber resilience.

We buy more products...and we're hacked. We adhere to compliance standards...but we get breached. We hire managed services providers...our data is compromised anyway. The industry's response has long been to build new products, knowing that buyers will come; when the technology fails to defend against a breach, managed services providers step in to remediate after the fact and "manage" the customer's environment against future incursions.

Then a Colonial Pipeline happens, and we buy more stuff.

It's a vicious cycle, but fortunately it's a cycle organizations can finally break. By stepping away from traditional notions of ownership (like buying a security solution) and embracing Membership Economy principles, organizations can improve cyber resilience while decreasing the complexity of their technology stacks and reducing their overall cyber spend.

What's the Membership Economy, Anyway?

The Membership Economy includes any organization whose members (customers) have an "ongoing and formal stake" in that organization.[1] The human desire to belong, to be part of a community or affiliated with an exclusive organization, is fulfilled in the Membership Economy, and Netflix is one of its best-known acolytes.

Importantly, the Membership Economy moves organizations away from transactional sales that are cost-based and require conversions, cross-sells, and other additional transactions toward what Baxter calls the forever sale -- a lifetime of customer value where retention and delight are the outcomes. The relationship ends only when the member cancels subscription; otherwise, that first transaction lasts forever.

Key components of the Membership Economy include:

- Continually focusing on the needs of members
- Understanding member frustration ***and*** satisfaction
- Embracing a willingness to f meet member needs and wants through flexibility, innovation, and evolution
- Communicating a strong, clear value proposition
- Investing in the membership experience

Ownership as Liability

Cybersecurity companies, like many technology organizations, focus on transactional sales. Customers buy a solution for a period of time--typically two to three years--and are largely left to fend for themselves until their contract comes up for renewal. Also like other technology deployments, security installations

[1] Baxter, Robbie Kellman."The Membership Economy: Find Your Superusers, Master the Forever Transaction, and Build Recurring Revenue". McGraw-Hill Education. 2015, p. 26.

can be complex, costly, and time consuming, often making it difficult for customers to change or add products in their production environments. Even when a customer is unhappy with a product, swapping it out for something new may be more trouble than the customer thinks it's worth, which leaves little incentive for transaction-driven companies to build meaningful innovation into their offerings.

Ownership then becomes a liability. The thousands--even millions--of dollars organizations spend on multiyear licensing agreements effectively hold them hostage regardless of product efficacy. In the event of a breach, they're still stuck in their contract and may even feel the need to buy more tools to bolster their security posture.

The product companies don't fare much better: Once they create a new offering, they become limited by the scope of their own design, for good or ill, and innovation remains stalled.

Groundbreaking innovation has toppled entire organizations that were displaced by the rapid advancement of others, as Blockbuster was by Netflix. Transactional organizations cannot hope to keep pace with the growing costs of breaches and the ease with which they can be executed without foundationally changing the way new defenses are designed, built, and adopted.

Membership--the Netflix model--is just such a foundational change. It can be every bit as disruptive and transformational to the cybersecurity industry as Netflix itself was to the movie rental and streaming industries. Here's how.

1) Subscriptions. Subscriptions make it easy for members to select the pricing and options that are best for them, and consistent and predictable revenue streams benefit shareholders and users alike. But subscriptions alone do not make a Membership Economy. Organizations must grow members into new offerings and ensure value is continuously delivered.
2) Loyalty programs. As American Express famously said, membership has its privileges. In cybersecurity, privileges can include freemium pricing models, discounted upgrades, free services engagements, and more.
3) Engagement. The Membership Economy can't work without high levels of member engagement, which is why Baxter recommends the program be beneficial for members as well as the company that serves them. Benefits stemming from loyalty create bonds, even emotional connections, between members and the companies they associate with, which in turn create vibrant communities of influencers and evangelists that become a continual source of innovation for Membership Economy organizations.

By staying close to your members and active in the communities you share with them, you're always a part of the feedback loop, enabling you to continue to evolve your offerings to meet member needs. Ongoing feedback ultimately becomes a source of competitive differentiation too, because traditional security organizations selling through transactions are less able to tap into widespread customer sentiment (positive or negative) and therefore less likely to be able to turn the information they do get into meaningful innovation.

Access over Ownership

Cybersecurity-as-a-service, or CSaaS, brings all of these concepts to life. CSaaS is inherently a member-driven model, allowing providers to focus on access rather than ownership. Instead of selling transactional point solutions or fee-for-services to create what we used to call customer “stickiness,” security companies can use the membership model to level the playing field and democratize cybersecurity, making the best protection accessible and affordable for every size organization, even those with no cybersecurity expertise in house.

The CSaaS membership model offers a new paradigm for successful protection from today’s advanced cyber attacks by pairing skilled security practitioners with proven processes and best-of-breed technologies. Importantly, CSaaS handles the heavy lifting associated with evaluating and recommending solutions from more than 4500 security vendors so that members can focus on scaling *their* businesses without worrying about securing the sensitive data and information they need to succeed.

CSaaS also ensures that recommended solutions are installed and configured completely (and correctly) in addition to providing ongoing remediation of vulnerabilities and regular maintenance of security tools, thus walling off the majority of entry points for cyber criminals and ensuring members get value from all of their security investments, from conception and strategy to implementation and maintenance.

By selling membership rather than ownership in the CSaaS model, members can achieve faster compliance to standards like NIST CSF, SOC 2, PCI, and HIPAA; they can also receive better cyber-attack protection from threats like the OWASP Top 10 and the CWE Top 25, giving them true resilience, lower costs, less stress, and the ability to implement the very best technologies available at any time, all the time.

The CSaaS membership model is Netflix for cybersecurity: inherent innovation and bespoke solutions at scale.

About the Author

Corey White is the co-founder and CEO of Cyvatar, an all-inclusive cybersecurity-as-a-service (CSaaS) company committed to helping businesses – of all sizes – learn how they can **prevent** cybercrime and ransomware attacks. White is a proven security industry veteran backed by more than 25 years of success managing security practices and consulting teams and delivering on strategic projects as well as tactical assessments, penetration tests, and incident response engagements. His work encompasses virtually every industry sector, including defense, technology, government, critical infrastructure, automotive, finance, healthcare, and manufacturing. Corey has a deep technical background, which has allowed him to deliver and oversee technical assessments, incident response engagements, strategic planning, and risk assessments. Corey served as the senior vice president of worldwide consulting and chief experience officer at Cylance managing a team of 150+ globally, culminating in the acquisition of Cylance by Blackberry for $1.5 billion. Also at Cylance, Corey created the first outcomes-based service, evolving traditional implementations to continue engagements with prevention experts until every client reached its goal, giving customers measurable, sustainable prevention. He managed seven practice areas led by distinguished experts in industrial control systems, red team services, incident containment and forensics, IoT and embedded systems security, ThreatZERO, strategic services, and education. Prior to joining Cylance in 2012, Corey was the director of consulting for Foundstone & McAfee/Intel professional services with responsibilities for all aspects of the business for the Southwest region.

Follow Cyvatar on LinkedIn and Twitter or connect with us through our company website https://cyvatar.ai/.

How To Do Disruptive Innovation Right

By Karla Jo Helms, FOUNDER & CEO, JOTO PR Disruptors

Industry disruptors are the driving force behind every industry innovation, advancement, and improvement for the end-users. These are the pioneers that defy their industries' status quo, putting forth not seeing how to create a better solution but also having the vision to see how that solution succeeds. For innovators, solving issues that plague themselves and their industries are more important than maintaining a comfortable status quo. They are unafraid of provoking their competitors or upsetting their possible allies. But when innovators upset the balance, they will meet with real resistance from their foes—those who don't want them to succeed. Innovators upset the balance. They threaten their position in the industry. Therefore, innovators are seen as dangerous, and these foes will work to take them down.

Lack of preparation has caused the downfall of innumerable innovators. Because they are so focused on their solution, they are inadvertently putting on blinders and never see the attack coming, leaving them blindsided and wholly unprepared for the lawsuits, libel, slander, and other techniques, ethical or otherwise, their foes will use against them.

Fortunately, new innovators can take steps to mitigate the inevitable attacks they will face. The first step in arming themselves against active resistance is doing thorough research on not just these foes, but on their "comrades in arms" as well.

Innovators must ask themselves:

- What are the possible obstacles to market adoption?
- Who are the INFLUENCERS that will inspire the early adopters?
- What is the probable level of resistance and realistic adoption rate?
- When, NOT IF, there will be a need for legal counsel? (hint: hire them upfront)

And perhaps most critical, Innovators MUST UNDERSTAND:

- That PR and Publicity must be at work WELL BEFORE achieving business goals

Disruptors who fail to heed any one of these concepts put not only their solution's success at great risk but their very business as well. Fortunately, any damage can be avoided by first taking these steps:

- Conducting market research on the key target audiences (including foes) to uncover the reasons behind acceptance or resistance to adoption. Understanding their perceptions beforehand can provide a significant benefit—prediction.
- Executing Key Opinion Leader market research that discovers the key target audiences' INFLUENCERS. Implementing the new media methodology today—communicating through influencers and key opinion leaders—makes adoption happen ten times faster.
- Utilizing the two preceding tools and their data to mathematically determine the size and potential impediments to adoption. For target audiences, this means estimating the level of effort (i.e., time, money, marketing) necessary to persuade a segment of the population to change their attitude or to think in a particular way.

Innovators should take special note: there is competition out there with the business model of using Patent Assertion Entities (PAEs), frivolous lawsuits specifically designed to drive out smaller businesses and then purchase their assets for pennies on the dollar. As mentioned earlier, disruptors must have their legal teams hired as soon as possible.

Once the legal council is established, innovators need to take further steps to prepare for the impending attacks:

1. Discover the competitions' SOP for identifying and stamping out the early competition. Have the legal firm do research of public records, lawsuits, etc.; they are very telling.
2. Recognize all stakeholders, their plausible or actual resistance or explicit resentment to change, and who among them could be litigious?

3. Verify all patents, trademarks, service marks, copywrites are filed or up to date.
4. Ideally, as soon as one year before initiating aggressive marketing, set out on a public opinion publicity campaign to get markets familiarized with the coming change. Publish stories of goodwill, thought leadership articles, etc. discussing it and popularizing the forthcoming solution.
5. Seek out any weaknesses to attacks and decide what should be done using PR and legal procedures.
6. Create a crisis communications plan that can be immediately implemented in the likely event of lawsuits or slander/libel incidents.

Disruptive innovators that took these steps have seen the benefits— established reputations for being thought leaders, gained the public's confidence, and had well-deserved ROI. To illustrate, the belief that decentralized workforces couldn't have the same level of secure and reliable data services outside of the office had been the long-established status quo, even before the advent of the global pandemic. When COVID-19 forced employees to work from home *en masse*, Technologent, a provider of information technology solutions and services, overturned that perceived necessary evil. They provided a solution for business data security and management woes—a single-source, cost-effective means to remove data silos, guard against breaches, provide client management, and more. They could provide all needs—security, software, infrastructure service, back-up, automation— through their "as a service" platform. However, before all else, they took the offensive, and the offenders to task, via messaging that expounded on their expertise on cybersecurity matters across the relevant business and technology trade publications, industry podcasts, and mainstream media sources. Their constant message in essence? Businesses could overcome perceived cost-prohibitive and technically unworkable data silo and security issues with their centralized service model.

Technogent utilized a publicity campaign of goodwill that told the story of how they were solving businesses' data management and security issues. Not only were they communicating an effective message, but they were also doing so via the appropriate channels. (Because they knew their key target audiences) Technologent introduced and nurtured the idea that businesses didn't have to accept their increased susceptibility to attack, loss, or lost revenue opportunities. For their efforts, Technologent drew not only massive attention, but it came from from the right audiences, with a disruption that reached across multiple industries that were experiencing unfeasible data management issues.

New disruptors should see their innovation as part of a larger process of solving their audiences' problems. If anything, they must never be lulled into a sense of complacency, naïvely believing their solution on its own is all but doomed from the start. Winning over hearts and minds and fighting off the foes will take a lot of preparation and due diligence. Yes, being an innovative disruptor isn't solely about that great solution – it's also about how to maintain it time and time again. Because true innovators never stand still, do they?

About the Author

Karla Jo Helms is the Chief Evangelist and *Anti*-PR(TM) Strategist for JOTO PR Disruptors(TM).

Karla Jo learned firsthand how unforgiving business can be when millions of dollars are on the line—and how the control of public opinion often determines whether one company is happily chosen, or another is brutally rejected. Being an alumni of crisis management, Karla Jo has worked with litigation attorneys, private investigators, and the media to help restore companies of goodwill back into the good graces of public opinion—Karla Jo operates on the ethic of getting it right the first time, not relying on second chances and doing what it takes to excel. Helms speaks globally on public relations, how the PR industry itself has lost its way and how, in the right hands, corporations can harness the power of *Anti*-PR to drive markets and impact market perception.

Karla can be reached online at https://jotopr.com/

EVENTS

SUPPORTED BY

UNITED ARAB EMIRATES
MINISTRY OF DEFENCE

UNITED ARAB EMIRATES
AIR FORCE & AIR DEFENCE

Beyond Joint: The Expanding Role of Air, Space and Cyberspace in Multi-Domain Operations

November 13, 2021 - Madinat Jumeirah, Dubai | www.diacc.ae

AIR POWER. REDEFINED.

Leading edge insights on **Information Dominance: Employing an All-Domain Operational Strategy**, Joint All-Domain Command and Control: Building an Agile and Resilient Combat Network, **Synchronizing Combat Effects: Connecting Sensors and Platforms**

Featuring **General Charles Q. Brown, Chief of Staff, United States Air Force**, Lieutenant General J.D. (Dennis) Luyt, Commander, Royal Netherlands Air Force, **Major General Ibrahim Nasser Al Alawi, Commander, UAE Air Force & Air Defence**, Lieutenant General Al Meinzinger, Commander, Royal Canadian Air Force, **Air Marshal Gerry Mayhew CBE, Deputy Commander (Operations), Royal Air Force,** General Gregory Guillot, Commander, United States Air Forces Central Command, **Lieutenant General Ingo Gerhartz, Chief of the German Air Force**

10th
DIACC
DUBAI INTERNATIONAL
AIR CHIEFS' CONFERENCE

Move into the future with transformational insights

GOLD SPONSORS

LOCKHEED MARTIN

Raytheon Emirates

DASSAULT AVIATION

ASSOCIATE SPONSORS

BOEING

MBDA MISSILE SYSTEMS

SAAB

PRATT & WHITNEY GO BEYOND

GENERAL ATOMICS AERONAUTICAL

MEDIA PARTNERS

nation shield

ARABIAN AEROSPACE

AFRICAN AEROSPACE

CYBER DEFENSE MAGAZINE

militär AKTUELL

AVIATION WEEK & SPACE TECHNOLOGY

ORGANIZED BY

SPPS

DigiConnect

EGYPT EMERGING TECHNOLOGIES FORUM

Driving Egypt's digital economy and society transformation through intelligent technologies

24 November 2021 | 10:00 AM Cairo time | via Zoom

Supported by:

Ministry of Communications and Information Technology

مصر الرقمية

As part of the national 2030 Vision, **Egyptian Ministry of Communication and Information Technology** has launched its **Digital Egypt Project,** establishing a digitalisation strategy to transform the country into a digital society and global telecom and tech centre through three key pillars: digital transformation, skills and jobs, and innovation.

In line with these developments, the Egypt Emerging Technologies Forum is hosted to provide a platform for the information and communication technology community in Egypt to explore the latest emerging technologies and innovations.

WWW.EGYPTEMERGINGTECHNOLOGIES.GMEVENTS.AE

Organized by

GM EVENTS

FOR SPONSORSHIP ENQUIRIES:

Bencily Thomas
Head of Sales
bencily.thomas@gmevents.ae
+971 52 969 7209

SCAN THE CODE
TO LEARN MORE

EXPO
TEL AVIV
PAVILION
2

iHLS
INNOTECH
TEL AVIV

iHLS INNOTECH 2021

CONFERENCE & EXHIBITION
CYBER, HLS & INNOVATION INTERNATIONAL EVENT

NOVEMBER 17-18, 2021 | 9:00-18:00

iHLS

Cyber Israel
Prime Minister Office
National Cyber Directorate

ISA
סוכנות החלל הישראלית

ISRAEL
Ministry of Foreign Affairs
Division for Cultural and Scientific Affairs

From Vision To Mission
MAFAT

משרד הביטחון
MINISTRY OF DEFENCE

3rd Annual

Indian Defence Conclave

INDIAN DEFENCE CONCLAVE - 2021

02nd - 03rd DECEMBER | 2021 NEW DELHI, INDIA

Organised by traicon a step to perfection

SPEAKERS

LT GEN RAJEEV CHAUDHRY VSM
Director General
Border Roads Organization

LT GEN SUNIL SRIVASTAVA, AVSM, VSM (RETD)
Director
Centre For Joint Warfare Studies

AIR MARSHAL ANIL CHOPRA PVSM AVSM VM VSM (RETD)
Director General
Centre for Air Power Studies

MAJ GEN (DR) BIPIN BAKSHI, AVSM, VSM, RETD
Deputy Director General
Manohar Parrikar Institute for Defence Studies & Analyses

COMMANDER VINEET ARORA
Joint Director
Ministry of Defence

COMMANDER (DR) SIBAPADA RATH
Research Fellow
National Maritime Foundation

WG CDR P MADHUSOODHANAN
Vice President Aerospace & Defence
Tamil Nadu Defence Industrial Corridor

MAJOR GENERAL K.A.D.A. KARUNASEKARA RWP RSP VSV USP NDU PSC
Commandant
NDC, Sri Lanka

SPONSORS PARTNERS

TIER ONE SPONSOR

APL APOLLO® STEEL PIPES

TIER THREE SPONSORS

VIAVI Solutions

GOPALAN AEROSPACE INTEGRATED AEROSPACE PARK

ihse. USA

FLUKE networks.

MERITOR RUN WITH THE BULL

VERDANT innovation in technology

Huezone Solutions Pte Ltd

Markforged | Phillips

SUPPORTING ORGANIZATIONS

National Maritime Foundation

DISA

aiai All India Association of Industries

MEDIA PARTNERS

raksha ANIRVEDA www.raksha-anirveda.com

Aviation & Defence Universe WE JUST REPORT FACTS, WE DON'T CHANGE THEM

traicon MEDIA & PUBLICATIONS

CYBER DEFENSE MAGAZINE WHERE INFOSEC KNOWLEDGE IS POWER

For Sponsorship Opportunities

Alfin | Tel: +91 90369 81048 | **Email:** alfin@traiconevents.com

IP DUBAI EMIRATES
المؤتمر الإقليمي لمكافحة الجرائم الماسة بالملكية الفكرية
Regional IP Crime Conference

THE 10TH REGIONAL INTELLECTUAL PROPERTY (IP) CRIME CONFERENCE IN THE MIDDLE EAST AND NORTH AFRICA

www.ipcrimeconference.ae

December 13-14, 2021
Habtoor Palace, Habtoor City, Dubai UAE

HOSTED BY

INTERPOL

eipa

IN PARTNERSHIP WITH

BPG
مجلس أصحاب العلامات التجارية
BRAND OWNERS' PROTECTION GROUP

جمارك دبي
DUBAI CUSTOMS

وزارة الاقتصاد
MINISTRY OF ECONOMY

شرطة دبي
DUBAI POLICE

وزارة العدل
MINISTRY OF JUSTICE

وزارة الداخلية
MINISTRY OF INTERIOR

In conjunction with the Expo 2020 and under the patronage and presence of HE Lt. General Dahi Khalfan Tamim, Deputy Chief of Police and General Security in Dubai, The Honorary President of the Emirates Intellectual Property Association, the Emirates Intellectual Property Association (EIPA) and the International Criminal Police Organization (INTERPOL) are organizing in collaboration with the Ministry of Justice, Dubai Customs, and Brand Owners' Protection Group (BPG), the 10th Regional Intellectual Property (IP) Crime Conference in the Middle East and North Africa.

This event will be held on 13-14 December 2021 to highlight and connect the Expo 2020 themes (Opportunity/Mobility/Sustainability) with intellectual property protection. This will include the most important developments and challenges in the enforcement of intellectual property laws, new opportunities to combat intellectual property crimes, presenting new technologies of facilitating legal control procedures, and presenting global best practices in the protection of intellectual Property and trafficking of counterfeit and pirate goods.

UNDER THE PATRONAGE AND PRESENCE OF

HE Lt. General Dahi Khalfan Tamim
Deputy Chief of Police
and General Security in Dubai
The Honorary President of the Emirates
Intellectual Property Association

FOR SPONSORSHIP ENQUIRIES:

Bencily Thomas
Head of Sales
bencily.thomas@gmevents.ae
+971 52 969 7209

SCAN THE CODE TO LEARN MORE

Organized by GM EVENTS

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

FEB 1st-3rd, 2022

New Orleans, LA, USA

A Homeland Security Event

Let's get back to the business of securing national infrastructure

After a long year of restrictions and lost opportunities due to the pandemic, highlighting new challenges and threats to our critical infrastructure, we need to get back to the business of building better resilience for future continuity and sustainability for economic prosperity.

Join us in New Orleans on February 1st-3rd, 2022 for the next Critical Infrastructure Protection & Resilience North America Conference and understand the latest threats, challenges and solutions, from both physical and cyber perspectives, against your CI.

Let's get back to business, back to better understandings and back to networking!

Registration Open

Register today and benefit from Early Bird delegate fees

For further details visit www.ciprna-expo.com/registration

SPECIAL DEAL FOR GOVERNMENT AND OWNER/OPERATORS

The 3rd Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operator/owners, agencies and governments to debate and collaborate on securing America's critical infrastructure.

As we come out of one of the most challenging times in recent history, it has stressed how important collaboration in protrection of critical infrastructure is for a country's national security.

Join us in New Orleans, LA, USA for the premier event for operator/owners and government establishments tasked with the region's Critical Infrastructure Protection and Resilience.

For further details visit www.ciprna-expo.com

Confirmed speakers include:

- Jacob Anderson, Strategy Branch Chief, CISA/ISD
- Brian Harrell, VP & Chief Security Officer, AVANGRID
- Ruth Christensen, Analyst, NCTC, FBI
- Lester Millet, Safety Agency Risk Manager / FSO Workgroup Chairman, Port of South Louisiana & Infragard Louisiana President
- Deron T. McElroy, Chief of Cybersecurity Services, CISA
- Todd Klessman, Deputy Associate Director, DHS/CISA
- Chris Rodriguez, Director, District Of Columbia Homeland Security And Emergency Management Agency
- Deborah Kobza, President, IACI
- Douglas Delancey, Branch Chief, Counter IED Strategy, Integration & Comms, Office For Bombing Prevention, CISA
- Stephanie Murphy, Vice President, Resiliency and Critical Infrastructure Programs, Tidal Basin Government Consulting
- Minna LeVine, Founder, SMART Community Exchange
- Ron Fisher, Director Of The Infrastructure Assurance & Analysis Division, Idaho National Laboratory
- George Rey, Aviation Sector Chief, InfraGard Louisiana BoD
- Steve Povolny, Head of Advanced Threat Research, McAfee
- Ron Martin, Professor Of Practice, Critical Infrastructure, Capitol Technology University

For speaker line-up visit www.ciprna-expo.com

The premier discussion for securing America's critical infrastructure

Platinum Sponsor: DISPEL

Silver Sponsors: tyco Security Products, Qognify

Bronze Sponsors: AccuBeat, CAPITOL Technology University

Supporting Organisations: INFRAGARD Members Alliance Louisiana, International Association of CIP Professionals, I-DIEM Institute for Diversity and Inclusion in Emergency Management, IACI International Association of Certified ISAOs, ISIO International Security Industry Organization, SPF Security Partners' Forum, NS&RC

Media Partners: WORLD SECURITY REPORT, World Security-index.com

DATA DRIVEN GOVERNMENT CONFERENCE 2022

DRIVING GOVERNMENT INNOVATION THROUGH DATA

DATE:
15TH - 16TH FEBRUARY 2022

VENUE :
MOVENPICK GRAND AL BUSTAN, DUBAI

THE MENA REGION'S GOVERNMENTS have set strategic goals to position themselves as digital leaders and spearhead data utilisation through their adopting a data-driven government structure. This approach is aimed at improving operations, driving innovation, delivering better services to citizens and supporting socio-economic development.

We are hosting the **2ND DATA-DRIVEN GOVERNMENT CONFERENCE** taking place on **15-16 February 2022, Movenpick Grand Al Bustan, Dubai,** with the support of the region's key government entities. The event will bring together 300+ international and regional stakeholders from across the region's government sector, international leading technology consultants and innovators to explore best practices and latest solutions that can enable an advanced and secure data and analytics infrastructure and a successful data-driven government implementation.

2022 SUPPORTING PARTNERS

Ministry of Communications and Information Technology

سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and Information Technology

هيئة الصحة بدبي
DUBAI HEALTH AUTHORITY

مجمع الشارقة للبحوث والتكنولوجيا والابتكار
Sharjah Research Technology and Innovation Park

IGOAI
INTERNATIONAL GROUP OF ARTIFICIAL INTELLIGENCE

المركز الوطني للطاقة
National Energy Center

UNITED ARAB EMIRATES
MINISTRY OF HEALTH & PREVENTION

وزارة الاقتصاد الرقمي والريادة

مؤسسة الإمارات للخدمات الصحية
EMIRATES HEALTH SERVICES

منطقة عجمان الحرة
Ajman Free Zone

oits
الجمعية العمانية لتقنية المعلومات
Oman Information Technology Society

FOR SPONSORSHIP ENQUIRIES:

Bencily Thomas
Head of Sales
bencily.thomas@gmevents.ae
+971 52 969 7209

SCAN THE CODE
TO LEARN MORE

Organized by GM EVENTS

Future Tech Event

UNDER THE PATRONAGE

سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and Information Technology

ENABLING OMAN'S VISION 2040

28 - 29 March 2022 | Oman Convention and Exhibition Centre | 9 am - 4 pm

HYBRID+ (In-Person and Online)

Future Tech is Sultanate of Oman's foremost B2B and B2G bespoke Technology Expo and Summit.

or Exhibiting Enquiries and Sponsorship Opportunities please contact:
Navneeth K, Director - Business Development
+968 9123 7892 | bdm@wpsummits.com
www.futuretechevent.com

ORGANISED BY

مسقط إكسبو
Muscat Expo

WPS
WHITE PAPER SUMMITS

#CYBERBYTE
@ROSSOWESQ

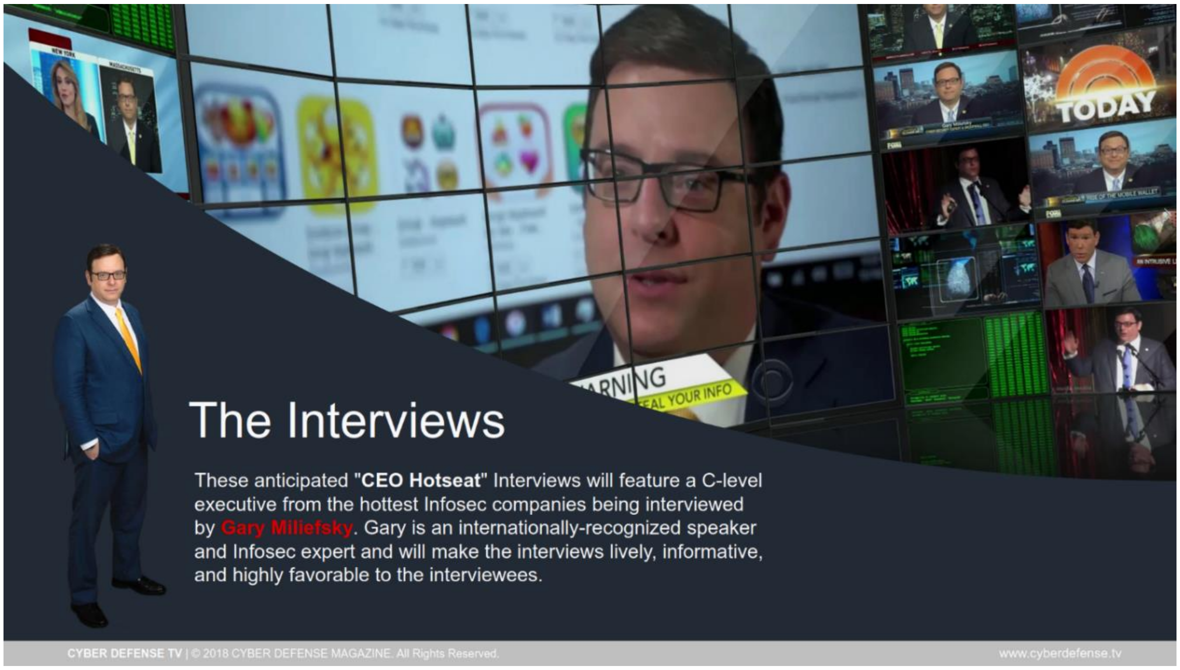
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



The Interviews

These anticipated "**CEO Hotseat**" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by Gary Miliefsky. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved.

www.cyberdefense.tv

Copyright (C) 2021, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com

Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

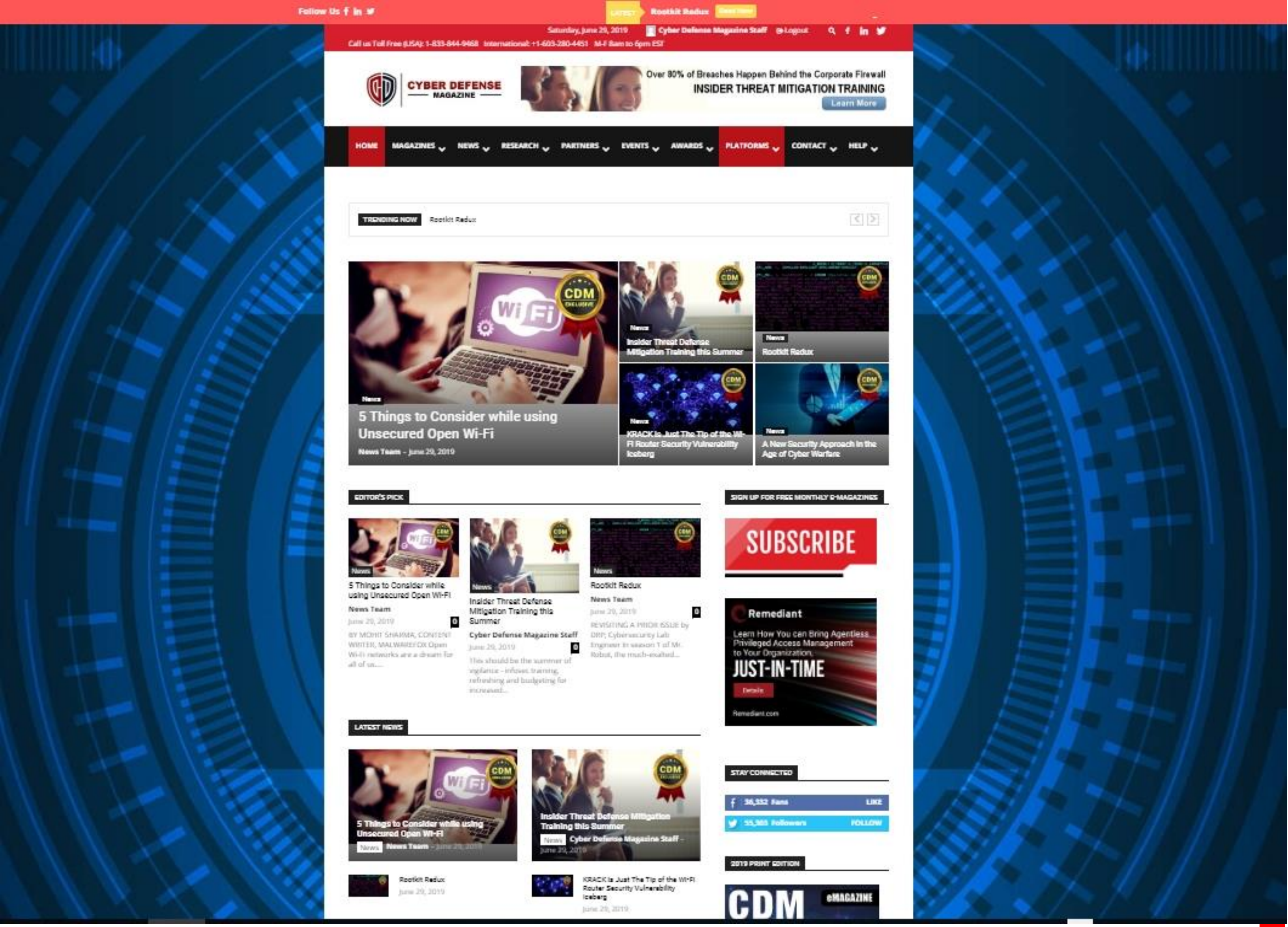
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 11/02/2021


Follow Us

LATEST Rootkit Radux

Saturday, June 29, 2019 Cyber Defense Magazine Staff Logout

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

CYBER DEFENSE MAGAZINE

Over 80% of Breaches Happen Behind the Corporate Firewall
INSIDER THREAT MITIGATION TRAINING
Learn More

HOME MAGAZINES NEWS RESEARCH PARTNERS EVENTS AWARDS PLATFORMS CONTACT HELP

TRENDING NOW Rootkit Redux

News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team - June 29, 2019

News
Insider Threat Defense Mitigation Training this Summer

News
Rootkit Redux

News
KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg

News
A New Security Approach in the Age of Cyber Warfare

EDITOR'S PICK

News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team
June 29, 2019 0
BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us....

News
Insider Threat Defense Mitigation Training this Summer
Cyber Defense Magazine Staff
June 29, 2019 0
This should be the summer of vigilance - infosec training, refreshing and budgeting for increased...

News
Rootkit Redux
News Team
June 29, 2019 0
REVISITING A PRIOR ISSUE by DRP, Cybersecurity Lab Engineer In season 1 of Mr. Robot, the much-exalted...

SIGN UP FOR FREE MONTHLY E-MAGAZINES

SUBSCRIBE

Remediant
Learn How You can Bring Agentless Privileged Access Management to Your Organization.
JUST-IN-TIME
Details
Remediant.com

LATEST NEWS

5 Things to Consider while using Unsecured Open Wi-Fi
News News Team - June 29, 2019

Insider Threat Defense Mitigation Training this Summer
News Cyber Defense Magazine Staff - June 29, 2019

Rootkit Redux
June 29, 2019

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
June 29, 2019

STAY CONNECTED

36,332 Fans LIKE

55,385 Followers FOLLOW

2019 PRINT EDITION

CDM eMAGAZINE

Books by our Publisher: [https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)](https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH)

9+ Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites and our new B2C consumer magazine CyberSecurityMagazine.com. *Millions of monthly readers and new platforms coming…starting with* *https://www.cyberdefenseprofessionals.com* *this month…*

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
eMAGAZINE
www.cyberdefensemagazine.com

AS SEEN ON TV
CBS NEWS
abc
CNN
FOX NEWS
NBC
FOX
MSNBC
USA TODAY
Inc.
The New York Times
Bloomberg NEWS
The Washington Post
FOX BUSINESS
BusinessWeek
YAHOO!
Forbes
Entrepreneur
REUTERS
The Boston Globe
ALWAYS FREE
NO STRINGS ATTACHED

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefensenewswire.com
www.cyberdefensemagazine.com

* with help from writers
and friends all over the Globe.