CYBER DEFENSE MAGAZINE

eMAGAZINE

FEBRUARY 2025



In This Edition

Expect The Unexpected

Zero-Day Exploits and State-Sponsored Threats: The Treasury Hack Exposed

Cyber Insurance Applications: How vCISOs Bridge the Gap for SMBs

...and much more...

MORE INSIDE!

CONTENTS

Welcome to CDM's February 2025 Issue ---------- 7

Expect The Unexpected ----------39

By Karina Klever, CEO, Klever Compliance

Zero-Day Exploits and State-Sponsored Threats: The Treasury Hack Exposed ----------44

By Debra Baker, CEO, TrustedCISO

Cyber Insurance Applications: How vCISOs Bridge the Gap for SMBs ----------49

By Pete Green, vCISO and Cybersecurity Consultant and Reporter for CDM

Balancing Control, Compliance, And Continuity----------54

By Jerry Kaner, CEO, Ciphertex Data Security

Top Things Your Organization Needs to Know About Knowledge-Based Authentication Today ----------58

By Matt Cochran, COO, ID Dataweb

SMB Cybersecurity Trends That Matter for 2025----------70

By Dor Eisner, CEO and Co-Founder of Guardz

Unmasking Employment Fraud ----------74

By Ryan LaSalle, CEO, Nisos

Walk Through the DDoS Fire ----------78

By Alex Pavlovic, Director of Product Marketing, Nokia Deepfield

The Federal Government's Treatment of Government Contractors' Emerging Technologies – Including Chat Interfaces And Code Generator ----------84

By Tenley A. Carp, Partner, Arnall Golden Gregory LLP

AI In Cybersecurity: The Risks and Rewards ----------88

By Michael Baker, VP and Global CISO, DXC Technology

Securing SMBs in 2025----------91

By George Skaff, SVP & General Manager, Cybersecurity SMB, OpenText

Cryptography: The Unsung Hero Fighting Cyber Threats from The Background ----------94

By Carlos Aguilar Melchor, Chief Scientist – Cybersecurity, SandboxAQ

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Table-Stakes In 2025: Threat Intelligence Management to Counter Emerging Challenges ---- 97

By Jawahar Sivasankaran, President, Cyware

Why Your Security Tools May Be Leaving You Exposed ---------- 102

By Martin Greenfield, CEO of Quod Orbis

Top Five Most Alarming Cybersecurity Trends Revealed - And What Your Business Should Be Doing About Them In 2025 ---------- 105

By Rajeev Gupta, Co-Founder at Cowbell

The OT Cybersecurity Challenge: Navigating the Journey To A Secure Industrial Future ---- 109

By Doug Barnes, OT Cybersecurity Consultant and Jay Smilyk, VP Global Sales, NanoLock

Raising Cybersecurity Awareness in The Age Of AI And Cyber Warfare ---------- 113

By Neal Quinn, head of Radware's cloud security services business

Why Medical Device Manufacturers Need MedTech Experts for SBOM Management -------- 116

By Ken Zalevsky, MedTech Expert & CEO, Vigilant Ops

Beyond The Breach ---------- 119

By Jon Fielding, Managing Director, EMEA, Apricorn

Advancing Technologies in The Year Ahead Make Digital Trust More Essential ---------- 122

By Tim Hollebeek, VP Industry Standards, DigiCert

The Risk of Identity Attack Paths: 10 Stats Everyone Must Know ---------- 125

By Jared Atkinson, Chief Strategist, SpecterOps

Attacks Against Networks and VPN Infrastructure Surged in The Last 12 Months – Preparing For The Road Ahead ---------- 128

By Lawrence Pingree, VP of Technical Marketing, Dispersive

Cryptography and Modern IT: A Digital Innovation Blind Spot ---------- 132

By Dr. Marc Manzano, General Manager, Cybersecurity at SandboxAQ

Securing GenAI Data Requires Sophisticated, Disciplined Practices ---------- 135

By Cloud Storage Security

Cybersecurity's Shift from Defense To Resilience Against Evolving Threats ---------- 139

By Engin Kirda, Program Co-Chair, ACM CCS 2024, and Northeastern University Professor

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Ensuring Security in the Cloud: The Importance of Choosing a FedRAMP-Validated Cloud Service Provider ---------- *143*

By Emil Sturniolo, Chief Security Officer at ETHERFAX

Establishing a Cybersecure Maritime Ecosystem ---------- *147*

By Sandro Delucia, Product Director, Speedcast

Prevent Cyber Attacks with Deepfake Detection Technology - A Complete Guide ---------- *151*

By Ryan Jason, Facia.ai

Cybersecurity Changes Companies Should Be Considering for 2025 ---------- *154*

By Marcelo Barros, Director of Global Operations — Hacker Rangers

Silent But Deadly---------- *158*

By Wes Hutcherson, Global Technology Evangelist, runZero

The Cloud Security Playbook Safeguarding Data in The Digital Era ---------- *161*

By Hardik Shah, Software Engineer, Microsoft Corporation

Strengthening Cyber Crisis Response Through AI ---------- *164*

By Haris Pylarinos, Founder and CEO of Hack The Box

Three Emerging Cybersecurity Trends Shaping 2025---------- *168*

By Adam Finkelstein, SVP of Global Client Leadership at Sygnia

The Next Y2K Is Closer Than You Think ---------- *171*

By Paul Davis, Field CISO, JFrog

Use AI to Enhance Your Patch Management Strategies ---------- *175*

By Zac Amos, Features Editor, ReHack

What Can We Learn from Recent Telecom Hacks?---------- *179*

By Chris Henderson, Senior Director of Threat Operations, Huntress

The Next Security Frontier: Agentic AI---------- *183*

By Ben Kliger, CEO and co-founder, Zenity

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

@MILIEFSKY

From the

Publisher…



On behalf of Cyber Defense Magazine and Cyber Defense Media Group, we are pleased to announce that once again, we are partnering in the RSA® Conference 2025. This year's theme is "Many Voices. One Community." You can see more at https://www.rsaconference.com/events/2025-usa.

We proudly echo this message from the RSA announcement: "At RSAC 2025, you're not just attending a conference—you're stepping into a vibrant, thriving community of thinkers, innovators, and achievers. Though we come from different corners of the cybersecurity world, we are united by a common mission: to foresee risks, counter threats, and embrace the challenges ahead. Together, we shape the future of security. Together, we shine as one."

For Infosec Solution Providers: Entering the Global InfoSec Awards for 2025 is your chance to showcase your cybersecurity innovation to the world. These awards highlight cutting-edge solutions and offer industry validation, setting you apart from the competition. Winning brings credibility, media exposure, and new opportunities. Don't stay in the shadows — let the world see how you're leading the charge in cybersecurity.

https://cyberdefenseawards.com/

Stay vigilant. Stay secure. And remember — cybercriminals never sleep, so neither can your cybersecurity strategy.

Warmest regards,

Gary S. Miliefsky

Gary S. Miliefsky, fmDHS, CISSP®
CEO/Publisher/Radio/TV Host

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

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

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

EDITOR-IN-CHIEF
Yan Ross, JD
yan.ross@cyberdefensemagazine.com
ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

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

https://www.cyberdefensemagazine.com

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

PUBLISHER
Gary S. Miliefsky, CISSP®

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



13 YEARS OF EXCELLENCE!

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

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

PROFESSIONALS WIRE WEBINARS

CYBERDEFENSECONFERENCES

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Welcome to CDM's February 2025 Issue

From the Editor-in-Chief

In this February 2025 issue of Cyber Defense Magazine, we again broaden our scope to acknowledge the impact of natural disasters and attacks on critical infrastructure. Specifically, our lead article chronicles the experience of a Cyber Security professional in responding to the effects of the California wildfires.

As a lesson in resilience and sustainability, we need to take note and prepare for adverse events, whether natural or manmade, and whether deliberate or otherwise. We would note that this broader view of the profession gives us reason to recognize that our readership extends far beyond CISOs and IT technical experts.

Editorially, we are dedicated to providing actionable information to all our readers, whether they are high-level professionals or other interested parties whose operations depend on sound cybersecurity practices. As such, we strive to make our coverage accessible to readers at all organizational levels.

We still focus on AI, quantum computing, supply chain issues, and ransomware developments. And featured areas of concern include such critical infrastructure sectors as finance, health care, automotive applications, and defense endeavors. But in seeking to meet the needs of our growing audience, we are also dedicated to expanding our coverage for greater positive results across the board.

We always strive to be the best and most actionable set of resources for the CISO community and all users of digital technology in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group.

Wishing you all success in your cybersecurity endeavors,



Yan Ross
Editor-in-Chief
Cyber Defense Magazine



About the US Editor-in-Chief

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

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.


SPONSORS

NIGHTDRAGON





***"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

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

ACCELERATE

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

www.nightdragon.com



Protect Your Defense Business with Cybersecurity Support from NSA.

Small and medium sized defense contractors are frequently targeted by cyber criminals and nation-state threat actors alike. Don't let inadequate security measures put your intellectual property and networks at risk. Our no-cost cybersecurity services can help protect your business from evolving cyber threats.

GET STARTED TODAY

nsa.gov/ccc



UNKNOWN
CYBER

"70% of Malware Infections Go Undetected by Antivirus..."

Not by us. We detect the unknowns.

www.unknowncyber.com

zivver

Secure email.
Effortless compliance.

Protect your sensitive data with advanced email encryption

- Sensitive data identification
- Large file transfer
- Human error prevention

HIPAA COMPLIANT

Gramm-Leach-Bliley Act COMPLIANT

www.zivver.com

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations



Information security, cybersecurity and privacy protection for the legal profession

Download White Paper

Download our white paper to understand how the legal profession is under attack and how ISO/IEC 27001 can help mitigate the risk.

The legal profession depends on the flow of highly sensitive information, such as client data, personally identifiable information (PII), case details, sensitive contracts, financial records and intellectual property. This white paper reviews how the value of this information makes the legal profession increasingly at risk of cyberattack and how ISO/IEC 27001 can provide the framework to keep information secure, prevent unauthorized access and mitigate the risk should a breach occur.

SGS

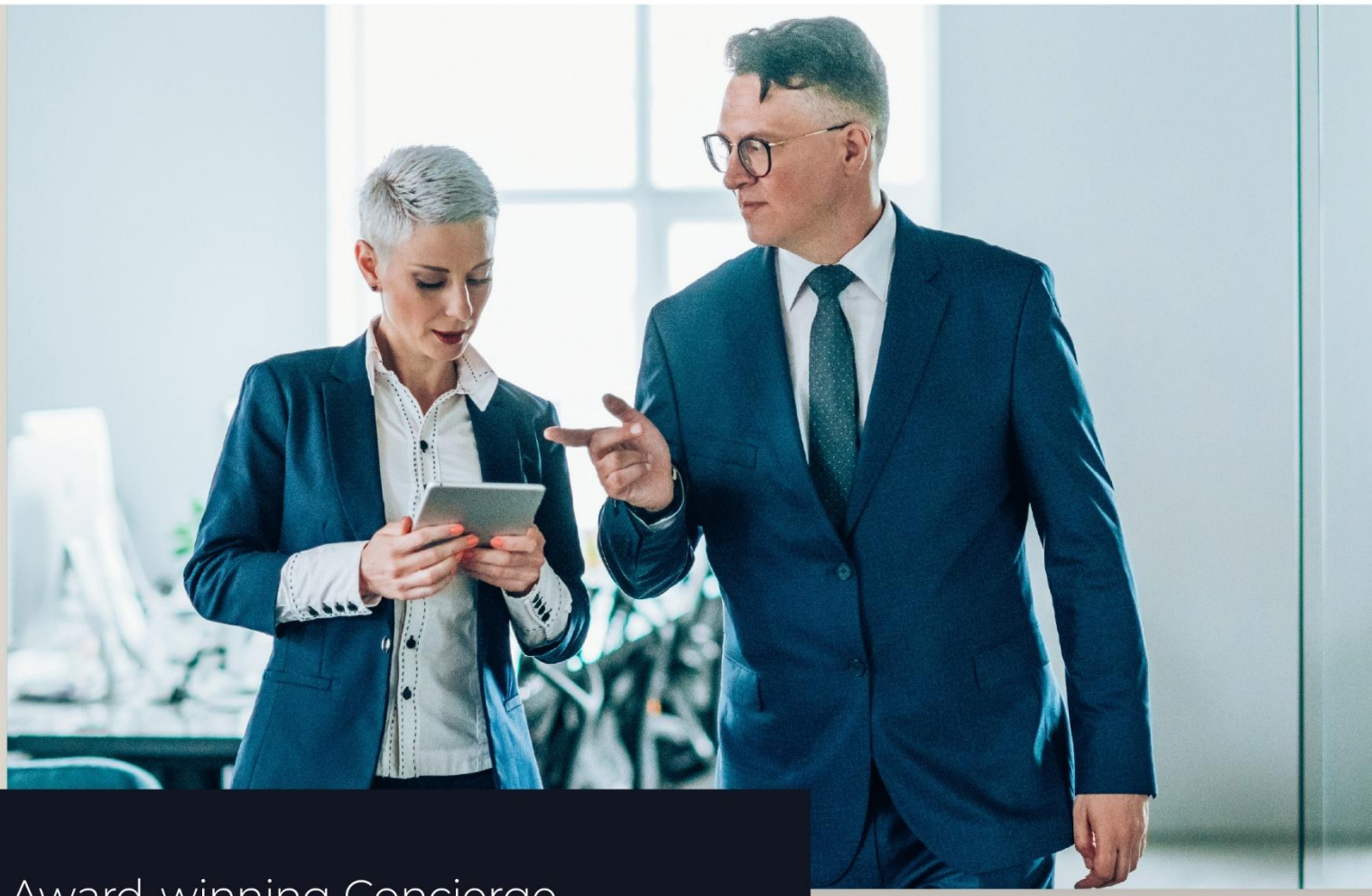
When you need to be sure

sgs.com

BLACKCLOAK™

Digital Executive Protection

Protecting personal digital lives requires an expert team and a tailored approach to ensuring that every aspect of digital privacy and personal cybersecurity is covered.



Award-winning Concierge Cybersecurity & Privacy™ Platform that protects you, your family, and your corporation.

LEARN MORE

CYE

Transform the way you manage cyber risk.

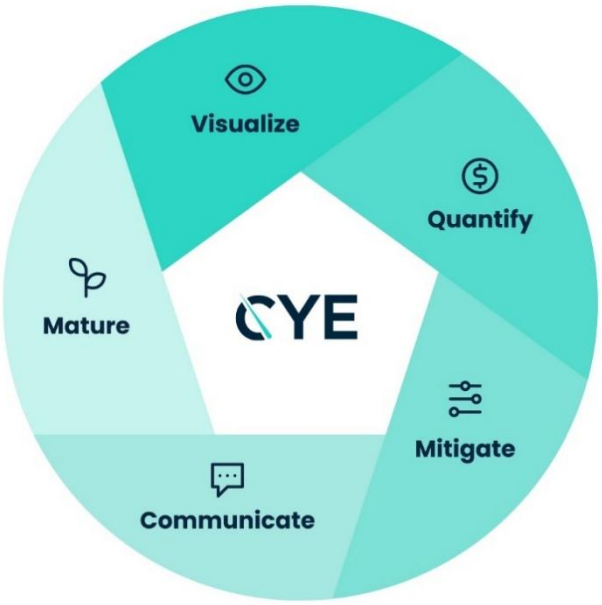
CYE's optimized cyber risk quantification solution enables you to:

Visualize

Predict probable attack routes by leveraging AI and data science with our SaaS platform.

Mature

Embrace transformation and unlock your organization's full potential with confidence.



Quantify

Determine the potential financial consequences of cyber risk in dollars, as well as the cost of remediation.

Communicate

Clarify and present your cyber risk in business terms to executives, security teams, and partners.

Mitigate

Focus your resources on addressing the most critical threats that truly pose risk to your business assets.

"The investment in CYE's tools and services has helped us receive the financial support over the past couple of years that we didn't have several years ago."

John Padilla, Associate VP of IT SONICWALL

The Benefits of Working with CYE

96%

of customers' business-critical attack routes are blocked within six months

88%

Reduction in remediation time following a cyber incident.

87%

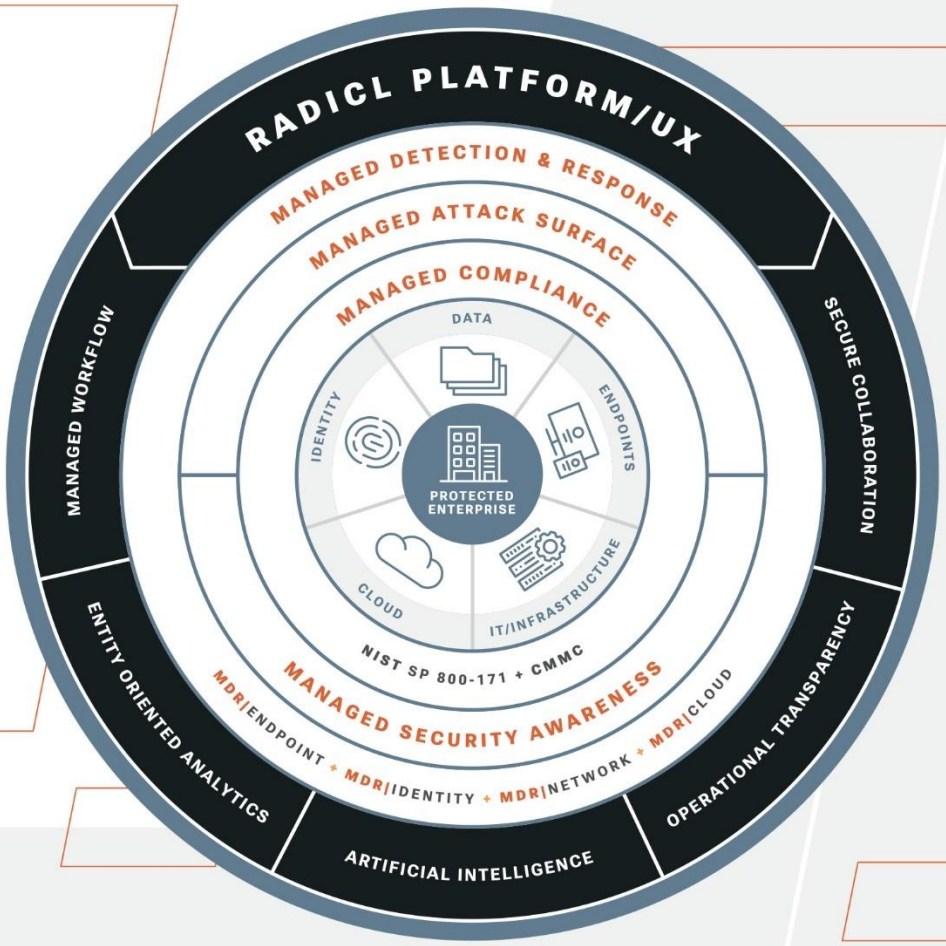
of customers improve ROI on their security budget.

Visit us at cyesec.com

RADICL™

We Protect American SMBs From Advanced Cyberthreats

If you want to maximally reduce your cyber incident risk, get RADICL!



- ✓ Endpoints Protected
- ✓ Identities Secured
- ✓ Vulnerabilities Reduced
- ✓ Incident Response 24 x 7
- ✓ CMMC / NIST 800-171 Assured



"Companies developing, holding, or delivering technology, information or operations of interest to nation state cyberthreats are being actively targeted by extremely advanced threat actors. These companies make up America's Defense Industrial Base (DIB) and Critical Infrastructure (CI) and are under constant attack. For the sake of national security, they must be better protected. These same companies, along with others in verticals like finance, legal, and healthcare are also in the crosshairs of motivated and advanced cybercriminals. RADICL was born to bring these "high value target" companies a radically different class of cyberthreat protection - protection previously only available to the largest of enterprises and government entities. If you desire the best protection possible, we'd love to talk to you."

Chris Petersen, CEO of RADICL

GIVING SMBS LONG-OVERDUE ACCESS TO ENTERPRISE-GRADE CYBERSECURITY PROTECTION.

RIDGE SECURITY

Make Your Risk Window Goal

ZERO

With Our Continuous Security Validation AI Agent

RidgeBot®

Get Started Today!

Keep up with CVE list published by CISA

Large exploit database 6000+

Wide testing coverage:

Windows
Linux
Websites
Database
OT / IoT
Cloud



WHEN MANAGING ASSET RISKS

PARTIAL VISIBILITY



IS JUST NOT GOOD ENOUGH.



WITH SEPIO, SEE ALL ASSETS. MANAGE ALL RISKS.

Learn more about Sepio's Asset Risk Management Platform >

www.sepiocyber.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Spin.ai

SaaS Security Platform for Mission-Critical SaaS Apps

Enhance Cyber Resilience, Security Operations, and Cost Efficiency



Schedule a Demo Today

www.spin.ai/demo

© 2024 Spin.AI. All rights reserved.

VMRAY

Good enough
is not enough.

SANDBOXING REINVENTED TO UNCOVER HIDDEN THREATS



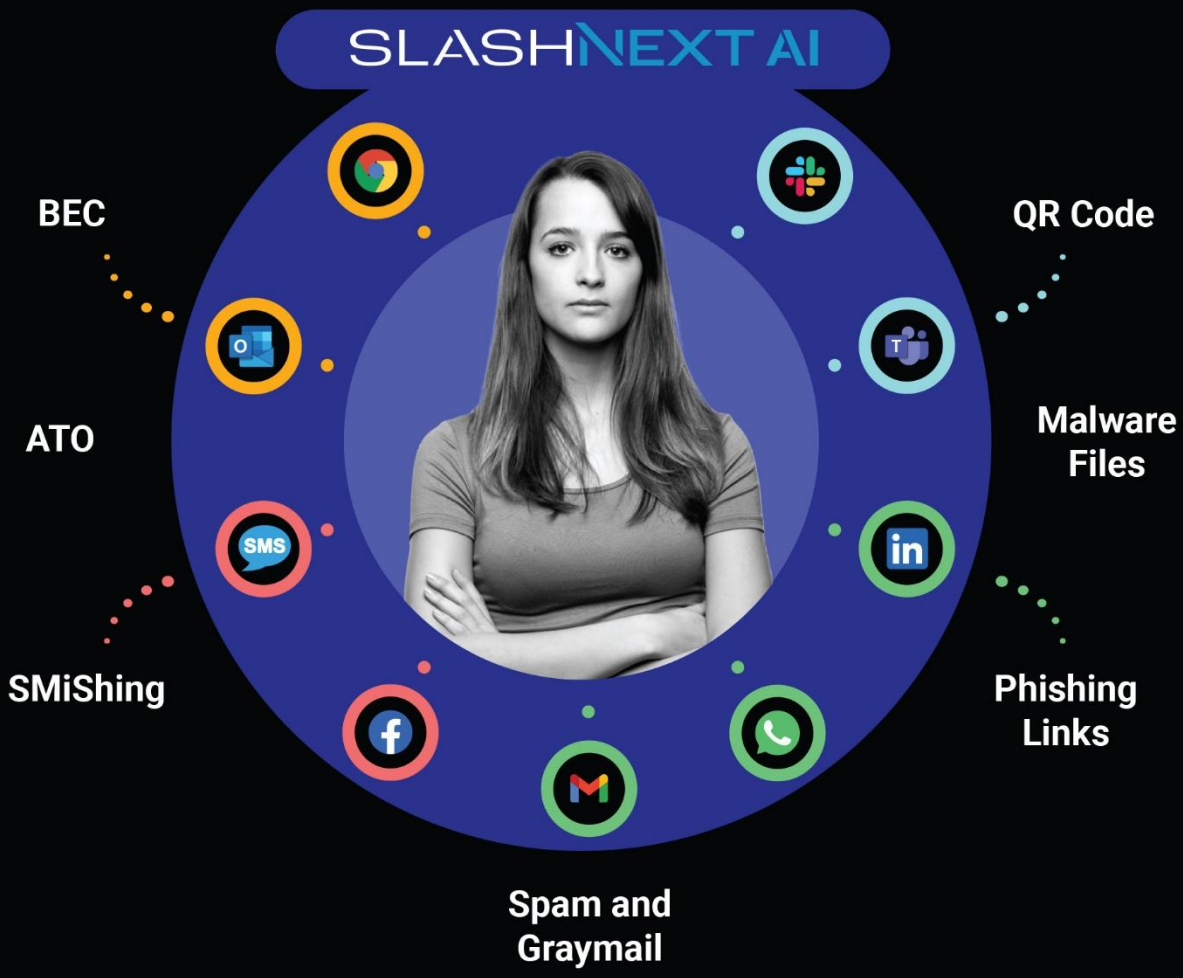
VMRAY.COM


BECOME THE
CYBER ARCHITECT
OF YOUR SECURITY STORY
Build a Strong Foundation for a Secure Future.
deepwatch™
www.deepwatch.com

SLASHNEXT

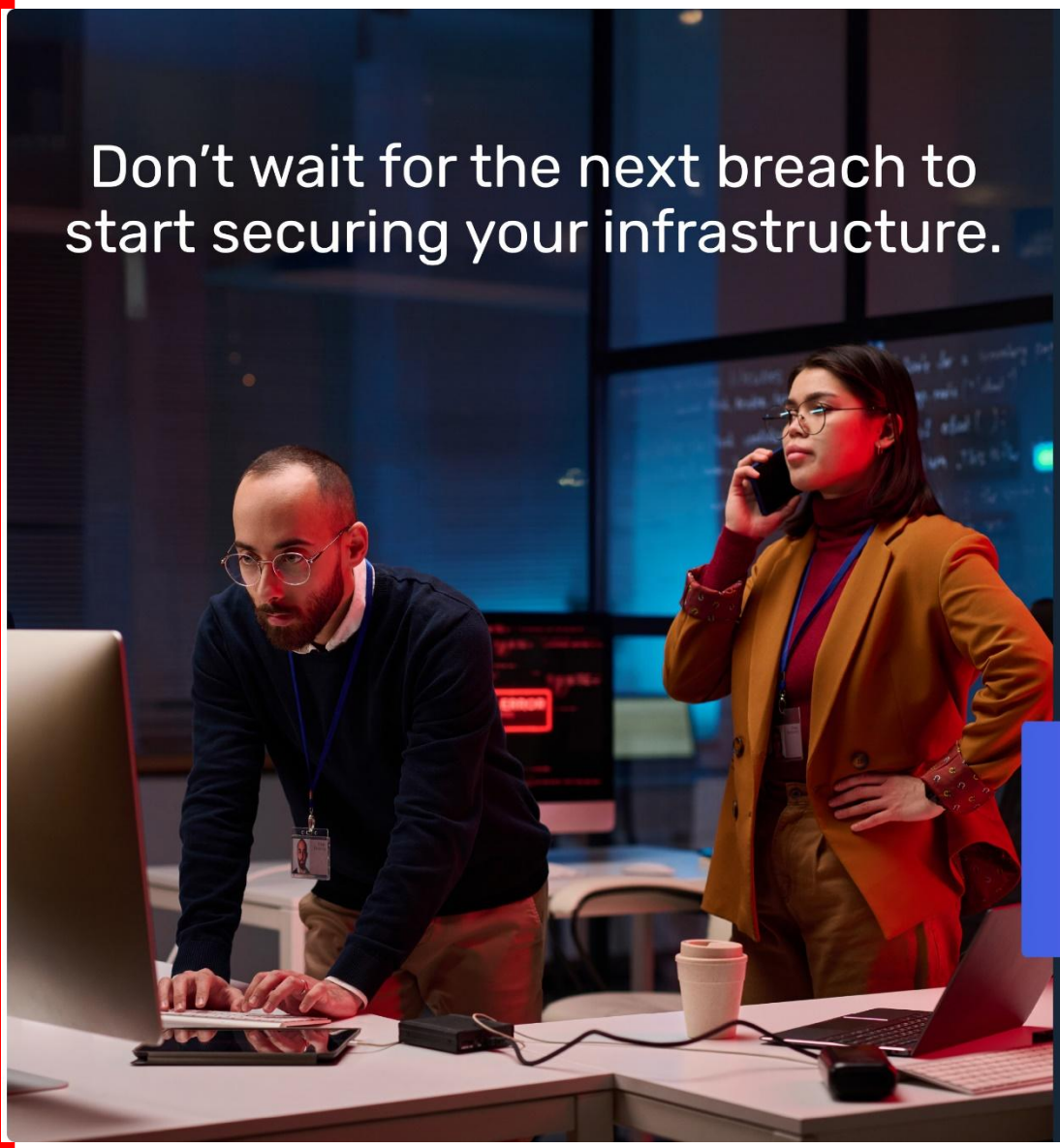
NEXT GEN AI EMAIL+ SECURITY

Make Email + Messaging Safe Again.



- 360° workspace protection
- 4X better threat detection
- 5 minutes to AI protection
- 2X higher SOC efficiency

www.SlashNext.com



Strengthening Your Security Post-Breach with Horizon3.ai

In today's rapidly evolving threat landscape, responding after a breach isn't enough. Horizon3.ai leads with a proactive defense approach through its cutting-edge autonomous penetration testing platform, **NodeZero**™.

With continuous cyber risk assessments, NodeZero adapts as your digital environment changes, ensuring long-term protection. NodeZero identifies and prioritizes vulnerabilities, providing actionable remediation strategies. Enhance your security posture, streamline stakeholder communication, and align defenses with organizational goals.



Visit **www.Horizon3.ai**
to download our white paper on
Enhancing Cybersecurity Post-Breach
and learn how NodeZero can safeguard
your organization against threats.

HORIZON3.ai

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Kodem

Security for everything you build.

Powered by runtime.

Kodem provides runtime-powered application security, giving you an attacker's view to discover, prioritize, and fix code, open source, and container risks across your stack.

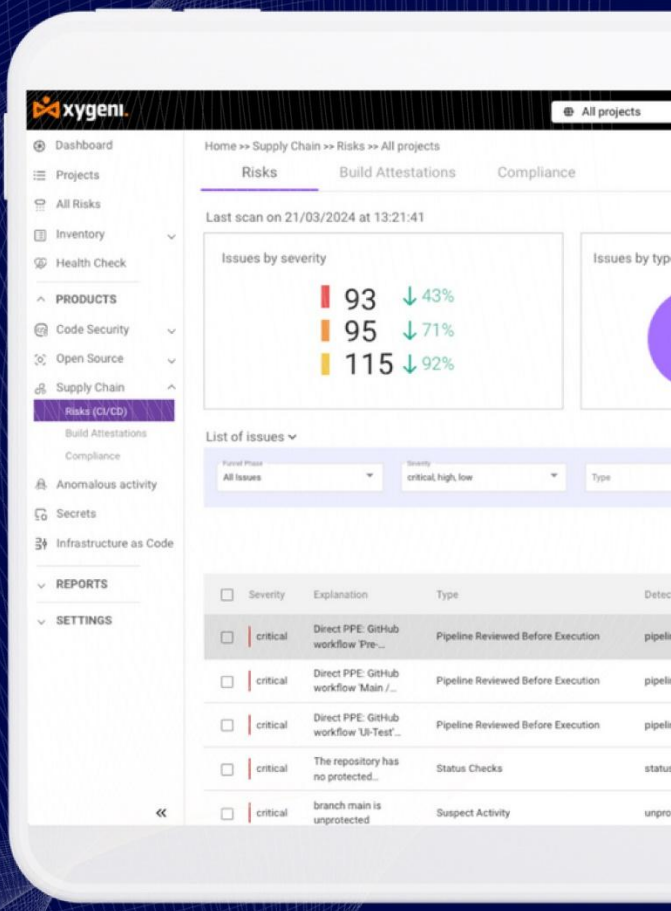
kodemsecurity.com

xygeni.

Secure Software Development & Delivery

- ASPM
- Open Source Security
- SSCS
- Build Security
- Anomaly Detection
- Code Security
- Secret Security
- IaCSecurity

Discover more at xygeni.io



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

this is why
hackers
hate us.

"Since you have ThreatLocker® installed, it became clear that we could not use Windows machines for our purposes."

– A real message
from an actual hacker.

this is why
you will
love us.

"Since you have ThreatLocker® installed, it became clear that we could not use Windows machines for our purposes."

– A real message
from an actual hacker.

Do you know your current systems' vulnerabilities?
Order your free
software health report now.

THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

threatlocker.com

THIRD-PARTY RISK MANAGEMENT

Modernize Your TPRM Program to Keep Up With Demand

Streamline Workflows and Maximize Your Team's Impact By Automating Steps So You Can Do More with Existing Resources



Simplify Monotonous Work So You Can Focus On Bigger Problems

TPRM teams spend countless hours on everyday tasks and burn through budgets and resources, leaving less time to focus on critical security concerns that will cause an impact.

Automate routine aspects of your program, from scoping your vendors to uncovering levels of inherent risk hiding in your portfolio. Turn elements of onboarding, ongoing monitoring, performance management, and even offboarding into a repeatable process to increase the volume of the third parties you focus on and free up more time to become a proactive protector of your organization.

Hands-Free Automation

Automate everything from assessment scoping to evidence collection with the click of a button. Run critical workflows in the background so that you can focus on impactful risk reduction.

Enterprise Integration

Seamlessly integrate with key enterprise systems such as Archer, MuleSoft, JIRA, Ariba, Archer and more through a robust web services-based API.

No-Code Configuration

Easily add features and functionality without relying on service engagements. Our platform is 100% configurable by the end user, meaning you don't have to wait weeks for the changes you need to meet program demands.

Reporting-as-a-Service

Provide stakeholders with the data that matters to them in seconds. Rapidly generate meaningful, board-ready reports that demonstrate the value of your program.

Implement Automation. Get Your Time Back.

Offload routine tasks to ProcessUnity to focus on TPRM work that matters.

- Sourcing – Automate the entire source to the onboarding lifecycle, simplifying RFx creation, supplier selection, and contracting.
- Onboarding – Streamline onboarding workflows, establishing a single, objective process for introducing new vendors to the business.
- Performance – Measure vendor performance against agreed upon SLAs and KPIs, track annual progress, and set threshold terms and alerts.
- Reporting – Generate dynamic reports and dashboards to get real-time visibility into the state of third-party risk.

ProcessUnity Third-Party Risk Management significantly reduces third-party onboarding and due diligence cycle times. Fueled by best-in-class workflow software, a universal data core for all TPRM information, the world's largest third-party risk exchange database and powerful artificial intelligence capabilities, ProcessUnity enables organizations to proactively mitigate first- and third-party risks.

ProcessUnity



txOne networks

Keep the Operation Running

TXOne Networks provides cybersecurity solutions that safeguard OT environments. Collaborating with top manufacturers and critical infrastructure operators, we develop practical, operations-friendly cyber defenses.

Copyright ©2024 TXOne Networks. All rights reserved.

txone.com

MACH37
CYBER ACCELERATOR

GET LAUNCHED

Our Mission

Today's real-time global connectivity has more complex threats and rapidly changing technology than ever before. In response, enterprise and consumer markets demand a steady stream of innovative new capabilities and solutions. MACH37 Cyber Accelerator® catalyzes the skills, foresight, and drive of the cyber industry's leading entrepreneurs, technologists, thought-leaders, and investors to anticipate that demand and accelerate the next generation of disruptive, high-growth cyber companies.

Our Program

Since 2013, MACH37® has operated in the heart of the cyber industry, just outside Washington D.C. in Northern Virginia. Our unique 90-day mentor-driven program leverages our workshops and expansive network of cyber experts from the public and private sectors to provide insights on how to build new cyber solutions and generate traction in the market. We emphasize the Lean Startup methodology and push technical founders out of the building so they develop and test their assumptions in a real world setting through brokered meetings with potential customers, channel partners, and investors. Using data collected from the market, we work with entrepreneurs to help them discover product-market-fit and hone their go-to-market strategy in a rapid time frame to build sustainable business models and drive growth.

MACH37® provides founding teams with extensive one-on-one mentorship from experts in entrepreneurship, strategy, public and private sector sales, marketing, product development, and venture capital investment. The advice from business and technical savvy mentors coupled with direct engagement with organizations facing cyber-related issues creates valuable connections that help founders prime a market for early product adoption. We give cyber startups a competitive advantage to attract seed-stage and Series A investors and become the next generation of leading cyber companies.

500-600
startups from around the world screened per year

450+ mentors world-wide

91 companies launched

84% of graduates are still in business

64% of graduates have raised follow-on investment post-Demo Day

$1M average seed round

hello@venturescope.com
www.venturescope.com
@venturescope

VentureScope®

STRATEGY · DEEP TECH · INVESTMENT

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

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

Expertise

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

2009
Founded

2010
Co-Founded and invested in WeatherAlpha

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

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

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

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

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

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

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

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

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

ALLEGISCYBER CAPITAL

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

The first dedicated cybersecurity venture firm in the world

About us

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

BUILDING AND FUNDING THE MOST INNOVATIVE COMPANIES IN CYBER

Signifyd | ELISITY | CONCEAL | panaseer | Synack

Lucidworks | DATATRIBE | DRAGOS | IRONPORT SYSTEMS | SHAPE SECURITY

www.allegiscyber.com

Altitude Cyber

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



Dino Boukouris

Managing Partner, Altitude Cyber

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

Founders & CEOs

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

Investors

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

Boards

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

Firm Highlights

Decades of experience as world class operators and advisors

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

Deep industry relationships and partnerships across strategic and financial partners

Cyber Network

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

Cyber Knowledge

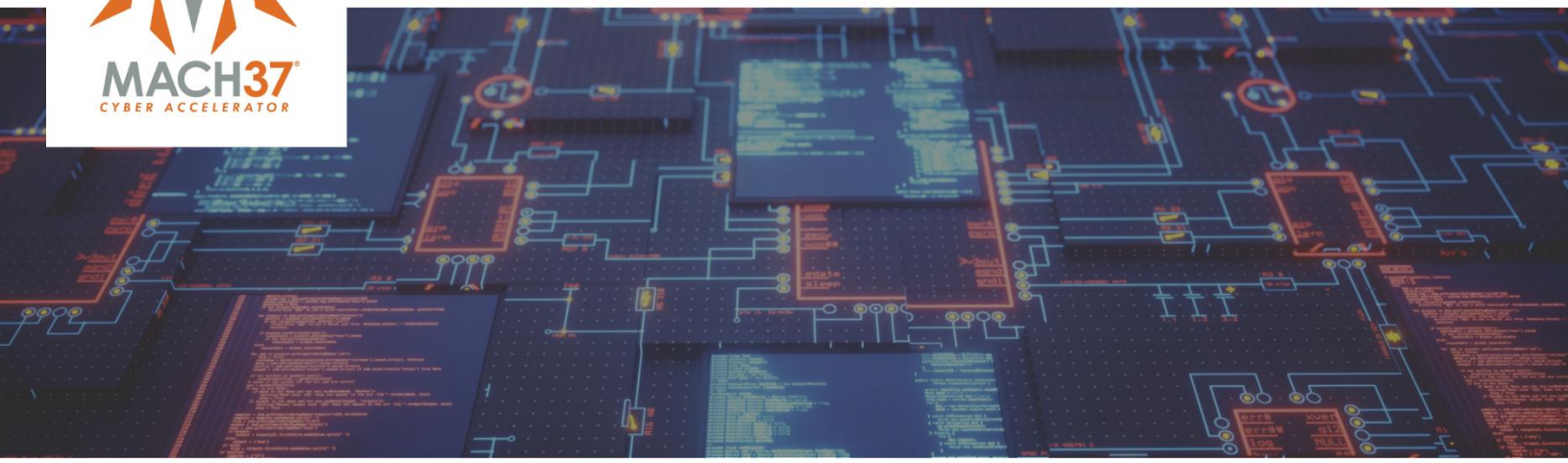
4,500+	Company Tracker
3,000+	M&A Transactions
8,500+	Financing Transactions

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

Altitude Cyber, LLC | www.altitudecyber.com

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

MACH37
CYBER ACCELERATOR



Our Industry Focus

- Cybersecurity
- Artificial Intelligence
- Machine Learning
- Space/Aerospace
- Quantum Computing
- Cyber Physical Systems
- Internet-of-Things
- Industrial Control Systems
- Neural Networks

Our Executive Team

Jason Chen | CEO & Executive Director | jason@venturescope.com

Jennifer Quarrie | COO, CWO & Strategy Director | jennifer@venturescope.com

Notable Alumni

RunSafe SECURITY

SylLab Systems

HUNTRESS

breachbits

HYPERQUBE

ATOMICORP

VIRGIL SECURITY

SYNCURITY
Built by Analysts, For Analysts

Optery FOR BUSINESS

PC PCMAG.COM EDITORS' CHOICE
2022, 2023, 2024

Remove your employees' personal data from the internet

- Prevent phishing & other social engineering attacks
- Reduce identity theft & fraud
- Protect your team from malicious actors
- Safeguard against real world harassment

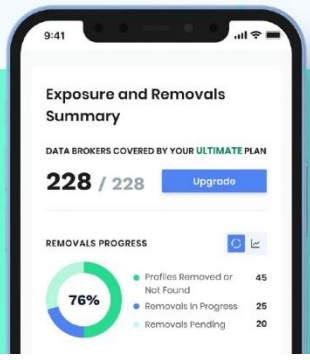
AS SEEN ON

SXSW · SECURITYWEEK · CR Consumer Reports · PC PCMAG.COM · TC · CNET · ZDNet · SC MEDIA

Why Optery for Business?

We're exclusively focused on data broker removal so you get the privacy & protection you need.

- Patented Search Technology
- Monthly Automated Scans & Removals
- Transparent Exposure & Removal Reporting
- Comprehensive Data Removal From Hundreds of Sites
- No Affiliations with Data Brokers
- SSO/SCIM/SAML Integration Options
- Clear, Affordable & Flexible Pricing
- SOC 2 Type 2 Certified



Create your free business account

business.optery.com/signup

SIXMAP

Zero Touch Automated **Network Defense**

See Every Port. Know Every Shadow.

SixMap provides automated, comprehensive visibility across IPV4 and IPV6 environments, uncovering hidden risks and prioritizing imminent threats. Discover every asset, pinpoint open ports, and protect your network – all we need is your name.

Schedule a Demo

Learn more and contact us at **www.sixmap.io**



www.cyberdefensemagazine.com



RSAConference™2025

San Francisco | April 28 – May 1 | Moscone Center

Many Voices.
One Community.



Together we secure.
Join us at RSA Conference 2025!

Cybersecurity's greatest challenges demand more than one perspective. That's why RSAC 2025 unites thousands of voices from around the world to collaborate, innovate, and secure our digital future.

From April 28 – May 1 you'll hear groundbreaking Keynotes, explore hands-on sessions, and participate in exclusive networking opportunities. This is where the global cybersecurity community connects to share insights and find solutions.

Why Attend?

- Hear from top experts tackling today's toughest challenges in cybersecurity.
- Experience cutting-edge solutions at the Expo that will drive your strategies forward.
- Collaborate with peers to unlock innovative solutions and gain fresh perspectives.
- Expand your network with professionals from every corner of the globe, forging connections that last a lifetime.

Be a part of something bigger. RSAC 2025: **Many Voices. One Community.**

Register now at RSAConference.com/cyberdefense25

#RSAC


ARTICLES



Expect The Unexpected

A First-hand Account of the 2025 Los Angeles Fires

Compounded By Lacking Disaster Recovery and Business Continuity Plans

By Karina Klever, CEO, Klever Compliance

Never did I think my living room would be wall to wall air mattresses accommodating friends whose houses had burned down. Never did I think this apocalyptic tragedy would be complicated even more by clients hitting a sheer state of panic because their businesses were at risk. While trying to manage all of this from the office at home, the power kept getting disconnected for varying periods. Luckily, I had several layers of redundancy to stay connected. The thawing meats that wouldn't fit into the RV fridge forced us to make and eat soups, supplemented by pizza. We had hot water since the gas was on, but the thermostat requires electricity as does lighting, so we all rotated hot showers with flashlights in the cold. Moving out of the uneasy space became a force of consciousness; I kept reminding myself that fires do not burn the seeds that are in the ground. I know there is inevitably a bright future ahead. Insurmountable recovery efforts will be starting soon, with the Olympics as a golden target, just a few short years away.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Not to minimize so many that have lost so much, but this article will focus on the business aspect of maintaining continuity in a crisis situation. These are the items that so many of us thought were definitely in place as part of our DR/BCP tabletops. For some companies, getting to the instructions meant rummaging through the drawers and dusting off the binders. Or maybe finding that email that had the folder link for that magical pdf you think you remember getting a few years back from that one consultant, gosh what was that guy's name. It would have been nice had there been enough time to find it all.

Yes, our businesses and jobs are our livelihoods. Many times, our identity, possibly our sense of pride, or even what causes angst, is attributed to our work. We will cover the business components after addressing the people first. Prioritizing people starts with simply knowing where they are and knowing that you've instilled in them expected behaviour patterns. Having a count for virtual and/or in-person workers reduces panic and lowers concern. If you believe that checking in with workers is a supervisory function, make sure your supervisors know this is expected of them. Instructions, drills, and reiterating expectations are critical here. This is not a back-shelf dust covered napkin scribble, rather an actively exercised methodology that's part of everyday company awareness. Solutions here may include emergency contacts being housed separately from main buildings, knowing how to use a land-line rotary phone (don't laugh, many have no idea how to do this), and having access to alternate communication methods &/or accounts. Putting political positioning aside, much of the coverage and connectivity the rest of the world received was made possible by Starlink, since many cell towers burned. Starlink is providing one month of connectivity free. The plan your company comes up with must be collaborative across departments and when done right, is not limited to an IT specific incident command hotline. It's most important to drill, drill, and then drill the execution of your plan, followed by another drill. Regardless of what you call it, training, or tabletop exercises, or a drill, it must be done.

During conversations with our clients during the fires, we heard complaints that they didn't know if their workers had survived. There was panic and concern. We reassured them that their workers must just be looking for housing and they were probably fine, but those were pacifying statements based on, well, nothing. As the days progressed, it became clear that the workers had no idea they had to notify anyone at work of their wellbeing. After all, everyone knew that LA was on fire. On the flip side, companies didn't know who they were missing, so didn't reach out. It was a complete disconnect amplified by lacking communications. As expected in a time of crisis, everyone was paralyzed with disbelief. This is why templatized communications, and headcounts, must always be at the ready. Prepare both internal communications and external communications as part of your normalized operations, in advance of an emergency. Internal communications can be department, role, or function specific – this is based on your audience. External communications can target varying recipients such as vendors or clients. Make sure that the person that needs to be contacted at your company is identified in your outbound message, and, that this contact person knows what kind of conversation to have when they're contacted. These may be questions about injuries or needed support.

We did have an overachieving client that had an emergency communication template at the ready and had one person assigned to receiving calls from workers. Your company may require more than one person. The other aspect working in this client's favor is they'd trained their workers on the necessity of providing notice of where they are in case of an emergency. This created a two-way well-paved road that removed guesswork, assumptions, panic, and fear. The client with a plan knew where everyone was, and their status, within hours - compared to other clients who were hoping and guessing, days later.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Now to the business of the business. Just like we need to know where our workers are, we need to know where our golden eggs are. For one client, golden eggs are vials of life-saving medicine that needs to remain frozen. Another client maintains a warehouse that is a critical component of a supply chain workflow. Potentially, your golden eggs support national infrastructure. Many of our clients consider their golden eggs to be data. Leveraging data classification principles identifies which data is the most important, or which inventory may be most important, so that proper protections can be built around it. For those that choose to hoard data and waste money on absurdities like encrypting publicly available data, stop. The bigger your dataset the more risk you have in accounting for it - for many reasons such as - too many vendors, too many backups all over the place, too many APIs that haven't been maintained, too many admins, too many tools to rely on, too many more examples. Many in the IT space say that it's impossible for each ticket to be a top priority – using this same adage, not all data is top priority. Without classifying your golden egg it's impossible to prioritize recoverability efforts because the entirety of the data may be too heavy a lift.

Data retentions and protections work best when data purposefulness and minimization principles are aligned to your actual company operations. The following principles rely on Data Classification: retention, destruction, encryption, access controls (including logical, physical, and APIs), and of course recovery. If backing up and recovering golden egg data looks exactly the same as backing up and recovering publicly available data, there are some definite efficiency opportunities.

There were two very succinct differences in our clients and how they handled this emergency. The clients who had too much data all over across vendors didn't know where to start assessing had they lost any data, how to find the most recent backup time/date stamp, what data was involved really, and they couldn't believe that one guy from IT forgot to update the recurrence before he went on vacation a few weeks ago. I heard too many stories about that darn lady from legal because she didn't know where the current version of the vendor contract was that had the phone number absolutely everyone needed, despite the IT Director thinking he remembered seeing something about data backup in there when it was signed a few years ago.

As a general rule for most clients, their DR/BCP documents were weak. Some were so weak they were literally empty templates. But interestingly, they were marked as 'done' because they appeared in the GRC folder. Guess everyone in the chain chose to not interact with these documents - Not the role that was supposed to write them, or review them, or approve them, or use them to conduct a drill. The lack of these instructions is really only hurting themselves. We need to force ourselves to stop and think what these are really for, and it isn't the auditors with their checklists. These are instructions for our people, our workers, our colleagues, our own folks, who just want to make it better and fix it. Just like the emergency communication templates that need to be created in a non-emergent situation, we have to document the instructions that need to be followed by our people who are in an emergency. There are countless sources of frameworks, best practices, approaches, recommendations and methodologies that can be followed when establishing DR/BCPs. If you don't want to do it yourself, hire someone.

Make sure your program aligns to your actual operations, else it is not followable and basically irrelevant. This means do not take those endless rows of vague controls and wrap non-existent processes around them just to mark off the completion of a policy, feeding into our industry's checkbox compliance madness. Another important element to consider if you are using templates is removing words that align

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

to ethereal timing or promises, such as: occasionally, periodically, frequently, sometimes, and shall. Instructions must be able to be followed exactly, because someone in a panic may not be able to decipher what exactly “frequently” means. Is it every five minutes? Fifteen minutes? One hour? Tomorrow? Be exact.

I’m compelled to insert some thoughts about tools. In short, many companies are drowning in them. Our expectations of having our staff come in and swivel chair between 3, or 5, or 7 platforms is absurd and contributing to our cyber security burnout. Not only do we have too many platforms, but they’re all sending emails too – creating yet another input of work to keep track of. Many of these platforms rely on the same source data for alerting, they just have different UIs. We’ve confused our environments unnecessarily making it impossible to effectively prioritize. On a good day trying to simultaneously look at multiple sources, while focusing on one and keeping the others updated, is just unnecessary busywork.

During the fires, the abundance of tools had a direct impact to preventing focus and determining what was important. The panic, combined with the multiple unprioritized inputs, just froze people because they had no instructions. The spin that too many tools caused erased the ability to enact basic DR/BCP principles such as risk management decisions, isolating impacted areas, bringing up alternate sites, and suspending access – they were just stuck at trying to figure out what tool was telling which part of the story and were completely overwhelmed. They had no idea where to start or what to do because no one had explained their role in case of an emergency. Unless there’s a high level of maturity, compounding competency areas such as change management don’t even have impact assessments aligned to business functions. In the middle of the madness, we had to calm clients down to traverse up the stack to gain a better understanding of potentially impacted departments, and lines of business.

Yes, there were clients that had plans. But even for them, we found holes although they were significantly less impactful to the business since the basics were covered. The frequent drills that these clients conducted reiterated what each person is accountable for when dealing with an emergency. Thankfully, they all remembered their targets and attacked them heads down, even in a panicky situation. These clients knew where their golden eggs were, were making decisions based on one source of truth, understood their priorities, had their workers and vendors accounted for, and were ready to make risk-based decisions on how to proceed while keeping operations intact. Their preparedness resulted in zero impact to their business, while, the clients that were in disarray caused themselves agony. Some clients are still recovering from the panicky decisions that were made.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Karina Klever is Chief Executive Officer of Klever Compliance. Karina has spent more than 35 years in technology, starting in 1989 as a computer operator. After programming and decades of project/program managing, compliance took a larger focus starting in the early 2000s. Karina would go on to establish GRC Centers of Excellence for Fortune 500 companies. Successes span industries, maturities, regulations, and frameworks. After years of witnessing compliance being implemented as nothing more than a checkbox exercise while leaving gaping security holes exposed, Karina opened her own boutique company to guide midsized companies into establishing governance programs that are appropriate for their particular industry, level of maturity, size, risk posture, and goals. Klever Compliance is on a mission to leverage appropriation and common sense across GRC Programs which results in better security and less unnecessary busywork.

Connect with Karina Klever www.linkedin.com/in/karinaklever. Follow Klever Compliance on LinkedIn https://www.linkedin.com/company/klevercompliance. Visit our website to understand our services https://www.klevercompliance.com/. Recordings of many past events, available for playback at your convenience, are available on our events page https://www.klevercompliance.com/events.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Zero-Day Exploits and State-Sponsored Threats: The Treasury Hack Exposed

By Debra Baker, CEO, TrustedCISO

On December 8, 2024, the U.S. Treasury Department suffered a cyberattack. CISA announced that China-sponsored hackers had breached the Treasury network and stolen unclassified documents. The attackers exploited a Zero Day critical vulnerability in the Beyond Trust application.

Apparently, this was a Zero Day vulnerability because Beyond Trust had not publicly announced the vulnerability when the attack occurred. Eight days later, Beyond Trust announced **CVE-2024-12356.** Since this was a state-sponsored attack, it is very difficult to prevent a Zero Day attack because even the vendor was unaware of the vulnerability.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

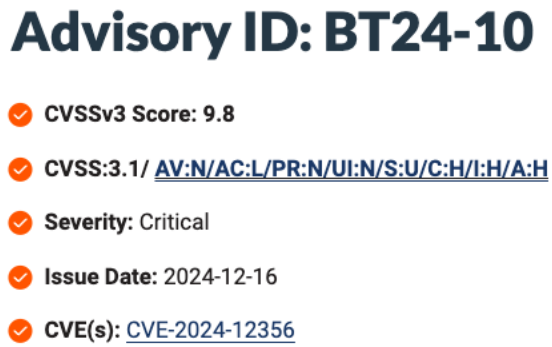


Figure 1 – Beyond Trust CVE-2024-12356

What is a Zero Day Vulnerability?

A zero-day vulnerability is a security flaw in software or firmware that is unknown to the vendor. Because it is undiscovered or not yet publicly disclosed, there are "zero days" available to mitigate or patch the vulnerability before it can be exploited.

Breaking Down the Vulnerability

The vulnerability, detailed under Advisory ID **BT24-10**, affects all versions of PRA and RS prior to version 24.3.1. **CVSS score of 9.8** out of 10 being the worst, shows how this is such a critical vulnerability. The reason is that it is exploitable over the network with no authorization required. When prioritizing **Common Vulnerabilities and Exposures (CVEs)**, there are three specific indicators plus the next hop to determine the urgency of addressing a vulnerability.

1. **Attack Vector (AV:N)**
2. **Attack Complexity (AC:L)**
3. **Privileges Required (PR:N)**

I cover the most important aspects of a vulnerability rating in my book CISO Guide to Cyber Resilience. One of the key metrics to consider in a CVSS score is the **Attack Vector (AV).** The Attack Vector metric describes an attacker's method to access the vulnerable asset. An attack vector labeled **"N"** denotes a **network-based attack**, which means the vulnerability can be exploited over the internet. This type of vulnerability is also known as a **remote code execution (RCE)** flaw.

For instance, if your company operates an externally facing web server with a network-exploitable vulnerability, it is critical to patch the server immediately. Such an asset effectively becomes a **ticking time bomb**, vulnerable to discovery and exploitation by hackers.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The next CVSS metric – Attack Complexity (AC), pertains to the external conditions that must be met for an attacker to successfully exploit a vulnerability. Essentially, the attack complexity classifies whether the vulnerability can be easily be exploited by a less-experienced hacker (AC:L). The easier it is to exploit the vulnerability, the lower the skill level of a hacker needed to exploit it.

The CVSS metric – Privileges Required, is based on the privileges required to carry out an attack and leverage the vulnerability. In this case with a "N" (PR:N), no privileges are required to exploit the vulnerability. The attacker does not need to be signed in or have access to the system's settings or files to initiate the attack.

These three indicators together **(AV:N), (AC:L), (PR:N)** mean this is an easily exploitable vulnerability from the internet. Other important aspects to take into consideration is the location and next hop of the device. For example, if the vulnerable device is externally visible on the internet, then it needs to be patched immediately or follow CISA's known exploitable vulnerability (KEV) catalog guidance. CISA gives recommended dates to patch actively exploited vulnerabilities.

Back to the Treasury Breach

The Treasury department's identity and access management system, Beyond Trust was compromised. What happened is that a critical vulnerability **CVE-2024-12356** was exploited to gain unauthorized access to the Treasury's network.

Through a malicious client request, attackers could execute operating system commands in the context of the site user. This flaw created a backdoor for hackers, enabling unauthorized access to sensitive Treasury workstations. As we learned above, there was no account or password required to exploit the vulnerability.

Lessons Learned

Because this was a Zero-Day exploit, there was no patch to apply. What this does highlight is that Regular penetration testing should be completed not just on production systems, but while the product is in development. I am a strong advocate of DevOps having a separate Penetration Team that is embedded in DevOps, but reports to the Information Security Team. This also highlights CISA's new Secure by Design initiative. All software development firms need to be doing more robust quality assurance testing before code is published to production. In general, I think that quality assurance teams are not given the budget, adequate time, or influence to ensure that quality secure code is being released. DevOps managers are pressured to meet unrealistic release dates, rather than quality code. You can see in the chart below from cvedetails.com, the massive problem with vulnerabilities that has only gotten worse in the past few years.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

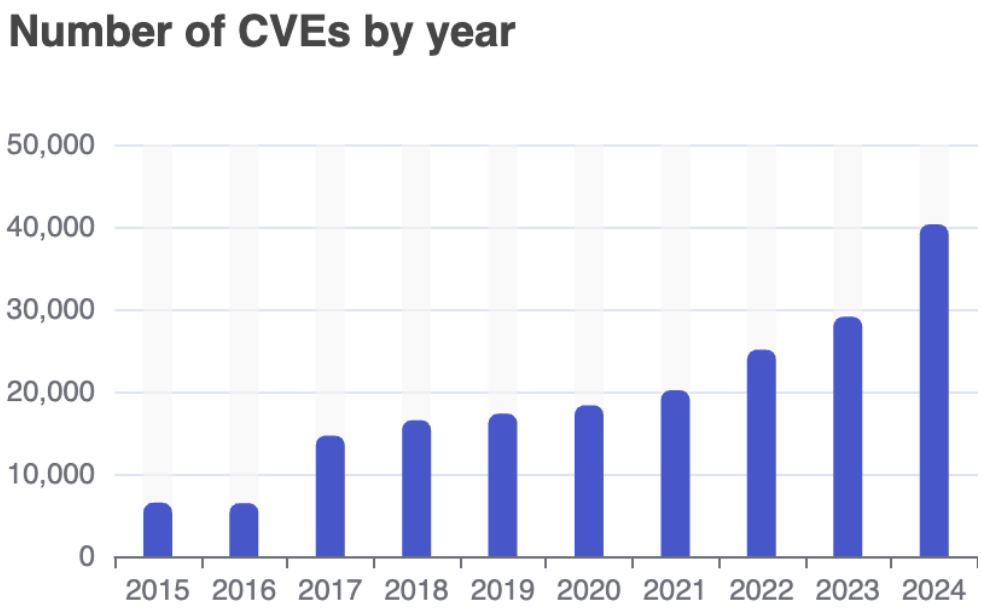


Figure 2 – Courtesy of https://cvedetails.com

Moving Forward

The U.S. Treasury attack is a stark reminder of the risks posed by unpatched vulnerabilities in critical systems. CVE-2024-12356 should serve as a wake-up call for federal agencies and private organizations alike to prioritize cybersecurity, implement rigorous vendor assessments, and stay ahead of emerging threats.

Preventative Steps for Organizations

To prevent similar attacks, organizations should:

1. **Conduct Continuous Monitoring:** Use advanced intrusion detection and prevention systems (IDS/IPS) to identify and mitigate anomalies in real-time.
2. **Conduct Regular Manual Penetration Tests:** Use a reputable Penetration Company to conduct manual penetration tests on your SaaS Service. For such a high security SaaS as Beyond Trust, quarterly manual penetration tests should be conducted.

Conclusion

CVE-2024-12356 should serve as a wake-up call for federal agencies and private organizations alike to prioritize cybersecurity, implement rigorous vendor assessments, and stay ahead of emerging threats. Especially, software development companies need to put an emphasis on quality assurance and tie Key

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Performance Indicators (KPI) to vulnerabilities for DevOps all the way to the CEO. This should be a wakeup call to all software development companies that quality assurance is paramount and more important than meeting release dates. Until we get the software vulnerabilities under control, the attackers are at a great advantage.

About the Author



Debra Baker, CEO of **TrustedCISO**, is a seasoned cybersecurity leader with over 30 years of experience, including a distinguished career in the U.S. Air Force and senior roles at IBM and Cisco. As the CEO of TrustedCISO, she provides expert guidance in strategic cybersecurity, risk management, and compliance. Debra helps organizations tackle complex frameworks such as SOC 2, ISO 27001, FedRAMP, StateRAMP, and NIST. A CISSP and CCSP-certified professional, she also holds a provisional patent for an AI-powered vendor assessment tool. Founder of **Crypto Done Right** and recognized among the Top 100 Women in Cybersecurity, Debra is also the author of **A CISO Guide to Cyber Resilience: A how-to guide for every CISO to build a resilient security program**. Her book is available for purchase on Amazon.

Debra can be reached online on LinkedIn, X, and at our company website www.trustedciso.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Cyber Insurance Applications: How vCISOs Bridge the Gap for SMBs

By Pete Green, vCISO and Cybersecurity Consultant and Reporter for CDM

Increasingly, small and medium-sized businesses (SMBs) face challenges in securing the right cyber insurance coverage. Unlike traditional insurance policies, cyber insurance applications are complex, proprietary to each carrier, and require a deep understanding of cybersecurity practices. For many SMBs, the process can be overwhelming and riddled with pitfalls. This is where the expertise of a virtual Chief Information Security Officer (vCISO) becomes invaluable.

A vCISO's role goes beyond providing strategic cybersecurity oversight. Virtual CISOs act as critical advisors, guiding SMBs through the intricate process of obtaining and maintaining cyber insurance coverage. From completing initial applications to handling renewals and managing claims, vCISOs ensure that businesses navigate these processes with confidence and readiness. They also help SMBs understand broader cybersecurity trends and how these impact their insurance needs, ensuring that decisions are both informed and forward-looking.

Streamlining Cyber Insurance Applications

The first step in obtaining cyber insurance—completing the application—can be daunting. These forms are far from standardized. Each insurer's application delves into unique technical requirements, asking businesses to detail their incident response plans, endpoint protections, and even third-party risk management strategies. For SMBs without in-house expertise, these forms often seem incomprehensible.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

vCISOs play a key role in this process by:

1. Conducting a comprehensive gap analysis to compare the organization's cybersecurity posture against the insurer's expectations.
2. Identifying and implementing necessary improvements, such as deploying multi-factor authentication or improving data backup processes.
3. Crafting tailored responses for each application, ensuring the language aligns with insurer expectations.
4. Collaborating across teams to minimize errors and expedite approval, often resulting in better terms for SMBs.

Interestingly, a 2023 report indicates that 41% of SMBs state that a lack of knowledge is the biggest challenge to staying prepared against cyber threats (Firewall Times). This underscores the importance of expert guidance to navigate the process and prevent application rejections.

In addition to these steps, vCISOs often assist SMBs in preparing for future insurance needs by maintaining detailed records of implemented security measures and ensuring that they are continually updated. This proactive approach positions the organization as a lower-risk candidate in the eyes of insurers, potentially leading to better coverage and/or lower premiums over time.

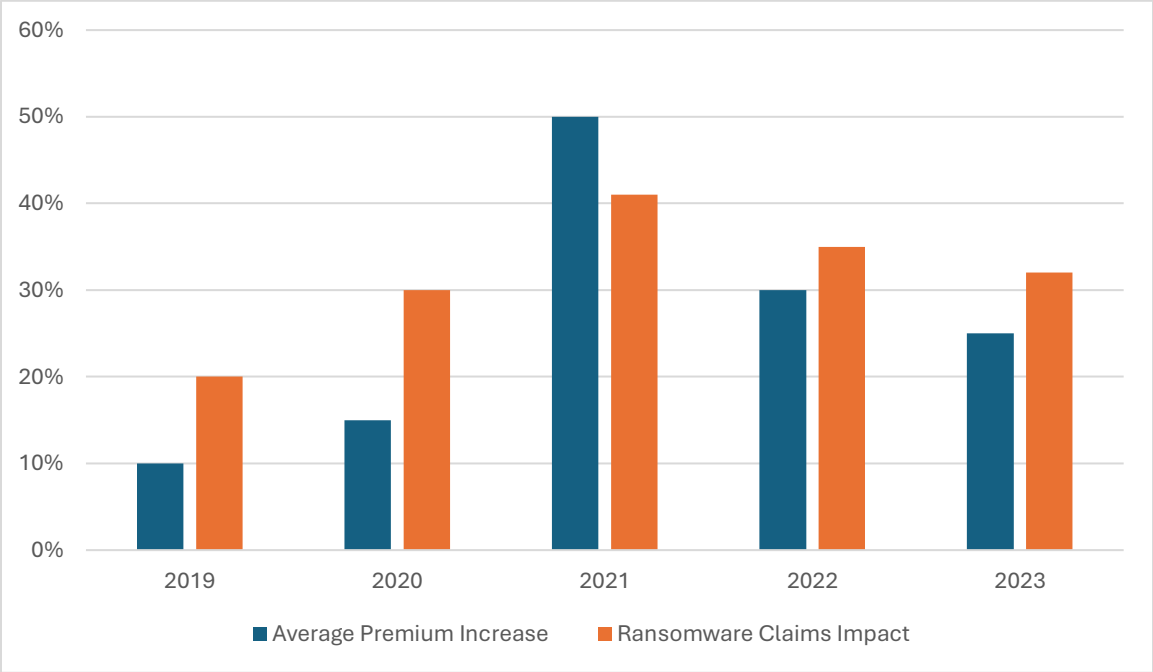


Table 1 – Average Premium Increases and Associated Ransomware Claims Impact

Sources: Marsh McLennan, "Global Insurance Market Index" (2022), Fitch Ratings, "Cyber Insurance Market Under Pressure from Ransomware" (2022), S&P Global Market Intelligence (2023), Gallagher Insurance, "Cyber Insurance Market Update" (2023)

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Preparing for Annual Renewals

Annual renewals present a new set of challenges. Policies evolve, and insurers introduce stricter requirements or higher premiums, often leveraging AI-driven tools to assess an applicant's cybersecurity maturity. Businesses unaware of these changes risk losing coverage or paying significantly more.

vCISOs tackle renewals head-on by:

- Reviewing existing policies and identifying new obligations.
- Ensuring SMBs compile the documentation insurers demand, such as penetration testing results or updated incident response plans.
- Demonstrating proactive improvements, such as adopting zero-trust principles, to illustrate a business's commitment to reducing risk.

In some cases, the renewal process can be straightforward. For organizations that have maintained strong security practices and completed initial insurer requirements, the vCISO's role might be limited to routine checks and minor updates. However, when premiums spike or terms change dramatically, the vCISO can negotiate with insurers to secure more favorable terms.

Cyber insurance premiums surged by 50% in 2022 as increased ransomware attacks and online commerce drove demand for coverage (Insurance Journal). This makes the renewal phase more critical than ever.

Beyond assisting with renewals, vCISOs also help SMBs stay prepared for mid-year audits or unexpected insurer inquiries. These interactions are increasingly common as insurers work to verify ongoing compliance with policy terms. The vCISO's ability to provide clear, organized evidence ensures that such audits proceed smoothly and without complications.

Navigating Claims Management

When a cyber incident occurs, filing a claim can feel like a second disaster. Policies are complex, and insurers scrutinize every detail—often using AI systems designed to flag inconsistencies. A vCISO provides crucial support during this high-stakes process.

Immediately after an incident, the vCISO ensures all necessary documentation is compiled, including forensic reports and incident logs. They interpret policy language to confirm the claim aligns with covered scenarios and work collaboratively with insurers to clarify technical details. Their approach minimizes delays and fosters trust.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Claims processes often introduce additional challenges when insurers rely on AI for evaluation. To counter this, vCISOs structure evidence in a format that AI tools can easily process. This ensures that critical data points are not overlooked and that valid claims are processed efficiently.

One noteworthy anecdote involves a mid-sized retail company that suffered a ransomware attack in 2023. The company's policy covered ransom payments, but due to improperly documented incident response actions, the insurer initially denied the claim. A vCISO was brought in to reframe the evidence and align it with policy requirements, ultimately securing a $1.2 million payout. This case highlights the critical role of vCISOs in claims management.

Additionally, the increasing reliance on AI-driven claims processes introduces both opportunities and risks. While AI can speed up evaluations, it can also misinterpret nuanced evidence. vCISOs, with their expertise in aligning evidence to insurer expectations, ensure that these technological gaps do not jeopardize legitimate claims.

The Value of Proactive Risk Evaluation

Proactive risk evaluation is a game-changer for SMBs seeking to maintain robust insurance coverage. vCISOs conduct regular risk assessments to quantify an organization's security posture and benchmark it against industry standards. This not only identifies areas for improvement but also helps maintain compliance with evolving insurer expectations.

Routine audits—led by vCISOs—keep security controls effective and relevant. Third-party risk evaluations are particularly valuable, given the rise in supply chain attacks. By ensuring vendors meet security standards, SMBs reduce their overall risk profile and strengthen their position during insurance applications and renewals.

Employee training programs also play a critical role. By educating staff on phishing, social engineering, and other common threats, vCISOs help prevent incidents before they occur.

Insurers often view such initiatives favorably, reflecting the organization's commitment to cybersecurity best practices.

vCISOs also assist in simulating potential attack scenarios and testing the organization's readiness to respond. These simulations, often conducted as tabletop exercises, provide invaluable insights into areas needing improvement and reassure insurers of the organization's preparedness.

Why vCISOs Are Essential for SMB Cyber Insurance

For SMBs, navigating the cyber insurance landscape is no longer just a box-checking exercise. Insurers demand detailed evidence of security measures, continuous improvement, and alignment with industry best practices. vCISOs bring the technical expertise and strategic perspective necessary to meet these demands while empowering SMBs to strengthen their overall security posture.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

From crafting tailored application responses to managing claims with precision, vCISOs bridge the gap between technical complexity and business needs. Their proactive approach ensures that SMBs not only secure coverage but also build resilience against future threats. As cyber insurance continues to evolve, the role of vCISOs will remain indispensable in helping businesses navigate this critical aspect of modern cybersecurity strategy.

About the Author

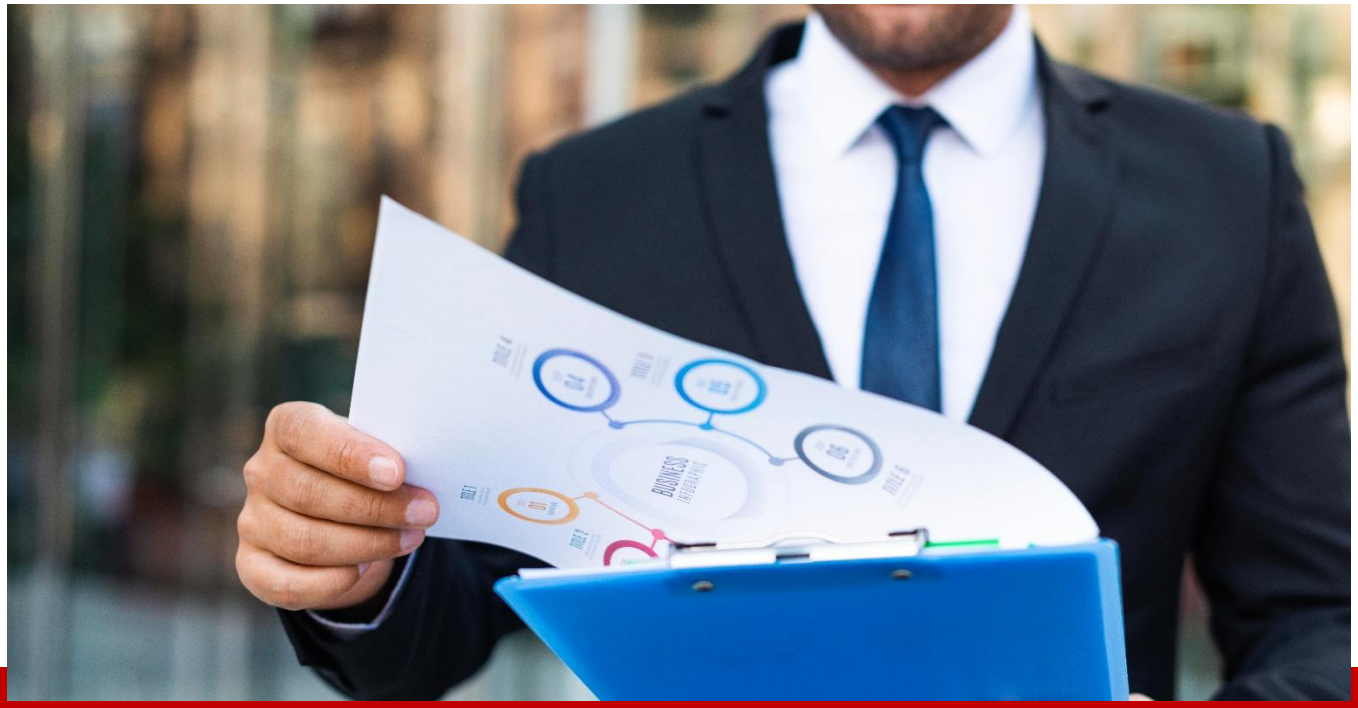


Pete Green, vCISO, Cybersecurity Consultant and Reporter for CDM. Pete Green has over 20 years of experience in Information Technology related fields and is an accomplished practitioner of Information Security. He has held a variety of security operations positions including LAN / WLAN Engineer, Threat Analyst / Engineer, Security Project Manager, Security Architect, Cloud Security Architect, Principal Security Consultant, Manager / Director of IT, CTO, CEO, and Virtual CISO. Pete has worked with clients in a wide variety of industries including federal, state and local government, financial services, healthcare, food services, manufacturing, technology, transportation, and hospitality.

Pete holds a Master of Computer Information Systems in Information Security from Boston University, an NSA / DHS National Center of Academic Excellence in Information Assurance / Cyber Defense (CAE IA / CD), and a Master of Business Administration in Informatics.

Pete can be reached online at greenish@gmail.com, @petegreen, https://linkedin.com/in/petegreen and at our company website https://www.cyberdefensemagazine.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Balancing Control, Compliance, And Continuity

What 2024 Taught Us About the Need for Hybrid Infrastructure

By Jerry Kaner, CEO, Ciphertex Data Security

For many organizations, the cloud has been a “game changer.” The convenience of hosted applications, the appeal of “pay-as-you-grow” models, and the promise of global reach led to its widespread adoption across industries. Unfortunately, several major outages last year revealed that public cloud platforms, however robust, are not fail-proof.

As systems went down, organizations across sectors found themselves temporarily paralyzed and vital services, from healthcare to banking, ground to a halt, impacting not just the entities themselves, but also those they serve. The financial toll was staggering, with downtime costs estimated to exceed $1 million per hour in some cases, and the operational fallout was equally substantial.

While cloud computing offers undeniable advantages in scalability and cost-effectiveness, ensuring business continuity and data security necessitates a more sophisticated, multi-layered approach. To stay ahead of the curve, organizations are leveraging hybrid infrastructure, where private clouds and Network-Attached Storage (NAS) systems complement public resources and create an adaptable framework that mitigates unforeseen disruptions.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Understanding Hybrid Infrastructure

Private clouds, by definition, operate with greater isolation and direct oversight, allowing enterprises to dictate the terms of compliance, performance, and resource allocation. In parallel, Network-Attached Storage (NAS) anchors essential data closer to home, mitigating the risks tied to single points of failure as well as keeping mission-critical information accessible and securely contained within familiar parameters.

Together, hybrid systems help form a stable core of resilience by allowing organizations to preserve functionality and prevent catastrophic downtime—even when larger systems falter. Additional measures like automated backups, encryption protocols, and immediate failover options ensure that if a public platform experiences a sudden disruption, the private environment can continue to operate, avoiding a system-wide standstill and the costly fallout that inevitably follows.

Strategic Allocation of Workloads and Risks

The ability to fine-tune resource distribution is a key advantage of leveraging hybrid infrastructure. Instead of relying solely on public resources that may buckle under unexpected strain, organizations can assign their most business-critical workloads to private clouds fortified by NAS. By doing so, they effectively limit vulnerability, preserve core operations, and maintain continuity in the face of market or infrastructure upheavals.

Meanwhile, non-critical processes that benefit from elasticity and pay-as-you-use economics can be offloaded to public platforms with fewer reservations. This division not only economizes resource expenditure but also clarifies the lines of defense. When downtime occurs, the private segment's localized systems respond decisively, buffering crucial services against the ripple effects of system-wide outages. It is a deliberate, thoughtful approach—one that recognizes that not all operations are created equal and that sensitive information deserves an added layer of protection.

Enhancing Cybersecurity Through Intelligent Integration

Digital adversaries continuously evolve and businesses who want to stay ahead must advance their security measures in tandem. Modern NAS doesn't stand passively by, holding static copies of data; it integrates intelligent safeguards that actively deter, detect, and contain attacks as they occur. For instance, security platforms augmented with machine learning and AI can spot subtle anomalies in traffic patterns, continuously verifying user and device identities before granting access.

Zero-trust architectures, encryption at rest and in transit, and well-segmented network zones intensify defense-in-depth strategies. With NAS serving as a focal point of data integrity, organizations gain the ability to isolate threats before they metastasize into full-scale breaches. Rather than reacting to incidents after the fact, they operate in a proactive posture—reducing the likelihood of critical data ever being compromised, and ensuring that even when under siege, vital assets remain shielded and recoverable.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Meeting Compliance and Regulatory Mandates

For organizations bound by strict legal frameworks and industry-specific standards, the need for transparent, traceable data management cannot be overstated. Private clouds reinforced with NAS offer not only a technological advantage but also a vital compliance safeguard. Localizing data storage means clearer audit trails, quicker response to external inquiries, and a tangible assurance that sensitive information remains under controlled jurisdictional boundaries.

In regulated sectors—healthcare, finance, and beyond—meeting mandates like HIPAA, PCI DSS, or GDPR involves more than just checking boxes. It requires demonstrable stewardship over the data's life cycle, from secure retention to timely recovery. With private and localized storage at the center, organizations find it easier to prove the integrity of their controls and the reliability of their records, satisfying even the most stringent oversight without compromising productivity or availability.

Economic and Operational Benefits Beyond Security

While resilience and compliance stand as fundamental drivers, the advantages of a hybrid model underpinned by NAS extend well beyond fortifying defenses. By selectively distributing workloads, enterprises free themselves from the trap of vendor lock-in, gaining the flexibility to pivot between providers or solutions without disrupting core functions. This adaptability not only reduces long-term costs but also simplifies scaling decisions as market conditions shift.

Tangible savings emerge when critical workloads run seamlessly on private infrastructure, avoiding unplanned outages and the staggering downtime costs they incur. Over the long haul, more predictable budgets and reduced exposure to risk translate into balanced growth strategies rather than reactive firefighting. In short, by blending public, private, and NAS elements, organizations can strike a sustainable equilibrium—ensuring that fiscal responsibility, strategic foresight, and operational agility remain as integral to their success as security and compliance.

Practical Steps for Strengthening Infrastructure and Mitigating Risk

Having witnessed the drawbacks of overreliance on any single platform, organizations now have the opportunity to chart a more stable, secure, and adaptive course. A few practical measures can help streamline this process:

1. **Evaluate Workloads and Data Sensitivity:** Identify which functions are mission-critical and which are not. Assign sensitive operations to private clouds fortified by NAS for enhanced control and reliability, while entrusting less critical tasks to public platforms that offer flexibility and cost benefits.

2. **Leverage Integrated Security Tools:** Incorporate AI-driven detection, zero-trust protocols and segmented network zones to ensure that both private and shared environments work in concert

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

against evolving threats. By placing NAS at the core of your data strategy, you remain prepared to isolate and neutralize breaches early.

3. **Establish and Maintain Clear Compliance Frameworks:** Align data storage practices with relevant regulations. Localize sensitive information, streamline audits, and simplify responses to legal inquiries by employing private cloud and NAS combinations that provide transparent, traceable records.

4. **Test Continuity and Recovery Scenarios:** Conduct drills, simulate outages, and verify that failover systems engage as intended. By proactively testing these mechanisms, you confirm that your hybrid configuration not only looks good on paper but functions reliably when it matters most.

5. **Adapt as Requirements Evolve:** As market dynamics shift and regulatory guidelines evolve, review your infrastructure choices. Adjust the balance of public and private resources, refine your backup strategies, and consider emerging technologies that enhance resilience, compliance and cost management.

Building Resilience for What Lies Ahead

Remember, as lucrative as it may seem to "put all of your eggs in one cloud," so to speak, no single platform, however advanced, can guarantee uninterrupted service. Rather than leaving sensitive data and mission-critical operations to chance, organizations should leverage infrastructure in which strategic workload placement, proactive security measures, and firm compliance standards reinforce one another. By combining the strengths of public offerings with the control and assurance of private systems, organizations ensure resilience now and in the future.

About the Author



Jerry Kaner is the Founder and CEO of Ciphertex Data Security. A trailblazer with over 30 years of experience in digital forensics and data security, Jerry's expertise and ultra-secure storage solutions have been trusted by the U.S. military, FBI, Interpol, and leading organizations worldwide. Jerry's innovative tools empower industries to protect critical data in high-stakes scenarios, from legal investigations to combat zones, solidifying his reputation as a leader in safeguarding the future of information security.

Learn more about Jerry's work at ciphertex.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Top Things Your Organization Needs to Know About Knowledge-Based Authentication Today

Discover how knowledge-based authentication can significantly strengthen digital security. Here we address types, benefits, limitations, and best practices for effective implementation at your organization

By Matt Cochran, COO, ID Dataweb

"Which street did you grow up on?"

We've all answered these kinds of questions countless times, often without giving them a second thought. These are examples of knowledge-based authentication (KBA) in action—a security measure that's growingly common in our digital interactions.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

In this article, we explore why KBA plays such a critical role in enhancing digital security. From its strengths and weaknesses to best practices for effective implementation, we dive into what makes KBA both a valuable tool and a potential vulnerability in our cybersecurity landscape.

If you're interested in how to bolster your organization's security measures—or just curious about those familiar questions we all answer—read on. Let's navigate the complexities of digital security together and share insights on making our online world safer.

KBA: Strengthening Digital Security Through Identity Verification

Every day, you hear about new cyber threats—phishing attacks targeting employees, data breaches exposing customer information, and hackers attempting to infiltrate your systems. With remote work becoming standard and digital transactions increasing, the challenge of protecting sensitive data intensifies. Verifying that individuals accessing your networks, whether workforce or customers, are who they claim to be, is critical to security.

This is where KBA comes into play. By leveraging personal information unique to each user, KBA adds a vital layer to your identity verification systems, helping to safeguard against unauthorized access.

This article dives deep into KBA, exploring its purpose, different types, strengths, limitations, and how it stacks up against other authentication methods. If you're a professional assessing security solutions, understanding the ins and outs of KBA can guide you toward stronger security measures and a better user experience.

What Should I know about KBA?

KBA verifies a user's identity based on something they know—specific information unique to them, similar to answering personal questions that ideally only you can answer. We've all likely encountered KBA when recovering a password, setting up a new online account, or during financial transactions. Often, it's a component of multi-factor authentication (MFA), serving as an additional security layer.

KBA operates on the principle of **"something you know"**, one of the three classic authentication factors, alongside **"something you have"** (like a security token) and **"something you are"** (PII data). Because KBA leverages personal knowledge, it provides a convenient way to verify identity without requiring physical devices or complex technologies.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

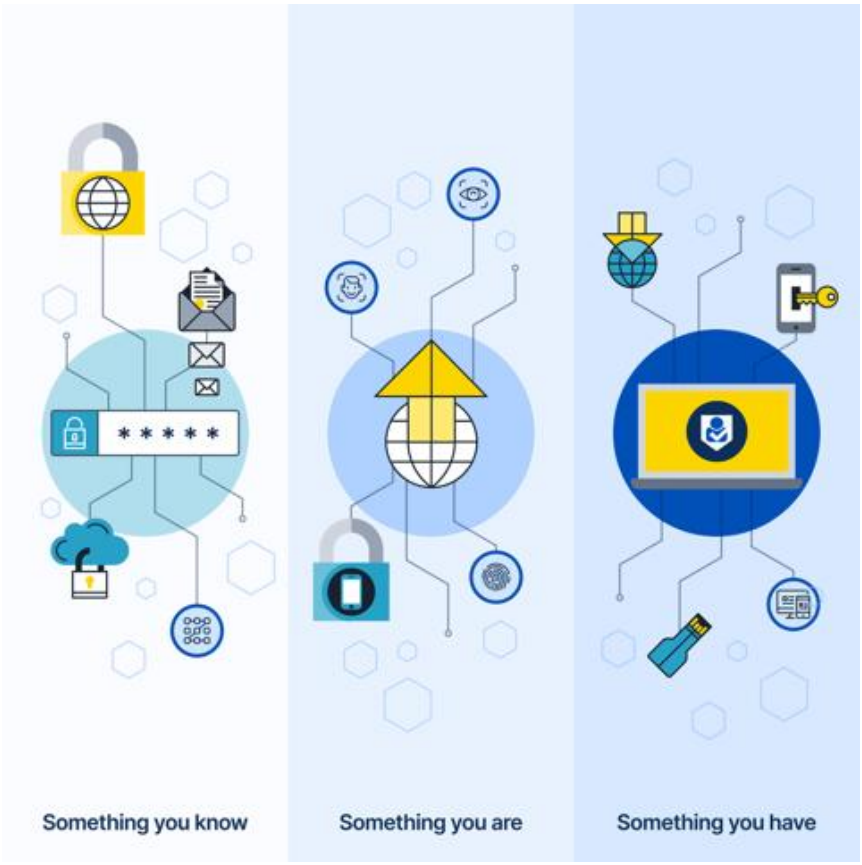


Image courtesy of ID Dataweb www.iddataweb.com

Static vs. Dynamic KBA

KBA comes in two common implementations:

- **Static KBA**: This involves pre-set questions like "What is your mother's maiden name?" or "In what city were you born?" Users select these questions and provide answers during account setup. While easy to implement, static KBA can be vulnerable if the personal information is accessible online or through social engineering.
- **Dynamic KBA**: This type generates questions in real-time, pulling from data sources like user behavior, credit reports, or public records. For example, you might be asked about a recent transaction or a previous address. Dynamic KBA is generally more secure but can be more complex and costly to implement due to the need for real-time data access and processing.

So Where Does KBA Fit In The Identity Verification Puzzle?

KBA is often integrated into MFA systems as a secondary layer. While some security methods rely on physical tokens or biometric data, KBA remains popular for its simplicity and accessibility. It doesn't

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

require special hardware or sensitive biometric information, making it particularly valuable in environments where quick and straightforward verification is essential.

For instance, in customer service scenarios, agents might use KBA to verify a caller's identity before discussing account details. In online banking, KBA can serve as an additional verification step during high-risk transactions.

Crafting Strong KBA Questions

The effectiveness of KBA hinges on the questions posed to users. The main trade-off is between security risk and keeping questions easy to remember for users. Well-thought-out questions minimize security risks.

Static questions

Static KBA questions are established during account creation. Examples include:

- **Common questions**: "What was the name of your first pet?" or "What is your favorite book?"
- **Personal history**: "What was the name of your elementary school?" or "What was your childhood phone number?"

While these questions are easy to remember, they can pose security risks. Answers might be easily discoverable through social media, public records, or even casual conversations. Moreover, users might forget the answers over time, especially if they haven't accessed the account in a while.

Dynamic questions

Dynamic KBA generates questions on the fly, based on real-time data:

- **Location-based questions**: "Which of these streets have you lived on?" or "In which city did you open your first bank account?"
- **Transaction-based questions**: "Which of the following was a recent purchase you made?" or "What was the amount of your last deposit?"

These questions are more unpredictable and tailored to the user, offering a stronger layer of security. Since the questions are generated from up-to-date information, it's much harder for an imposter to guess the answers.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

However, dynamic KBA requires access to reliable data sources and raises privacy considerations. Organizations must handle personal data responsibly and comply with regulations like GDPR or CCPA.

Crafting Effective Questions

An effective KBA question should be:

- **Unique but memorable**: It should be something only the user knows but can easily recall.
- **Not easily discoverable**: Avoid information that could be found on social media, public records, or through casual acquaintance.
- **Specific to the user**: Questions that are personal but not commonly shared.

For example, "What was the make and model of your first car?" is both specific and not easily guessed. It's important to strike a balance between security and usability; overly obscure questions might frustrate users, leading to account lockouts or increased support calls.

Despite the emergence of new authentication methods, KBA continues to have various strengths that make it a popular, still very relevant method.



Image courtesy of ID Dataweb www.iddataweb.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Security Advantages Of KBA

KBA can be something like a first line of defense in scenarios where deploying more advanced authentication methods isn't feasible due to cost, user accessibility, or technological constraints.

KBA is useful in low to medium-risk environments where robust verification is needed without burdening the user.

Convenience And Ease Of Access

One of KBA's biggest strengths is its accessibility. Users don't need any special devices, software, or prior setup beyond providing answers to security questions. This makes it user-friendly for people who may not be tech-savvy or who might have limited access to technology.

For example, elderly users or those in areas with limited technological infrastructure can still participate in secure transactions using KBA.

Versatility Across Industries

- **Financial services**: To prevent unauthorized access, verify identities before sensitive transactions, and fulfill KYC requirements. Dynamic KBA questions during service-desk calls are commonly seen here.
- **Healthcare**: Protecting patient data, especially with the rise of telehealth services where patients access medical records online.
- **Government services**: Ensuring that only eligible individuals access certain benefits, file taxes, or participate in government programs.

In each case, KBA provides a balance between security and user convenience, making it a practical choice for many organizations.

Weighing KBA Strengths And Weaknesses

Like any security method, KBA has its strengths and weaknesses. Understanding these can help determine if it's the right fit for your organization.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Strengths To Consider

- **User-friendly**: KBA is straightforward, requiring no additional hardware or complicated setup. Users are generally familiar with answering security questions.
- **Cost-effective**: It's less resource-intensive compared to biometric systems or physical tokens. Implementation costs are relatively low since they primarily involve software and database management.
- **Scalable**: Easily integrated into existing systems and scalable across various applications. Organizations can deploy KBA across multiple platforms without significant infrastructure changes.

Weaknesses to Be Aware Of

- **Information exposure**: Personal data used in KBA can sometimes be found online, making it vulnerable. Social media platforms and data breaches have increased the availability of personal information.
- **Susceptibility to phishing**: Attackers can trick users into revealing answers through deceptive emails or calls. For example, a phishing email might ask a user to "verify" their security question answers.
- **Privacy concerns**: Especially with dynamic KBA, using sensitive data can raise privacy issues. Users might be uncomfortable with organizations accessing certain personal information.
- **Not ideal for high-risk scenarios**: In situations requiring stringent security, KBA might not be sufficient. High-value transactions or access to sensitive data might necessitate stronger authentication methods.

Understanding these limitations is crucial for organizations to implement KBA effectively and mitigate associated risks.

Comparing KBA and Other Authentication Methods

To choose the best authentication strategy, it's essential to compare KBA with other available methods.

Multi-Factor Authentication (MFA) combines KBA with other verification methods like one-time passwords (OTPs), biometrics, or security tokens. This layered approach enhances security by requiring multiple forms of verification from different categories (something you know, have, and are).

For example, a user might need to enter their password (something they know), a code sent to their phone (something they have), and answer a KBA question. This makes it significantly harder for unauthorized users to gain access.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Biometric Authentication uses unique physical characteristics—fingerprints, facial recognition, iris scans—that are hard to replicate. While offering high security, it requires special hardware and can be costly to implement.

Biometrics are less prone to being forgotten or stolen compared to passwords or security questions. However, they raise concerns about privacy and data protection. If biometric data is compromised, it can't be changed like a password.

Behavioral Biometrics analyze user behavior, such as typing patterns, mouse movements, or navigation habits. It's still emerging but shows promise in detecting anomalies that could indicate unauthorized access.

This method operates passively, without requiring explicit actions from the user, enhancing security without impacting user experience. However, it requires sophisticated algorithms and can be resource-intensive.

Device-Based Authentication focuses on recognizing trusted devices. It uses device identifiers, geolocation, and other device-specific information to authenticate users.

This method reduces reliance on user memory or personal information. However, it assumes that the user's device is secure and hasn't been compromised.

Contextual Authentication involves passive analysis of the context of the login attempt—such as location, time of day, or network used. For example, if a user who typically logs in from New York suddenly tries to access the account from another country, the system might require additional verification.

When combined with KBA, contextual authentication can enhance security without compromising user experience. It allows for risk-based authentication, applying stricter measures only when something seems amiss.

Common Shortcomings When Implementing KBA…And Some Solutions

Avoiding common mistakes can make your KBA implementation more effective.

Using predictable questions

Steer clear of questions with answers that are easily found or guessed. Questions about pet names, birthdays, or favorite colors are often too generic and can be discovered through social media or casual conversations. I recommend crafting unique questions that are less likely to be publicly known.

Over-Reliance On Static KBA

Static questions become predictable over time. Attackers might collect enough information over time to answer these questions correctly. I recommend combining static and dynamic KBA or integrate additional security measures like MFA.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Neglecting To Update Questions

Personal information can change—people move, change names, or forget their previous answers. Not providing ways for users to update their security questions is a mistake. I recommend allowing users to review and update their KBA information periodically.

Ignoring Privacy Concerns

Using sensitive data without user consent can lead to trust issues and legal complications. I recommend being transparent about data usage, obtaining full consent, and complying with all relevant privacy regulations.

Complicating the user experience

A complex or cumbersome ID verification process can frustrate users, leading to abandonment or decreased satisfaction. I recommend balancing security needs with a smooth user experience by limiting the number of questions and ensuring they are user friendly.

7 Best Practices for Effectively Implementing KBA

Following best practices maximizes the benefits of KBA and enhances overall security for your organization.

1) Select Thoughtful Questions - Reduce the risk of unauthorized access and minimize user frustration, while making it harder for attackers to guess answers. Make sure the questions:

- **Are Unique and Memorable** - Choose questions that are significant to the user but not easily guessed.
- **Avoid common knowledge** - Steer clear of questions about information that might be publicly available.

2) Layer Your Organization's Security Measures - Layering security creates multiple barriers for attackers, significantly reducing the likelihood of unauthorized access. It addresses the weaknesses inherent in relying solely on KBA. Consider:

- **Combining KBA with MFA**: Use KBA alongside other authentication methods like OTPs, biometrics, or security tokens.
- **Risk-based authentication**: Implement stricter verification when the system detects unusual activity.

3) Keep It Dynamic - Dynamic KBA that adapts over time enhances security by making it difficult for attackers to prepare or preempt answers. It also accommodates changes in user behavior or information. I recommend:

- **Regularly updating questions**: Change dynamic questions frequently to prevent predictability.
- **Using real-time data**: Leverage up-to-date information for generating questions.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

4) Educate Your User Base - An informed user base is a crucial line of defense. Education reduces the risk of social engineering attacks and empowers users to participate actively in maintaining security. Recommendations include:

- **Awareness programs**: Inform users about the importance of keeping their personal information secure via newsletters, alerts, etc.
- **Phishing prevention**: Teach users how to recognize and avoid phishing attempts.
- **Guidance on selecting strong answers**: Encourage users to choose answers that are not easily guessed.

5) Regularly Review And Audit - Regular reviews help maintain the integrity of the KBA system. Audits can reveal weaknesses that need addressing, while compliance checks prevent legal issues.

- **Security audits**: Conduct periodic assessments to identify vulnerabilities in the KBA system.
- **Compliance checks**: Ensure that KBA practices align with legal and regulatory requirements.
- **Performance metrics**: Monitor the effectiveness of KBA by tracking incidents of unauthorized access or user complaints.

6) Prioritize The User Experience - A positive user experience encourages compliance with security measures. If the process is too burdensome, users may seek ways to bypass it, undermining security. I recommend:

- **Streamlining the process**: Limit the number of questions to what's necessary for security.
- **Providing support**: Offer assistance to users having trouble with KBA, such as help desks or alternative verification methods.
- **Ensuring accessibility**: Be sure the KBA process is accessible to users with disabilities.

7) Protect Data Privacy - Protecting user data builds trust and ensures compliance with privacy laws. It reduces the risk of data breaches that could compromise KBA answers. Recommendations include:

- **Data minimization**: Collect only the data necessary for KBA.
- **Secure storage**: Protect stored KBA data with encryption and access controls.
- **Transparency**: Clearly communicate how user data is collected, used and protected.

Is KBA Right for Your Organization? Five Considerations

Deciding whether to implement KBA? Here are your top considerations.

1) Assess Your Risk Level

Matching the security level to the risk ensures resources are used efficiently while maintaining appropriate protection.

- **Low to medium risk**: KBA may suffice for basic account access or low-value transactions.
- **High risk**: For sensitive data or high-value transactions, additional authentication methods are advisable.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

2) Know Your User Base

An authentication method that aligns with user capabilities enhances adoption and effectiveness.

- **Demographics**: Consider the age, technical proficiency, and preferences of your users.
- **Accessibility needs**: Ensure the authentication method is usable by all segments of your user base.

3) Compliance Matters

Compliance is not optional. Using an authentication method that doesn't meet regulatory standards can result in penalties and legal issues.

- **Regulatory requirements**: Determine if KBA meets industry-specific regulations like HIPAA, PCI DSS, or GDPR.
- **Audit trails**: Ensure the system can provide necessary documentation for compliance purposes.

4) Evaluate Resources

Adequate resources ensure the KBA system is reliable and secure. Underestimating the requirements can lead to system failures or security breaches.

- **Technical infrastructure**: Assess whether your systems can support KBA implementation and maintenance.
- **Data management**: Consider the capabilities for securely handling the data required for KBA.

5) Cost-benefit analysis

A thorough cost-benefit analysis ensures that the chosen authentication method is economically viable and aligns with organizational goals.

- **Implementation costs**: Calculate the expenses involved in setting up KBA.
- **Potential risks**: Weigh the costs against the potential losses from security breaches.
- **ROI considerations**: Evaluate whether KBA will provide a return on investment through reduced fraud or increased user trust.

KBA remains a modern, highly valuable tool in the realm of digital security. Its ease of use and accessibility make it an attractive option for many organizations. However, it's essential to recognize KBA's limitations while ensuring its thoughtful implementation.

By following best practices—selecting effective questions, layering security measures, keeping user experience in mind, and regularly updating your system—you can enhance your organization's security posture.

As cyber threats become more sophisticated—from advanced phishing schemes to complex social engineering tactics—organizations face the constant challenge of protecting their digital assets.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

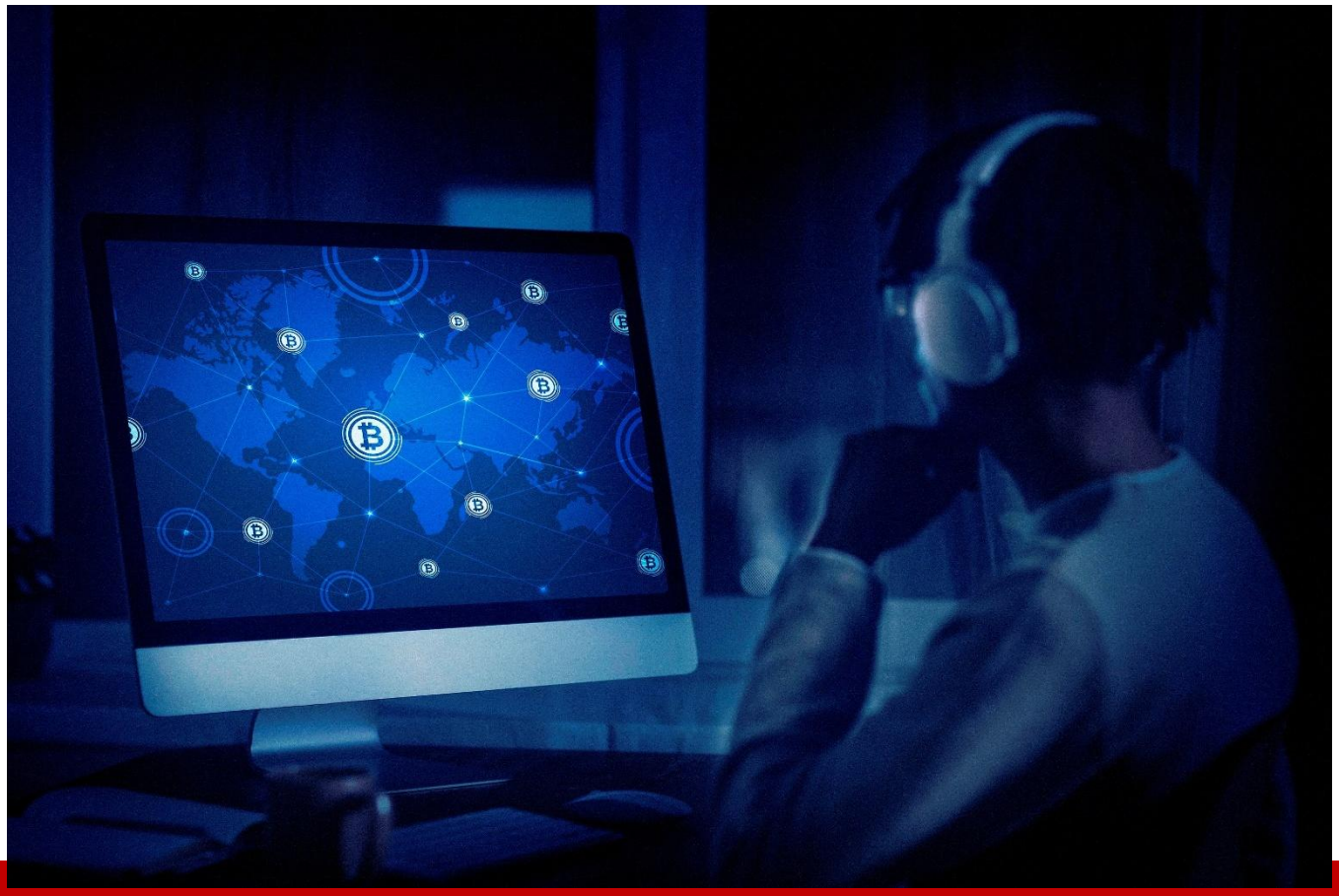
KBA isn't a silver bullet for all security issues, but when thoughtfully implemented, it serves as a valuable component in a multi-layered defense strategy. By integrating KBA into your organization's security protocols, you enhance protection against unauthorized access, safeguard sensitive information, and provide peace of mind for your organization, your users, and even external partners.

About the Author



Matt Cochran is the COO of the **ID Dataweb**. He is an enterprise IT expert with experience leading strategy, architecture and design of internet-scale, cloud-based identity management systems. His responsibilities with **ID Dataweb**, provider of digital trust to leading enterprises in more than 170 countries, include leadership of the product and solutions roadmap, and he enjoys working daily with customers, industry partners and standards groups. Matt lives in Richmond, VA. Prior to ID Dataweb, Matt was part of the Corporate Enterprise Architecture team at General Electric, where led strategic initiatives including the introduction of a cloud-based customer identity management solution, and the modernization of GE's legacy identity systems to support current standards. He can be reached online at matt.cochran@iddataweb.com, and at our company website iddataweb.com.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



SMB Cybersecurity Trends That Matter for 2025

By Dor Eisner, CEO and Co-Founder of Guardz

Small and medium businesses (SMBs) are a pillar of the global economy – driving innovation, creating jobs, and enriching communities.

They're also an increasingly viable target for cyber threats.

To fend off increasingly sophisticated cyberattacks, SMBs today must embrace innovations such as AI-powered unified detection and response, user-centric cybersecurity, cyber insurance products, and enlisting the help of Managed Service Providers (MSPs). These future-forward solutions that safeguard operations and enable SMBs to focus on growth will bolster their resilience and success in an increasingly complex digital landscape.

Here is what SMBs should keep in mind as they approach their cybersecurity in 2025.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Evolving Threat Landscape

SMBs were once deemed low-value targets for hackers. Cybercriminals would employ low-effort, high-return "spray-and-pray" tactics to target these vulnerable businesses at high volume. SMBs have since learned that their small size does not eliminate their appeal as a target for hackers, and they've begun to adopt more secure cybersecurity solutions.

Unfortunately, so too have cyberattacks on SMBs grown rapidly in scale and sophistication.

Even as SMBs recognize the true threat posed by hackers, a gap still remains between the perceived and actual security of many organizations. A worrying 44% of SMBs believe their current antivirus solution fully protects their business, employees, and data — a false sense of security that leaves them even more exposed to modern threats.

SMBs also face constraints that larger enterprises can more easily overcome – limited budgets, small-to-nonexistent IT teams, and less robust infrastructure. This resource gap, paired with misconceptions about their security, makes SMBs easy targets for attackers and underscores the need for security solutions tailored to SMBs' unique needs.

Recognizing that current tools may fall short is the first step toward building a more resilient security posture.

AI Redefining Detection & Response for SMBs

AI is poised to be the biggest driver of change for SMB cybersecurity in 2025, particularly through its ability to empower unified detection and response platforms. These AI-integrated platforms streamline and centralize cybersecurity operations, making cybersecurity management significantly easier for SMBs and the MSPs that serve them.

Decentralized solutions are a hurdle for SMBs, who struggle to address the deluge of alerts and remediation needs coming from so many different directions – indeed, 77% of SMBs use between 4 – 10 different cybersecurity point solutions.

By automating and unifying threat response processes across security tools and providing user-centric insights, unified detection and response enables better, faster, predictive incident response defense strategies. This cohesive approach helps SMBs to address sophisticated cyber threats without being hampered by resource constraints.

It is AI's unique ability to analyze vast amounts of data quickly and accurately that enables these platforms to identify anomalies, predict potential threats, and automate responses. For example, an AI algorithm can catch a threat-portending alert faster than a human analyst and neutralize the attack before it causes any damage.

Unified detection and response offers SMBs enterprise-level protection that is still tailored to smaller size and operational complexity.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

User-Centric Insights

User-centric detection & response will be crucial for SMBs.

Even for MSPs tasked to handle security for myriad SMBs, fragmented solutions and alert fatigue hinder their ability to protect clients effectively – 47% of MSPs are overwhelmed by the large volumes of security data.

A user-centric approach shifts the focus from systems-based protection to safeguarding individual user behaviors and interactions. By examining the big picture of user patterns and habits, automating threat detection, and unifying security tools into a seamless system, SMBs can achieve enterprise-level defense without overwhelming their limited resources. Integrating this simplified approach to threat management enables SMBs to address digital risks while positioning themselves for sustainable growth.

Cyber Insurance

A key trend to watch in 2025 is the growing adoption of cyber insurance in SMB's cybersecurity strategies.

Traditionally seen as a safety net for post-attack recovery, modern policies now offer proactive risk management services, supporting SMBs with incident response planning, vulnerability assessments, and employee training. These services help elevate SMBs security posture even amid limited resources and manpower.

It is important to note that SMBs shouldn't rely solely on insurance or allow it to make them complacent. Rather, cyber insurance should be part of a balanced cybersecurity approach that combines an array of preventive measures to ensure resilience and preparedness.

MSPs

In 2025, the role of MSPs will expand even further as they continue adopting the cutting-edge technologies needed to provide cybersecurity tailored to SMBs.

MSPs can offer SMBs access to advanced tools such as unified detection and response platforms, threat intelligence feeds, and 24/7 monitoring, as well as bringing expertise in compliance with GDPR, CCPA, or industry-specific standards. Beyond mere technical support, MSPs can also end up serving as SMBs trusted advisors, offering strategic guidance on long-term security planning.

As third-party service providers whose sole focus is cybersecurity, MSPs can offer the focus and dedicated threat management that SMBs can't always handle on their own, including threat monitoring, risk management, and insurance coverage. By combining these elements, MSPs reduce the burden on SMBs, allowing them to focus on what matters most – running and growing their business.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

…And a Cyber-Safe New Year!

It is undeniable that SMBs will face a rising tide of cybersecurity challenges in 2025 – but these hurdles are not insurmountable. With cutting-edge solutions proliferating on the market and strategic partnerships with MSPs more viable than ever, SMBs can turn cybersecurity from a daunting task into a strategic advantage.

Cybersecurity is an ongoing journey, and SMBs must remain proactive, adaptive, and informed. By staying ahead of the trends and leveraging the innovations of 2025, SMBs can build a resilient foundation for their future success.

About the Author



Dor Eisner is the CEO and Co-Founder of Guardz, working to create a safer digital world for SMBs. Dor has over 20 years of experience in the field of cybersecurity. Prior to founding Guardz, Dor worked at IntSights, a Rapid7 company, as their VP of Business Development, as well as at Alarum Technologies as Director of Sales. Dor began his career in cybersecurity in the IDF's 8200 Unit as Cyber Security Team Lead. Dor can be reached online at https://www.linkedin.com/in/dor-eisner-17067744/ and at our company website https://guardz.com/ .

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Unmasking Employment Fraud

The popularity of remote and hybrid work has created fertile grounds for a rise in employment fraud.

By Ryan LaSalle, CEO, Nisos

The popularity of remote and hybrid work has redefined the workplace, offering flexibility and accessibility to companies and employees alike. That said, this evolution has not come without some hidden vulnerabilities that have created fertile ground for a rise in employment fraud.

From individuals seeking financial gain to nation-state actors with more nefarious intentions, the remote employment model has opened new avenues for fraudulent activities. For businesses unaware of or unprepared for these risks, the consequences can be devastating - with data breaches, financial losses, reputational damage, and insider threats all possible outcomes.

There are some less devastating outcomes as well - such as underperformance, or low employee productivity from splitting time across more than one full-time job. In some positions there are contractual exposures to client data or non-compete clauses that could be violated due to fraud, or legal liabilities to worry about if third parties become involved who are not under the employer's umbrella of protection.

Understanding the threat of employment fraud and developing strategies to identify and prevent it is fast becoming a critical capability for security teams.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Faces of Fraud

Employment fraud is not one-size-fits-all. It can take several forms, each driven by their own set of motivations and presenting a unique set of risks:

1. **Identity Fraud**: The simplest type of employment fraud is identity fraud. By creating a false identity, applicants conceal their true qualifications or backgrounds, often because they don't really have the skills they profess to (such as an advanced degree or a specific software certification), or because they're looking to evade legal issues (i.e., a criminal record, or live in a country under sanctions). Some applicants have more qualified friends stand in for them during an interview, so they can pass a skills assessment and secure a job they're not qualified for.
2. **Outsourcing or Polywork Fraud**: Alongside the increase in remote work has been an increase in employees either outsourcing their workloads to a gig worker or freelancer, or employees holding several full-time jobs at the same time, with none of their employers aware of the situation. Essentially these employees are breaching the workplace policies of several companies, while still collecting full salaries. This not only undermines workplace trust but can also lead to subpar work quality and confidentiality risks.
3. **Criminal Organization or Nation-State Fraud**: These actors target companies to infiltrate systems, bypass sanctions, or launder money. Recent cases, such as North Korean operatives securing remote IT roles, underscore the sophistication of these schemes. Their motivations often include economic disruption, the ability to gain access to systems for data theft or hacking, or even simply for financial gain to support broader political or criminal agendas.

Spotting the Warning Signs

Employment fraud doesn't just appear out of nowhere, however. There are several warning signs to be aware of - and identifying fraud early can save organizations from significant harm. Some warning signs can be identified before an employee is hired, while some only become evident afterwards. While any one of these signs may not say with certainty that there is fraud at work, identifying them should push internal teams to take a deeper look at the employee in question. If several red flags are present, then it may be time to take action.

Pre-Hire Warning Signs:

- **Inconsistencies in Information**: Multiple profiles with similar photos or discrepancies in employment history are all telltale signs. Fraudsters also often create barebones professional profiles with no personal content or history, which can also indicate a fabricated persona.
- **Suspicious References**: Employment references that evade video calls or provide vague, generic feedback may be in on the fraud. Additionally, some references may appear overly rehearsed - or fail to provide any concrete examples or contextual information about past performance. In some cases, applicants have been known to serve as their own employment reference.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Post-Hire Warning Signs:

- **Discrepancies in Skill Sets**: This red flag is easy to identify. Fraudulent employees often list advanced technical skills in their resumes, only for it to quickly become apparent post-hire that they are unable to do what they claimed. This mismatch often becomes evident during the first few weeks on the job. For some employees, having a low level of engagement with corporate tools, data or systems can stand out, especially when it is unlike the rest of their peer group.
- **Information Changes:** Frequent address changes after hiring, or a sudden address change just before the delivery or a work phone or laptop could indicate fraudulent activity, as could a request to send payment to a different address. Sometimes the inability to answer a simple question about their location such as "how is the weather?" can be a warning sign.
- **Technical Issues:** Other warning signs to look out for include the existence of remote access software on their computers, the employee never turning on video or never being seen on video very clearly, or difficulties in their availability for calls or meetings. The use of foreign IP addresses, VPN usage, the installation of mouse jiggler software, or the laptop's physical location being inconsistent with the employee's claimed location can be indicators of fraud.

How Companies Can Defend Themselves

In addition to being vigilant when it comes to recognizing potential red flags, there are several strategies that employers can adopt to help fortify their defenses and weed out any fraud before it becomes impactful. While there may be legitimate reasons for an employee to have moved several times recently, or to be careful about what personal information is shared publicly, these strategies can help ensure you're only finding false alarms and not ignoring real fraud.

1. **Enhanced Applicant Screening**: Organizations should try to require on-camera or in-person interviews to confirm the applicant's identity. For remote positions, ensure video interviews are conducted with clear, verifiable visual checks. Utilize tools to detect emerging threats like deepfake technology, ensuring candidates genuinely match their submitted documentation.
2. **Thorough Documentation Checks**: Where feasible, conduct in-person verification of identity documents. In remote setups, implement secure digital verification methods and cross-reference applicant-provided information with public records to ensure consistency. Ask questions if there are discrepancies; simply asking may scare a real fraudster off.
3. **Comprehensive Reference Checks**: Reference checks were mentioned as a red flag - but it's worth mentioning here as well. Ask for references, don't take no for an answer, and then verify them through direct, detailed conversations. Ensure their legitimacy and connection to the applicant by asking targeted questions about specific projects, responsibilities, and work contexts. Consider independent verification of references through background-check services as well.
4. **Secure Onboarding Practices**: A natural follow-on to stronger application controls is to keep the same level of heightened awareness when it comes to onboarding. Require in-person onboarding or robust virtual identity verification before granting access to company systems or equipment. Virtual verification can include live document presentation and biometric authentication. Monitor for last-minute address changes and verify new addresses with trusted sources.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

5. **Leverage Open Source Intelligence (OSINT)**: If you fear there may be fraud at hand, conduct deep dives into applicants' online presence to confirm consistency in professional history and personal details. Look for anomalies such as identical photos used for multiple profiles or sudden bursts of activity on professional platforms.
6. **Collaborative Investigation Efforts**: Above all, ensure that your organization's HR, legal, and security teams are working together to address any fraud concerns, pooling their expertise for a thorough assessment. Cross-department collaboration can identify patterns or inconsistencies that might otherwise go unnoticed.

Stopping Employment Fraud

The dangers of employment fraud extend far beyond false resumes. Once inside an organization, fraudsters can access sensitive systems and data, posing significant insider threat risks. These vulnerabilities can ripple through partner networks, amplifying the potential damage. A single compromised hire can lead to significant breaches that affect customer trust, financial stability, and industry standing.

Organizations that assume they are too small or secure to be targeted may find themselves caught off guard. Small businesses, often without dedicated security, HR or legal teams, are particularly vulnerable, as fraudsters may see them as easier targets.

Remote work is here to stay, and with it, the need for vigilant and adaptive strategies to combat fraud. Employers must continually refine their processes, integrating technology and collaboration across departments to stay ahead of emerging fraud strategies.

About the Author



Ryan LaSalle is the CEO of Nisos. He leads a mission-driven team who helps clients use the power of open-source intelligence to unmask the digital threats and identify the real-world people seeking to do them harm. Ryan served as the North America Lead for Accenture Security, nurturing the talented teams that bring transformative solutions to better defend and protect clients. During more than 25 years with Accenture, Ryan led client engagements across commercial, non-profit and the public sector by integrating emerging technologies into advanced solutions to drive agility and meet business needs. He holds patents in human resource management, knowledge discovery and establishing trust between entities online. Ryan is a frequent speaker at international security conferences and has authored numerous articles on cybersecurity. He holds a Bachelor of Science degree in electrical engineering from Princeton University and lives in Alexandria, VA with his wife Melissa, their two kids, and pandemic puppy. Ryan can be reached online at info@nisos.com and at our company website https://www.nisos.com/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Walk Through the DDoS Fire

AI Models for Improved Network Security

By Alex Pavlovic, Director of Product Marketing, Nokia Deepfield

For many years, the distributed denial-of-service (DDoS) threat landscape revolved around reflection/amplification attacks launched by malicious players hiding behind spoofed IP addresses. Around 2020, it all changed. The proliferation of IoT devices, many of which were insecure, coupled with the growing availability of gigabit (and even multi-gigabit) bandwidth, led to a wave of botnet-driven attacks. Things changed again in 2024 when we saw novel attacks featuring more automation, likely driven by increased usage of artificial intelligence (AI).

These automated DDoS attacks have placed an unprecedented burden on digital service providers across the internet ecosystem. From traditional communications service providers (CSPs) to cloud and internet exchange providers (IXPs), webscale companies and content delivery networks (CDNs), everyone is feeling the effects.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

It's not just the volume and sophistication of DDoS attacks that have risen sharply. The attacks are also happening much more frequently. Many service providers now see hundreds of significant security events in their networks every day. There's a lot of "shapeshifting" happening, too. Attacks can be much shorter, focus on single or multiple targets, and use different attack vectors over time in a manner that can only be attributed to automation, likely facilitated by AI.

Fighting AI with AI

Many view AI and its sibling, machine learning (ML), as promising technologies for network security and improved network defense. More and more service providers are fighting AI with AI in an asymmetrical game that requires them to counter cheap and easy DDoS attacks with costly DDoS defense systems.

When it comes to DDoS and network security, AI can deliver many benefits, from easier, error-free configuration to improved operational agility through capabilities such as automated security information and event management (SIEM), or endpoint and extended detection and response (EDR/XDR).

For DDoS security, AI and ML are likely to bring their key benefits in faster, more accurate detection and scalable yet granular mitigation. These capabilities will protect network services and ensure uninterrupted connectivity for end users and customers.

Which AI is best suited for DDoS security?

Generative AI (GenAI) and large language models (LLMs) are great for applications where the vast knowledge residing in large data sets can create new, derived and generated content. For network security, including DDoS security, GenAI is well suited for configuration, reporting, incident correlation and problem resolution. Many security products and solutions already use GenAI for these purposes.

AI enables some of the notable GenAI use cases in SIEM or EDR/XDR products, focusing on improved incident analysis and response. For example, GenAI can quickly sift through logs and forensic data to pinpoint the root cause of a security incident. On the other hand, it can help service providers improve their operational agility by creating detailed incident response playbooks tailored to specific threats.

Predictive AI technology uses data analysis to identify patterns, anticipate trends and behaviors, and forecast and predict upcoming events. As such, predictive AI is an excellent choice for automating DDoS detection and mitigation to address the demands of a dynamic and evolving threat landscape. It can help service providers stay a step ahead of malicious actors by analyzing and correlating historical data on real-time DDoS security events and incidents, with a promise to excel at quick and accurate identification of DDoS patterns and trends and swift mitigation of emerging threats. For DDoS security, the most compelling capabilities of predictive AI include:

- **Trend and pattern recognition**: Fast, accurate identification of potential threats based on anomalies in traffic behavior, unusual traffic flows or new types of DDoS attacks detected globally.
- **Automated mitigation**: Surgical removal or blocking of malicious traffic in real time with minimal impact on legitimate network traffic.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- **Dynamic security policy adjustments**: On-the-fly generation or adaptation of security policies and mitigation strategies to respond to evolving or changing threats.

It is worth noting that many of the tasks presented to predictive AI technology can be achieved with sophisticated ML implementations, where super-fast processing of data in an "if-this-then-that" manner can yield significant benefits and improve both DDoS detection and mitigation.

AI models are what they eat

Data is the lifeblood of AI, and this is also true when it comes to implementing AI for DDoS security. Today, these implementations are largely done by DDoS security vendors and anti-DDoS service providers that have in-house AI tools.

A key requirement for using AI models for network security is *explainability*. In network security, it is imperative to be able to trace back and explain every decision. In other words, networking and security professionals must be able to answer questions like, "Why was this traffic flow flagged as DDoS?" and "Why was this mitigation strategy chosen to neutralize this DDoS attack?"

Access to high-quality DDoS-related data is critical for ensuring explainability and training AI models to do their jobs reliably. Super-large, highly relevant and highly confident data sets about DDoS events are must-haves. Relying on insufficient or misrepresented data sets can lead to invalid results and "house-of-cards" failures.

DDoS detection accuracy can be greatly improved by complementing DDoS-related knowledge related to a specific network with data about the larger internet security context, including common threats and repeat offenders. This knowledge often comes from third-party sources that collect and maintain information about common threats across a much larger attack surface. There are several industry initiatives aimed at obtaining and sharing this information; some focus on sharing among consortiums of service providers, while others focus on sharing via a national agency or a regulator or obtaining the wider security context directly from a vendor that may maintain a much larger knowledge base, sometimes with a global context. These augmented data sets can provide a highly effective foundation for training predictive AI models for DDoS detection.

Once we have good data, the next challenge is to train AI models. While the knowledge base and DDoS security-related data sets may not be as vast as those used to train well-known GenAI models, they are dynamic and growing. With each new attack and threat, the data sets for a predictive AI model present more information that can be used to distinguish good traffic from DDoS traffic in real time.

It's important to emphasize that the human factor is still indispensable for making important decisions about DDoS detection. Highly experienced security professionals help to optimize and improve AI models so the models will better "understand" what constitutes a DDoS attack, especially for novel attacks (such as the NoName067(16) attacks that have affected many service providers in 2024). These domain experts play an essential role by identifying important contextual factors and providing insights about how patterns may shift over time. Vendors and service providers still need the humans-in-the-loop approach to enhance the real-world applicability of AI models for DDoS detection.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

DDoS mitigation has a different set of requirements for AI. Here, we are concerned with using AI to *optimize the mitigation strategy* to remove as much malicious traffic as possible while minimizing the impact on legitimate traffic with an *optimal or minimal set of network resources*. The input for AI-optimized mitigation must consider the composition of a particular DDoS attack, which may encompass many concurrent attack vectors, as well as the network's actual DDoS mitigation capabilities and limitations.

Figure 1 shows how an AI-optimized set of 1,609 filter entries mitigated a complex DDoS attack composed of many concurrent vectors, with over 100,000 source IP addresses and 256 target addresses.

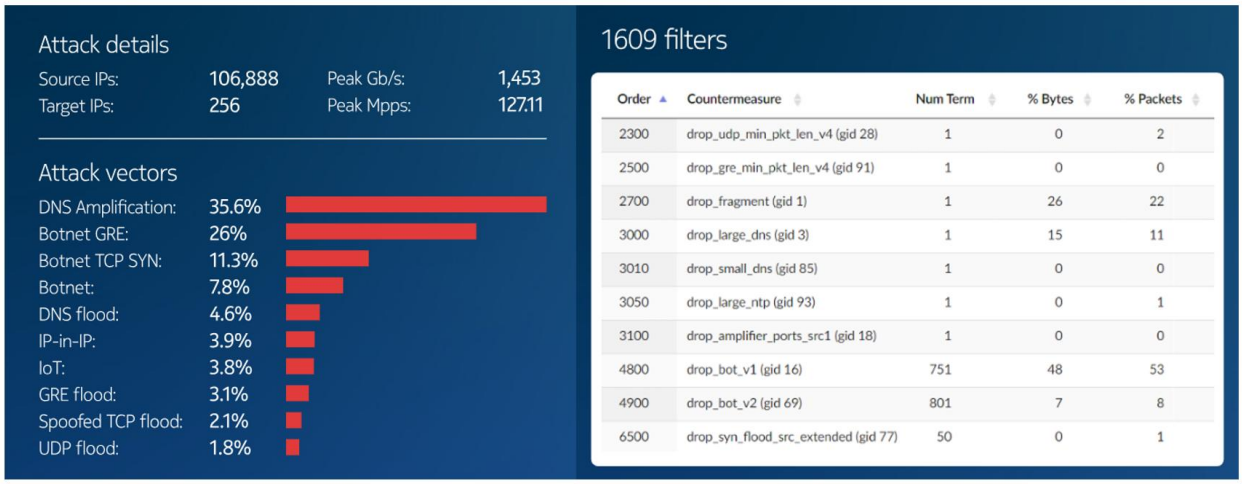


Figure 1: Mitigation of a large DDoS attack using an AI-optimized set of filters

Walking through the fire

The true proof of the effectiveness of an AI model for DDoS security lies in its ability to quickly identify a threat or attack and trigger agile and granular removal of the DDoS traffic by a mitigation system. As Charles Bukowski wrote, "What matters most is how well you walk through the fire."

While it is vendors who (most often) perform model training and fine-tuning, evaluation of the performance and effectiveness of a DDoS security solution is predominantly left to service providers. This is a challenging endeavor because many DDoS solution vendors offer unique ML algorithms, novel advanced countermeasures, specialized hardware and other capabilities that are technically challenging for service providers to evaluate.

In an industry filled with claims and counterclaims, the best way to determine and benchmark the value of a DDoS mitigation solution is to consider three key metrics:

1. Mitigation speed and performance (including false positive and false negative ratios)
2. Scalability
3. Cost

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Of course, the central metric for any DDoS solution is its ability to filter DDoS traffic. The key concern, however, is not whether 100% of DDoS traffic will be mitigated. A solution that blocks *all* network traffic will block *all* DDoS traffic and *all* legitimate traffic.

We need a mitigation solution that is both fast and selective.

Speed of mitigation has quickly become one of the most important metrics. This is sometimes expressed as "time to drop first (DDoS) byte," but with the emergence of fast-changing, short-lived DDoS attacks, the emphasis has switched to how long it takes to mitigate the entire attack. Modern DDoS security solutions need to complete full detection and mitigation in well under one minute.

For selectiveness of mitigation, the important metric is the false positive rate—how much of the legitimate traffic was dropped. Historically, high false positive rates of 10% and even more have been tolerated and accepted, which translates to a lot of good network traffic wrongly identified as DDoS and removed. With AI technology coming to the rescue, we should demand and expect more: predictive AI models should be able to achieve much improved false positive rates—below 1% for basic amplification/reflection and under 5% for most vectors.

Similarly, the false negative rate is a metric that describes the percentage of traffic that was *not* identified as DDoS and, therefore, passed along as good traffic. However, this is harder to track because some emerging threats need time and repetition to be properly identified as attacks. You need to be aware of all threats, including those you missed.

Scalability and cost are somewhat interrelated. An effective AI-enabled DDoS solution needs to scale to terabit levels even though the network may not encounter that volume of traffic today. This scalability must be achieved at a fraction of the cost of legacy, non-AI-based DDoS mitigation systems, which sometimes range to thousands of dollars per Gb/s of protected/mitigated traffic.

What can we do better?

With the increasing size and complexity of the DDoS threat landscape, service providers are not alone in seeking better DDoS security. It is a shared responsibility and concern for all participants in the global internet service delivery chain—from domains where applications, content and services are created through intermediaries such as IXPs and CDNs to service providers and their end users and customers.

Here are three things we can all do to improve overall DDoS and network security.

First, sharing intelligence is a key element of the fight against DDoS attacks. If we all share more insights about attackers and their methods, we will be better equipped to defend ourselves. For predictive AI systems, it's essential to share and use relevant and confident data that includes all important contextual features (e.g., time, geo-location, IP packet parameters) while observing privacy and complying with frameworks such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Second, continuous monitoring of AI models' performance for DDoS detection and mitigation of novel threats and attacks is essential. This tracking will indicate when and how AI models may need to be updated or retrained or when new data sources and features need to be added.

Third, our industry needs to work on standardizing benchmarking and performance measurement of DDoS security solutions. Maybe it's time to follow the good and decades-old network engineering practices established for interoperability and implementation testing of new networking features and protocols and do something similar for DDoS and network security. While it is a much more sensitive area than generic networking, imagine a public DDoS hackathon that evaluates the performance of anti-DDoS solutions in a round-robin or may-the-best-one-win approach.

In a time when automation and AI are everywhere and are increasingly deployed by malicious actors to bring networks down, we must embrace these technologies to improve network defenses, too. What matters most is how well we walk through the DDoS and network security fire, and this is a fire we must fight and walk through together.

About the Author



Alex Pavlovic is Director of Product Marketing at Nokia. Alex has spent over 25 years in the telecom industry in many environments: academia, regulatory, consulting, and Tier-1 hardware and software telecom vendors. Currently, Alex is a Director of Product Marketing at Nokia, focusing on the Nokia Deepfield portfolio of applications for network intelligence, analytics and DDoS security.

Alex can be reached online at LinkedIn, and at our company website nokia.com/deepfield.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Federal Government's Treatment of Government Contractors' Emerging Technologies – Including Chat Interfaces and Code Generator

By Tenley A. Carp, Partner, Arnall Golden Gregory LLP

The federal government's cybersecurity treatment of "chat interfaces," "code generators," and other emerging technologies is evolving, as these technologies introduce unique challenges related to privacy, security, and compliance for federal government agencies. The certification process for such emerging technologies depends on the specific framework under which the technology will be used. These frameworks include the Federal Risk and Authorization Management Program ("FedRAMP"), a government program that standardizes the security of cloud services used by the federal government; the Cybersecurity Maturity Model Certification ("CMMC"), a program that evaluates the ability of organizations to protect sensitive data for the Department of Defense ("DoD"); or agency-specific guidelines.

Emerging technologies like chat interfaces (e.g., artificial intelligence ("AI")-powered tools) and code generators are classified based on their risk and impact. These tools must address potential vulnerabilities, such as data leakage, unauthorized access, and misuse. The federal government will assess risk under the framework of the National Institute of Standards and Technology ("NIST")

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

guidelines, especially NIST SP 800-53 (for security controls) or NIST SP 800-171 (for protecting controlled unclassified information).

The federal government's key challenges include:

- **Privacy Risks:** If these emerging technologies process sensitive or personal information, federal agencies must ensure compliance with regulations like the Federal Information Security Modernization Act ("FISMA") and applicable privacy standards.
- **AI/Machine Learning ("ML") Security:** Chat interfaces and AI-powered systems require transparency and accountability for decision-making processes. The AI Risk Management Framework (AI RMF) developed by NIST provides specific guidance.
- **Supply Chain Risks:** If the emerging technology relies on third-party tools or libraries, it must demonstrate supply chain integrity under frameworks like CMMC, discussed above.

FedRAMP for Cloud-Based Emerging Technologies Certification Guidelines and Submission Process

Technologies offered as cloud-based services must undergo FedRAMP certification if used by federal agencies.

Steps

1. **Categorize Service:** Determine the impact level (low, moderate, high).
2. **Documentation:** Prepare a System Security Plan (SSP) and other required documentation.
3. **Audit:** Engage a Third-Party Assessment Organization (3PAO) for a security assessment.
4. **Submission:** Submit assessment reports to the Joint Authorization Board (JAB) or a federal agency for review.

NOTE: The JAB, composed of representatives from the DoD, the Department of Homeland Security (DHS), and the General Services Administration (GSA), reviews the security package and grants a Provisional Authority to Operate. This path is more rigorous and suitable for cloud services widely used across the government.

5. **Authorization:** Obtain either a Provisional Authorization to Operate (P-ATO) or an Agency Authorization to Operate (ATO).

Timing

The timing for FedRAMP approval depends on the type of authorization path selected and the complexity of the system being assessed. Thus, submission to a federal agency that is acting as a sponsor to complete the FedRAMP authorization process or a cloud service provider with a FedRAMP complaint security package using a 3PAO to validate its implementation will typically take six to 12 months, whereas submission to the JAB typically takes 12 to 18 months. FedRAMP approval might also take longer if the systems require higher levels of security or if there are "resource constraints" (such as a limited availability

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

of agency sponsors, JAB reviewers, or 3PAO capacity). Therefore, these timeframes are averages and it could take longer to obtain FedRAMP approval than the estimates listed here.

CMMC for Defense-Related Technologies Certification Guidelines and Submission Process

The DoD plans to include CMMC requirements in contracts starting in mid-2025, with a phased rollout extending into 2028. For tools handling Controlled Unclassified Information (CUI) within the Department of Defense ecosystem, the CMMC process requires hiring a Certified Third-Party Assessment Organization (C3PAO) for evaluation. The CMMC is a framework established by the DoD to enhance cybersecurity practices within the Defense Industrial Base.

Process and Timeline to Obtain CMMC Authorization

1. **Preparation Phase:**
    - **Assessment of Current Practices:** Evaluate existing cybersecurity measures against the required CMMC level.
    - **Implementation of Controls:** Address any gaps by implementing necessary security controls.
    - **Documentation:** Develop comprehensive policies, procedures, and system security plans.

2. **Assessment Phase:**
    - **Third-Party Assessment:** Engage a C3PAO to conduct a formal evaluation.
    - **Remediation:** Address any identified deficiencies and update documentation accordingly.

3. **Certification Phase:**
    - **Submission:** Provide assessment results to the DoD for review.
    - **Approval:** Await official certification, which is valid for three years.

Timing

The preparation phase is typically six to 18 months, depending on organizational size and current cybersecurity posture. The assessment phase is typically two to four months for Level 1 and 10 to 18 months for Level 2, though this can vary based on organizational complexity. The Certification Phase depends on DoD's review and approval process. Thus, the total estimate time for CMMC approval is six to 12 months or more.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Conclusion

The federal government's evolving approach to government contractors' emerging technologies, including chat interfaces and code generators, highlights both the immense potential and the complex challenges these innovations bring to the defense and broader public sectors. As technologies like artificial intelligence, machine learning, and automation continue to shape the landscape, contractors are faced with navigating a regulatory environment that seeks to ensure security, ethical standards, and compliance with federal requirements.

For contractors, this presents a dual challenge: the need to innovate and leverage new technologies for operational efficiency, while also meeting stringent cybersecurity and regulatory demands, such as those outlined in frameworks like FedRAMP and CMMC. The government's increasing reliance on these technologies requires contractors to maintain a delicate balance between technological advancement and the protection of sensitive data.

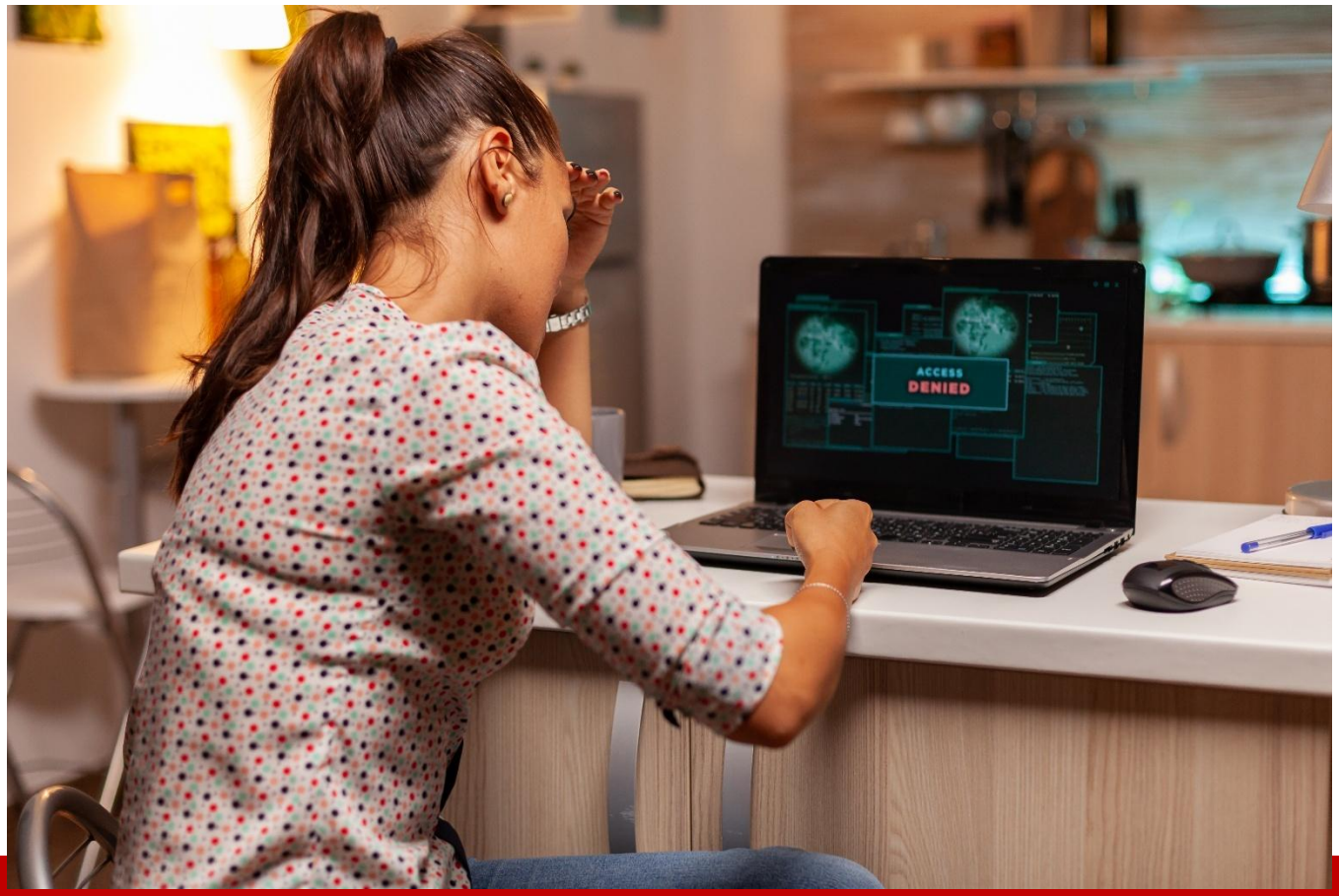
As these technologies become integrated into federal contracts starting in 2025, it will be crucial for contractors to stay ahead of regulatory changes, invest in robust cybersecurity practices, and proactively engage with evolving compliance standards. While the federal government's treatment of emerging technologies presents challenges, it also offers contractors the opportunity to be at the forefront of innovation. By aligning technological advancements with security and regulatory requirements, contractors can not only contribute to the nation's defense and technological advancement but also secure a competitive edge in the rapidly evolving market.

About the Author

Tenley A. Carp is a partner at Arnall Golden Gregory LLP and the chair of the firm's Government Contracts practice. She can be reached at tenley.carp@agg.com.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



AI In Cybersecurity: The Risks and Rewards

By Michael Baker, VP and Global CISO, DXC Technology

AI's role in cybersecurity is paradoxical: a tool for both attackers and defenders. The same capabilities that make AI a powerful ally in the fight against cybercrime can also be exploited by malicious actors to develop more sophisticated and targeted attacks.

AI as a tool for cybercriminals

As AI systems become increasingly sophisticated and pervasive, cybercriminals are harnessing its power to launch more sophisticated and targeted attacks.

For example, phishing emails have evolved from basic deceptive messages to highly sophisticated attacks that are increasingly difficult to detect and significantly more dangerous. Today, 40% of phishing emails targeting businesses are generated using AI, according to VIPRE Security Group."

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Attackers are also successful at using methods like deepfakes — a form of AI that can be used to create convincing hoax images, sounds and videos — to perpetrate fraud or manipulate an audience into action.

And AI's adaptive nature is one of its most potent features in social engineering attacks, which manipulate people into giving away sensitive information or compromising security through company email but increasingly through other modes like text messages and social media.

By using AI in these attacks, cybercriminals can appear more credible and trustworthy, leading more victims to fall for fraud attempts or manipulation, which could lead to system compromise and data loss.

Empowering defenders at the speed of AI

At its heart, AI recognizes patterns and abnormalities in massive datasets — that is why it is such an important component of modern cybersecurity.

For example, AI enhances threat detection through advanced pattern recognition and anomaly detection. Unlike traditional methods, AI can analyze vast amounts of data in real-time, identifying threats that might be missed by human analysts. This leads to faster incident response times and reduces the window of opportunity for cybercriminals to take advantage of a compromise.

AI also enables predictive analytics, allowing businesses to anticipate and mitigate potential threats before they materialize. By analyzing historical data and identifying trends, AI systems can provide insights into future attack vectors, enabling proactive defense strategies before a human analyst even gets involved.

For example, DXC is working with Microsoft product teams to help shape Microsoft Security Copilot: a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes. Today 44% of organizations can confidently identify ways AI could strengthen their security systems, according to the Ponemon Institute.

AI as a force multiplier

As organizations confront the complexities of escalating cyber threats, they need people with the right skills to protect their data and systems.

The good news is AI can work as a force multiplier for smaller security teams, which gives organizations a better chance against the newest vectors of cyber risk.

This is not meant to replace valuable and scarce expertise, but rather augment it by using AI to support overtaxed security analysts, identity management professionals and incident responders who need to sort through an increasing amount of information to do their jobs.

Today 50% of organizations say they’re using AI to compensate for a cybersecurity skills gap, according to the Ponemon Institute.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

For example, the integration of AI in security operations centers automates repetitive and time-consuming tasks. AI can handle routine monitoring, data analysis, and initial incident responses, freeing up human analysts to focus on more complex issues and higher-value tasks.

This not only increases efficiency but also improves the accuracy, reliability, and velocity of security operations.

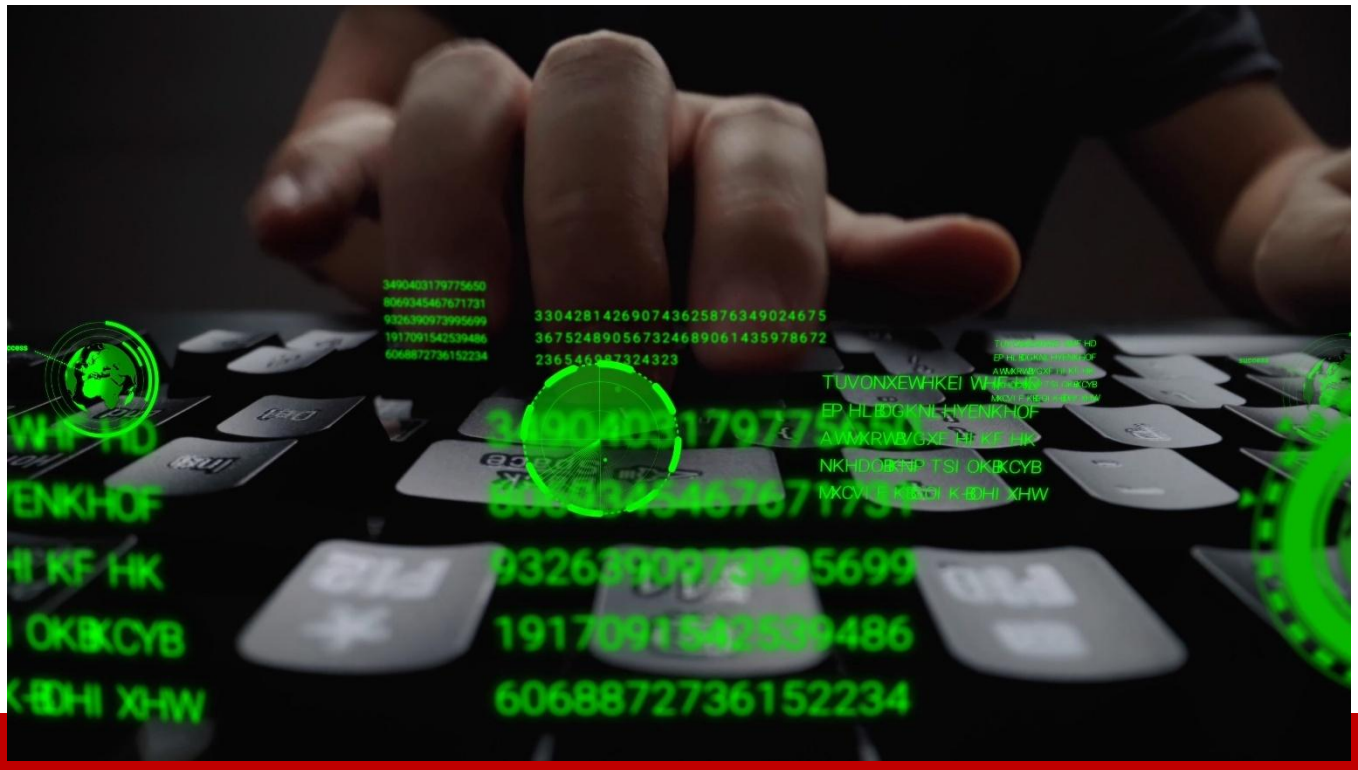
About the Author



Michael Baker currently serves as Vice President & IT Chief Information Security Officer for DXC Technology. An accomplished cyber security executive, Baker brings over 20 years of experience in the field across cyber leadership, talent development, risk management, audit, and compliance serving the aerospace and defense industry as CISO along with a variety of clients across industries as a seasoned consultant. As CISO, he manages a team of professionals across internal cyber operations, network defense, policy, awareness, incident response, threat intelligence, secure architecture, and reputational protection. Baker is also a current member of the Cybersecurity Maturity Model Certification Accreditation Body Industry Advisory Group (CMMC-AB IAG).

Michael Baker can be reached at https://www.linkedin.com/in/michaelebaker/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Securing SMBs in 2025

Key Cyber Threats and Strategies to Stay Ahead

By George Skaff, SVP & General Manager, Cybersecurity SMB, OpenText

In 2024, cybersecurity attacks made headlines. From the massive SaltTyphoon telecommunications breach to BlackCat ransomware group shutting down Change Healthcare's systems, no industry left 2024 unscathed.

While these high-profile attacks will continue to make headlines this year, small to medium businesses (SMBs) also face an uptick in cyberattacks, but with far less resources. In fact, OpenText Cybersecurity's 2024 Global Ransomware Survey found that 76% of SMB respondents experienced a ransomware attack within the last year, outpacing the rate of attacks reported by larger enterprises.

This year, increasingly sophisticated technology including AI will require businesses to rethink their security strategies to address intricate, highly complex threats and adopt a more integrated approach to protecting their digital environments.

Below are three critical trends in the year ahead — and the steps they can take to stay ahead of the curve – that businesses need to be aware of.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

1. AI-Powered Threats – and Solutions – Will Reshape SMB Cybersecurity Strategies

2024 saw an AI boom, and 2025 will deliver on the promises made by both vendors and bad actors around AI in cybersecurity. Businesses will be increasingly targeted by AI-augmented attacks, including highly adaptive malware and phishing campaigns that evolve in real time to bypass traditional defenses.

The Financial Times recently reported that corporate executives are being hit by highly personalized, sophisticated phishing scams, likely powered by AI to enhance attack precision and effectiveness. With over 90% of successful cyberattacks stemming from phishing emails, businesses will expand their defenses past traditional methods like endpoint security and standard email filters, which will no longer suffice against these advanced threats.

To counter AI-augmented attacks, businesses will adopt AI-powered security solutions that provide continuous, automated protection and response capabilities. For example, employing AI-powered managed detection and response (MDR) solutions will provide organizations with continuous threat hunting and monitoring, allowing them to identify attacks in real time, reducing vulnerability to modern threats and preventing damage and breaches.

2. Ransomware and Supply Chain Attacks Converge to Put the Pressure on SMBs

Ransomware remains a leading threat to all organizations, with tactics evolving in both severity and frequency. With businesses often viewed as low-hanging fruit due to limited budget and security resources, they will continue to be a prime target of ransomware in 2025. To maximize impact, ransomware attackers will utilize “breadth attacks,” prioritizing scale over sophistication by casting a wide net across smaller targets with limited defenses.

The OpenText Ransomware Survey also highlighted growing alarm over ransomware attacks targeting software supply chains, with 91% of organizations expressing concern about attacks on a company’s downstream software supply chain, third-party and connected partners. This trend is particularly pressing for SMBs, which often rely on a small network of managed service providers and third-party platforms, making them more vulnerable to supply chain threats than their larger counterparts.

To defend against these dual threats, businesses will need to think critically about their defenses, assessing vendors more closely for risk, adopting zero-trust principles and streamlining their security stacks to reduce exposure.

3. Zero-Trust and Proactive Defense Move from a Nice-to-Have to a Must-Have

As SMBs adapt to evolving threats in 2025, zero-trust frameworks will no longer be just aspirational, but essential. Businesses will increasingly implement zero-trust principles to reduce vulnerabilities and significantly minimize the impact of attacks and breaches.

A simple, cost-effective approach to building a strong zero-trust foundation starts with securing identities through multi-factor authentication (MFA) and role-based access controls, ensuring only verified users

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

and compliant devices can access resources. From there, businesses should ensure endpoint protection with antivirus and device management tools, segment their networks to limit potential breaches and use tools to detect and respond to threats.

As we move into 2025, SMBs must prioritize a layered defense strategy to navigate an increasingly complex cybersecurity landscape. By pairing foundational frameworks like zero-trust with technologies like AI-driven monitoring, detection and response, even resource-constrained businesses will create a more holistic and resilient security posture.

For many, partnering with a managed security service provider (MSSP) can greatly help in scaling solutions needed to manage modern challenges. Through strategic partnerships and a multi-layered approach, businesses can confidently safeguard their digital environments against evolving threats.

About the Author



George Skaff is SVP & General Manager, Cybersecurity SMB at OpenText, where he leads a worldwide go to market group that strives to deliver competitive cybersecurity solutions for the SMB market globally. George is also the General Manager for the Cybersecurity Consumer business.

Most recently, he was SVP of Marketing for Daon, a company focus on market leading identity verification and biometric authentication solutions for various verticals.

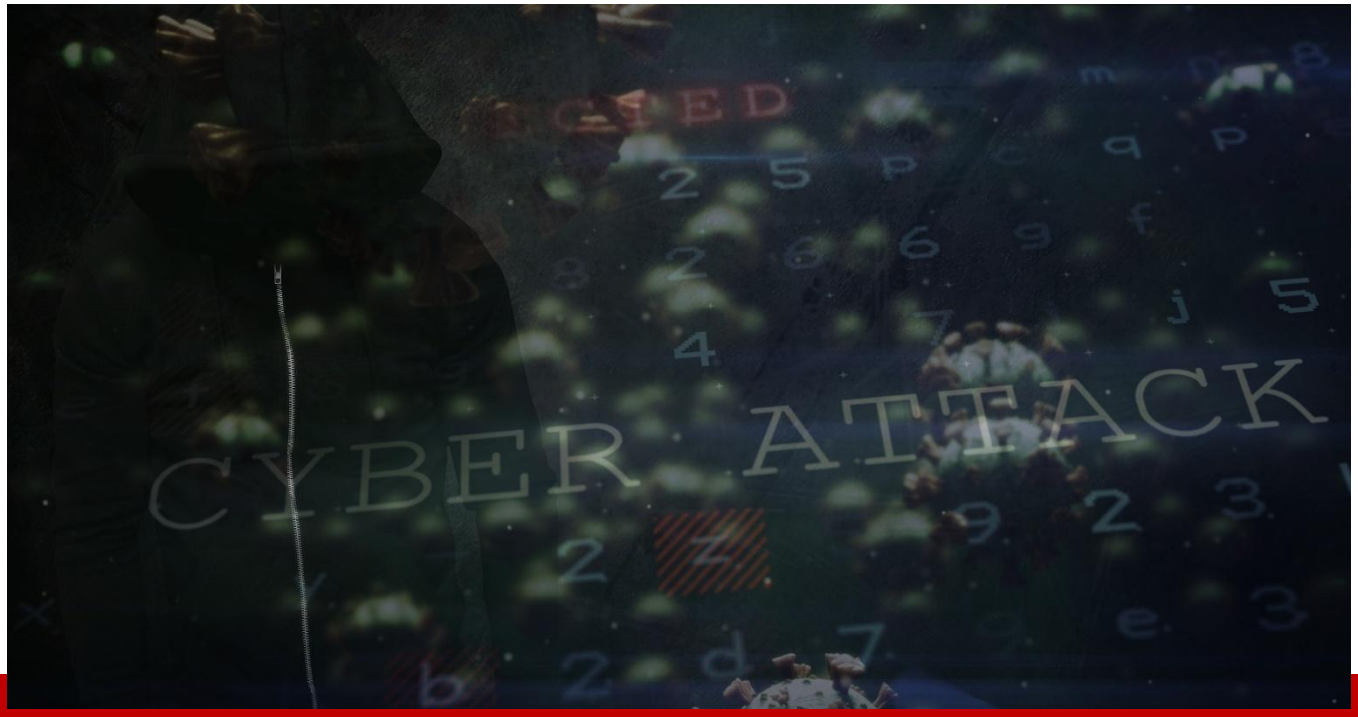
Before that he was the General Manager of the Digital Line of Business at Nuance Communications. Prior to that role, he served as the Head of WW Marketing at Nuance Enterprise Division, which included the security and biometrics business.

George has more than 30 years of experience at both publicly and privately held companies, primarily in the SaaS space. He has held various senior positions at global companies including SGI (acquired by HP), Wyse (acquired by Dell), NEC computers and Logitech.

George speaks three languages fluently and has lived and worked in many international time zones. He enjoys the outdoors whenever he can, whether he is hiking, golfing or playing pickleball.

George Skaff can be reached at https://www.linkedin.com/in/gskaff/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Cryptography: The Unsung Hero Fighting Cyber Threats from The Background

By Carlos Aguilar Melchor, Chief Scientist – Cybersecurity, SandboxAQ

With the rise of mobile and cloud computing across the globe, our attitude towards cybersecurity has undergone a major change. Organizations are finally beginning to understand how important it really is to be in control of their cybersecurity. As cyber threats evolve at a rapid pace, organizations must prioritize preventing all manners of cyber horrors, not only the most evident ones.

Indeed, the threats that are not easily seen can be the most dangerous to organizations. Cybersecurity measures like firewalls, endpoint security, identity access management (IAM) tools, and others are nowhere near foolproof in a world in which cyberthreat actors have jumped lightyears ahead. And our greatest countermeasure is one that is rarely spoken about. Stealthy and silent, cryptography is the unsung defender that is protecting us against the evolving threat landscape.

Cryptographic Capabilities

Cryptography offers effective defense against the most common threats we face today. By encrypting sensitive files, and properly protecting the associated encryption keys, we take a huge step towards preventing attackers from gaining access to our crown jewels. If we encrypt to the highest industry

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

standard, we ensure that even attackers that exfiltrate personal, payment, or IP data will not be able to use that information. So, cryptography mitigates the risk of extortion in ransomware campaigns.

Cryptography, with robust key-management policies, can also protect against advanced persistent threats (APTs). Indeed, key-management policies ensure key rotation and guide employees on best practices when generating and issuing keys. Practices like these lay the groundwork for more secure authentication and authorization because they enable time-limited and granular access to resources and data. This practice protects services, data at rest, and data in transit, all of which are key in the context of APTs.

But as with all great tools, cryptography must be used properly to effect positive results. Despite its many benefits, encryption and authentication mechanisms remain largely overlooked by allies. This oversight has led to fragmented and poorly managed, or not managed at all, cryptographic ecosystems, and most global organizations today would likely be unaware of the precise state of their cryptographic assets. This leads to regular outages, high governance and risk mitigation costs, and a state of vulnerability in an area where most organizations consider themselves secure. Many business executives believe encryption to be a straightforward, box-ticking exercise and are not aware of the spectrum of quality that pertains to it, nor of the associated direct and indirect losses resulting from low quality approaches.

Leverage it Effectively

Any plan must begin with a status audit. How does the organization use cryptography? What keys are live and in service, how are they secured, and how are they allocated? Care must be taken to specify the frequency of key rotation and to understand, in detail, the potential business impacts of compromise for every key in service. And when vulnerabilities are discovered, what then? A plan of action is required for such discoveries. The same scrutiny must apply to vulnerabilities in cryptographic libraries, to urgent key rollovers, and to the cryptographic algorithms that underpin it all.

Continuous and (partially) automated auditing is thus key. However, it can lead to significant technical debt that some enterprises may struggle to manage effectively. Implementing cryptographic agility can help reduce this burden by allowing systems to adapt to new cryptographic standards, or repair issues, more easily and cost-effectively. My colleagues and I think of it as the ability to effectively manage risk related to the changing needs of cryptographic systems. Gartner tells us that crypto-agility plays a major role in defending against a fluctuating threat landscape. In 2017, the analyst firm said those organizations with an established crypto-agility plan would suffer 60% fewer breaches that could be tied back to encryption failures. So, there is a measurable incentive to get it right.

Every enterprise wants to be technologically agile. This must also apply to our most silent sentinels. While giant, wooden horses may be a thing of the past, crypto-agility can protect us from the thousands of would-be infiltrators that try to tunnel into our digital estates daily. If we take it seriously.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Carlos Aguilar Melchor is Chief Scientist, Cybersecurity at SandboxAQ, a B2B company delivering AI solutions that address some of the world's great challenges. Carlos has been working within the Post-Quantum Cryptography (PQC) domain as an academic for 20 years across numerous universities, including the very prestigious Institut Supérieur de l'Aéronautique et de l'Espace (ISAE-SUPAERO). He was also a consultant for 10 years, working for companies such as Airbus and supporting two of the teams present in the third round of NIST's PQC standardization. He is the co-inventor of a patent covering many of the existing PQC key exchanges, and the author of nearly 100 publications cited more than two thousand times. Carlos can be reached online at LinkedIn and at SandboxAQ.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Table-Stakes In 2025: Threat Intelligence Management to Counter Emerging Challenges

Collective Defense – the Immediate Sharing of Actionable Insights – Builds Resilience, Allows Proactive Mitigation of Risks Before They Become Realized.

By Jawahar Sivasankaran, President, Cyware

The cybersecurity landscape is evolving at an unprecedented rate. New tools, techniques, and technologies are transforming the way attackers attack and defenders defend, bringing forth new threats that will plague organizations throughout 2025 and beyond.

As look forward, there's no better time to consider some of these threats and the strategies that will help protect against them. Making informed predictions is a core part of the proactive strategies essential to addressing emerging threats and threat intelligence has a great role to play in 2025.

Cybersecurity Predictions for The Road Ahead

Although no one has the magic ball and we cannot predict with full certainty, there is a strong likelihood of the following happening in 2025.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Proliferation of AI-Driven Cyber Attacks

AI-driven cyber-attacks are set to escalate in 2025, transforming the scale and sophistication of malicious activities. Phishing campaigns powered by generative AI will create flawless, personalized emails that adapt in real-time to bypass security measures. Adaptive malware, enhanced by AI, will learn and evolve, making detection increasingly difficult.

Generative AI enables even small cybercriminal groups to launch large-scale, highly targeted attacks without advanced technical skills. By automating processes, adversaries can tap into the vastly distributed world of cybersecurity tools and technologies, democratizing cybercrime and increasing its reach.

As AI integrates deeper into daily life, risks extend beyond direct attacks. Employees inadvertently sharing sensitive data with AI platforms like ChatGPT already pose significant threats. Organizations must adopt robust controls to balance AI's benefits with privacy concerns, ensuring data protection against accidental exposure while staying vigilant against evolving AI-powered threats.

Continued Sophistication of Social Engineering Attacks and Exploitation of Social Media

In 2025, cybercriminals will increasingly exploit the convergence of social media and generative AI to carry out highly sophisticated social engineering attacks. Platforms like LinkedIn, where users expect legitimate professional connections, will continue to be fertile ground for impersonation. AI-powered tools will craft convincing personas, enabling attackers to pose as employees, executives, or trusted partners, breaching corporate defenses with ease.

Deepfakes and AI bots will further amplify these threats by mimicking voices, appearances, and behaviors in real-time, blurring the lines between genuine interactions and forgery. Imagine participating in a video conference call, only to realize later it was an AI-generated deception. These technologies will disrupt not just individual users but also financial transactions, corporate decision-making, and brand reputations.

Organizations must evolve their security measures, integrating advanced tools and adopting zero-trust principles. Employee training will also be critical to navigating this new environment where every interaction demands scrutiny and skepticism.

Escalation of Supply Chain Attacks

By 2025, security attacks targeting supply chains will reach unprecedented levels of sophistication, with AI and automation enabling rapid, targeted attacks. These advanced techniques can allow ransomware to spread swiftly across interconnected networks, making early detection and mitigation critical. As a result, supply chain attacks are projected to escalate, with large-scale incidents expected to disrupt industries globally.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The reliance on critical vendors magnifies the cascading effects of such attacks, pushing businesses to adopt cyber insurance and governments to enforce stricter regulatory standards. Organizations must prioritize compliance, enhance phishing defenses, and train employees to counter increasingly convincing AI-driven impersonations and attacks.

Regulatory Changes Will Impact Cybersecurity Practices

As the regulatory landscape grows increasingly stringent, with frameworks like NIS2 demanding a greater focus on cybersecurity, organizations will be forced to direct more time, resources, and money toward their cybersecurity strategies. While these regulations are intended to strengthen security postures, they also add layers of operational complexity, forcing businesses to dedicate more focus and effort to meeting these standards.

The Importance of Effective Threat Intelligence and Collective Defense in 2025

Effective threat intelligence and collective defense are vital in 2025 to address the evolving cyber threats. Sharing actionable insights enhances resilience, enabling organizations to anticipate and mitigate risks before they evolve into impactful incidents. A collaborative approach strengthens defenses across interconnected ecosystems, ensuring compliance and safeguarding businesses against increasingly sophisticated adversaries.

Adopting a Deeper View of the Risk Environment

Ensuring security in 2025 relies on understanding risks beyond corporate borders, including those impacting your supply chain and third-party partners. Leveraging tools such as Cyware's Collaborate (CSAP) - which includes vulnerability advisory sharing, threat assessment surveys, action assignment, and security collaboration capabilities – will grant you a panoramic view of your risk environment that also gives you the deeper intelligence perspective to protect customers from third-party risks.

The Role of Threat Intelligence in Proactive Defense

As threats evolve and attackers grow more sophisticated, timely and actionable cyber threat intelligence will play an increasingly important role in protecting organizations. This intelligence is crucial for anticipating and mitigating threats to your business, helping you establish a deep understanding of individual threat actor profiles and the broader cybersecurity threat landscape.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Building Resilience Through Collective Defense

While competing organizations are often reluctant to work with each other, when it comes to cybersecurity, we really are stronger together. Taking part in collective defense efforts – such as by joining sector-specific Information Sharing and Analysis Centers (ISACs) and operational collaboration frameworks that leverage public-private partnerships – grants you greater visibility into the threats your business faces, allowing for more efficient and effective threat intelligence management and response.

Ensuring Compliance with Regulations like NIS2

Regulations like the NIS2 Directive and DORA explicitly mandate that organizations operating in critical sectors of the EU share threat intelligence and collaborate on security measures. While meeting these requirements will require time, resources, and finances, it's important not to view these regulations as an operational obstacle. These requirements aren't designed to punish organizations; they exist to ensure cybersecurity resiliency. Non-compliance can be damaging, but the consequences of a successful attack are often far worse.

Looking Ahead

Although 2025 is set to be a particularly tough year for cybersecurity, with supply chain attacks escalating, AI supercharging attack techniques, and bolstered regulations burdening compliance teams, these challenges are not insurmountable.

By implementing threat intelligence management and collective defense strategies, organizations of all shapes and sizes can take the fight to threat actors and prepare themselves for the year ahead.

You need an approach that connects data across your organization, automates incident response, and facilitates real-time collaboration so you can respond to threats before they cause any damage. To learn more about gaining a holistic approach to cybersecurity that integrates threat intelligence, security orchestration, and automation, feel free to reach out to me and my colleagues.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Jawahar Sivasankaran currently serves as the President of Cyware, leader in Cyber Threat Intelligence space. He has served an Operating Advisor with leading Private Equity and Consulting firms, focused on due diligence and portfolio operations and is active in the early-stage startup community as investor and advisor.

His previous operating leadership role was with Appgate, where he served as the President and COO, leading all Go to Market functions including Sales, Marketing and Customer Success. He previously led Global Security Specialization Sales for Splunk and spent 15+ years at Cisco in various leadership roles, including leading global Sales & Business Development through Managed Security Providers, Strategic Partners, and Global Alliances.

Jawahar can be reached on X at @CywareCo and at our company website https://www.cyware.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Why Your Security Tools May Be Leaving You Exposed

By Martin Greenfield, CEO of Quod Orbis

As the cyber landscape continues to shapeshift at speed, there is a concerning disconnect between security capabilities and confidence levels that could be leaving many enterprises exposed.

This is happening at a time when the stakes are getting higher. For example, financial institutions are currently preparing for the EU's Digital Operational Resilience Act (DORA). This regulation mandates robust ICT risk management and comprehensive security monitoring – yet many organisations are relying on a patchwork of tools that may leave them exposed to increasingly sophisticated attack methods like AI deep fakes and spearphishing.

But this challenge extends far beyond finance; every sector faces mounting pressure to demonstrate both security effectiveness and regulatory compliance.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Our latest data shows that organisations have accumulated an average of 19 security solutions per team – however, 41% still report a lack of technology as their biggest challenge in maintaining a robust security posture.

This disconnect points to a deeper problem. In short, there needs to be greater acknowledgement that strong cybersecurity is not about having more tools, but having the right ones.

Most concerning is that while 93% of IT decision-makers feel confident they have the necessary tools to maintain visibility across their infrastructure, 95% admit they haven't been able to easily access specific digital assets in the last year. This false confidence is creating dangerous blind spots that leave organisations vulnerable to both security breaches and compliance failures.

Understanding the challenge

The modern enterprise infrastructure has become a labyrinth of critical assets, connections and endpoints. To offer some perspective, the average IT team now manages 31 endpoints per person across their organisation. In a 1,000-person company, that's over 30,000 devices requiring constant monitoring and protection. This complexity is compounded by the rapid adoption of cloud services, hybrid working models and an expanding array of connected devices.

The larger the organisation, the bigger the issue. According to our data, companies with more than 1,250 employees show the least confidence in their existing tools (88%) and struggle the most with accessing critical assets (97%). These larger enterprises often grapple with a mix of legacy, bespoke and modern systems, resulting in the lowest visibility rates (79%) compared to smaller businesses.

The disparity in confidence levels between technical and compliance teams is especially telling. While 94% of information security directors express confidence in their system visibility, only 66% of compliance directors share that optimism. This gap highlights a critical misalignment between technical capabilities and compliance requirements – a gap that could prove costly as regulatory frameworks become more demanding.

Breaking the reactive cycle

The traditional approach of rapidly investing in new security solutions whenever new threats emerge has created an unwieldy tech stack that generates more problems than it solves.

Organisations are trapped in a reactive cycle. Almost four in 10 firms (39%) report a lack of actionable data despite their numerous tools, while 37% cite budget constraints as a major challenge. This reactionary stance not only strains resources but also creates dangerous gaps in security coverage.

System monitoring tools are emerging as potential solutions to these challenges. Continuous monitoring tools create cohesion amongst teams pulling all disparate tools into a single view point. By providing real-time visibility and assessment of security measures, these tools allow teams to proactively identify and remediate control failures before they escalate into security incidents. Given that 82% of organisations

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

agree that greater visibility over digital assets would significantly improve their security posture, it is an approach well worth adopting.

It's promising that 72% of IT teams have had their IT budget increased in the past three years, but businesses need to break free from the typical cycle of throwing money at a problem and hoping something sticks. At the same time, teams will have to battle boards over more tooling and convince them they are not plugging gaps but increasing their visibility.

Indeed, businesses are suffering from a blind spot that's leaving them exposed. Misplaced confidence in existing security tools means these businesses are susceptible to data breaches and non-compliance fallout with potentially crippling financial and reputational consequences. The disconnect between confidence and tangible output signifies a need for a paradigm shift.

Moving forward

However, such a shift requires not just new tools, but a fundamental change in how we approach security monitoring and compliance.

For security teams, the benefits are clear. Our research shows that 38% believe automation will accelerate document creation, while 37% see it improving board pack preparation and 36% anticipate more time for strategic security assessments. More importantly, 35% expect reduced human error and enhanced data accuracy. The time saved through automation – up to 60 hours annually per team member on board reporting alone – can be redirected toward strategic security initiatives.

As regulatory requirements continue to evolve across industries, including the upcoming DORA regulation, organisations can't afford to maintain the status quo. The gap between perceived and actual security capabilities represents a significant risk, one that could lead to both security breaches and compliance failures.

The message is clear. It is time for businesses to move beyond the false confidence in their swollen security stack and focus on achieving genuine visibility and control across their entire infrastructure.

About the Author

Martin Greenfield is the CEO of Continuous Controls Monitoring solutions provider, Quod Orbis. He has over two decades in the cyber security space. With his team, Martin helps deliver complete cyber controls visibility for our clients via a single pane of glass, through Quod Orbis' Continuous Controls Monitoring (CCM) platform. Their clients can see and understand their security and risk posture in real time, which in turn drives their risk investment decisions at the enterprise level.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Top Five Most Alarming Cybersecurity Trends Revealed - And What Your Business Should Be Doing About Them In 2025

Cowbell's Latest Cyber Roundup Report for 2024 Explores the Year's Most Alarming Cybersecurity Trends, Offering Business Leaders Actionable Steps to Mitigate Cyber Risk

By Rajeev Gupta, Co-Founder at Cowbell

As we approach the end of another year, one thing is for certain; the cybersecurity landscape has evolved yet again. Looking back on 2024, businesses have faced a rapidly shifting threat environment - one where we've seen the rise of advanced technologies, increasingly complex supply chains, and the widespread adoption of cloud infrastructure. All of which has contributed to an expanded attack surface, exposing organizations to more frequent and severe cyber threats than ever before.

Our recently published Cyber Roundup Report 2024 offers an in-depth analysis of these threats, which draws on data from over 46 million small and medium-sized enterprises (SMEs) across the U.S., U.K., and Japan.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Let's start by delving into some of the most pressing cybersecurity trends the data uncovered before we look at what proactive steps businesses should be taking in light of these trends:

1. Supply Chain Attacks Up 431%

Between 2021 and 2023, we found that supply chain attacks surged by a staggering 431%, with further growth projected by 2025. These attacks are effective because they exploit the trust between interconnected organizations and their vendors or suppliers, and can potentially compromise multiple entities simultaneously through one weak link. The dramatic rise can be attributed to a number of factors, including:

- Increased digitization and interconnectivity of business operations.
- Growing complexity of supply chains, making them harder to secure.
- The potential for high-value targets through a single point of entry.
- The challenge of maintaining visibility and control over third-party security practices.

2. Manufacturing faces escalating cyber risks

In terms of identifying the most vulnerable sectors, we found manufacturing came top, with cyber risk scores 11.7% below the global average. Cyber incidents in this sector are not only 1.6 times more frequent but also 1.2 times more severe compared to other industries. These statistics can be attributed to:

- A heavy reliance on automation and interconnected devices.
- Legacy systems and bespoke software that may lack modern security features.
- High sensitivity of data, including intellectual property and design plans.
- Increasing digitization of manufacturing processes without corresponding security measures.
- Complex supply chains that introduce potential points of vulnerability.

3. Ransomware targets public administration and education

Public administration and educational services continue to face heightened cyber exposure, with a more dangerous threat landscape than the global average. The report also highlighted a 70% increase in ransomware attacks on educational institutions in the last year and 20-40% higher severity of claims than average. Factors contributing to this include:

- Budget constraints, which can often lead to outdated IT infrastructure and security measures.
- Large user bases with varying levels of cybersecurity awareness.
- Valuable personal and research data that attracts cybercriminals.
- The critical nature of services, increasing pressure to pay ransoms in case of attacks.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

4. Larger Businesses See 2.5X More Cyber Incidents

Enterprises with annual revenues exceeding $50 million experience cyber incidents 2.5 times more frequently than smaller organizations. While these companies may have more resources to invest in cybersecurity, their size and complexity introduce new vulnerabilities, specifically:

• Larger companies present a more attractive target due to their valuable data assets.

• Complex IT infrastructures in larger organizations create more potential entry points for attackers.

• Higher public profile of larger companies can make them targets for reputation-damaging attacks.

However, smaller businesses are not immune. While they may face a lower frequency of attacks overall, they remain at risk due to supply chain vulnerabilities and limited cybersecurity resources. What's more, the consequences of a single incident can be devastating for a small SME, with severe financial losses, downtime, business interruption, and, in some cases, closure, all on the line.

5. Critical technologies present the greatest risks

Operating systems, content management tools, virtualization technologies, server-side technologies, and business applications are foundational to many business operations. However, these exact five technology categories were identified as presenting significant cybersecurity risks. Thanks to their ubiquity and complexity, they're all highly vulnerable to exploitation, posing far-reaching consequences when breached.

Interestingly, the report also found that the choice of cloud providers plays a pivotal role in cybersecurity outcomes, with businesses using Google Cloud reporting a 28% lower frequency of cyber incidents and the lowest severity of breaches compared to users of other platforms. By contrast, Microsoft Azure showed the highest severity of cyber incidents.

Action points for business leaders

Understanding these trends is half the battle. Next, business leaders should consider implementing the following action points with the above trends in mind:

- Conduct regular cyber risk assessments: Identify critical assets and data, evaluate existing security controls, and prioritize risks based on potential impact. Businesses can even leverage tools like Cowbell Factors to benchmark their organization's security against industry peers and identify vulnerabilities.
- Strengthen supply chain security: Implement robust third-party risk management practices, including vetting suppliers, conducting security audits, and monitoring vendor cybersecurity performance. This should include ensuring contractual agreements mandate strong cybersecurity measures across your supply chain.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- Invest in employee cybersecurity training: Not only do business leaders across the board need to provide ongoing, role-specific training focused on phishing awareness, safe data handling, and secure remote work practices - but they should also promote a culture of cybersecurity awareness within the organization.
- Fortify incident response and backup systems: As well as developing a detailed incident response plan, with clearly assigned roles and responsibilities in the event of a cyber event, implementing automated, regular backups stored offline or in segmented networks is one of the best ways to minimize ransomware impact.
- Take a proactive approach to technology risk management: Establish a rigorous patch management program for operating systems, server-side technologies, and business-critical tools. Also look to secure content management and collaboration platforms with access controls, encryption, and regular audits.
- Tailor cybersecurity strategies to industry-specific risks: It's vital you consider your industry when implementing cybersecurity strategies. Those in manufacturing, for example, should prioritize securing operational technology, updating legacy systems, and protecting intellectual property, while those in education and public services must focus on ransomware defenses, including strong backup strategies and email security enhancements.

Only by truly understanding these trends and implementing the recommended action points, can business leaders take the necessary steps toward improving their organization's cyber resilience.

And one final note - cybersecurity is not a one-time effort. The threat landscape will undoubtedly continue to evolve as we head into 2025. As such, the long-term success and security of businesses across all sectors requires continuous vigilance, adaptation, and investment to stay ahead.

About the Author

Rajeev Gupta is Co-Founder at Cowbell, a leading provider of cyber insurance for small and medium-sized enterprises (SMEs). Gupta was the GM for the Application Protection Business Unit at Zimperium, a leader in mobile security. He comes with 20 years of hands-on experience in software architecture and design of large-scale secure enterprise applications. Prior, at CA Technologies, he was the Head of Product for the Application Delivery business unit, where he mentored several customer teams and led efficient software development strategies for Fortune 500 clients.



Rajeev can be reached online at rajeev@cowbellcyber.ai and on LinkedIn and at our company website https://cowbell.insure/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The OT Cybersecurity Challenge: Navigating the Journey to A Secure Industrial Future

By Doug Barnes, OT Cybersecurity Consultant and Jay Smilyk, VP Global Sales, NanoLock

In today's rapidly evolving industrial landscape, organizations face critical challenges securing their Operational Technology (OT) environments. As industrial and manufacturing sectors continue to modernize their operations, the convergence of IT and OT systems has created new vulnerabilities that cybercriminals are eager to exploit. The complexities of the OT cybersecurity journey demand careful navigation and strategic planning to build a robust security posture for the industrial world.

The Current State of OT Cybersecurity

The cybersecurity landscape in industrial settings presents a complex challenge. Despite increased spending on cybersecurity solutions, many organizations still lack OT cybersecurity maturity. Many organizations have implemented cybersecurity measures such as network protections, but they often lack robust protection mechanisms for their production floors. This often leaves critical assets, such as Programmable Logic Controllers (PLCs) that control operations on production floors, unprotected. This gap is particularly concerning as it leaves critical infrastructure vulnerable to potentially devastating attacks.

The implications of this vulnerability are far-reaching. Attacks on these systems have the potential for severe financial repercussions, disrupting operations and causing significant economic damage. More

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

alarmingly, compromised OT systems could impact employee and public safety, as well as essential services, potentially leading to life-threatening situations.

The IT-OT Convergence Challenge

One of the most significant challenges in OT cybersecurity is the convergence of IT and OT systems. Traditionally, these two domains were operated separately, with OT systems often being air-gapped and isolated from external networks. However, the drive for increased efficiency, remote monitoring, and data-driven decision-making has led to the integration of these systems, creating new attack surfaces for cybercriminals to exploit.

IT is far more advanced and mature than OT in terms of cybersecurity. The challenge arises at the IT/OT convergence point, where traditional IT cybersecurity strategies are not suited for the unique requirements of OT environments. This highlights the fundamental challenge organizations face when trying to secure their OT environments by adopting IT security practices:

1. **Legacy devices**: Many OT environments rely on legacy devices that were never designed with cybersecurity in mind. These devices often lack basic security features and can't be easily updated or patched. Moreover, replacing legacy devices is a costly endeavor, as OT devices are expensive and upgrading to newer models typically requires shutting down operations, further increasing the overall cost.
2. **Operational Priorities**: In OT environments, availability and reliability often take precedence over security. Any security measure that could potentially disrupt operations is likely to face resistance.
3. **Diverse Technology Landscape**: Industrial environments often feature a mix of technologies from various vendors and different generations, making it challenging to implement a security measure that can cover all.
4. **Increased Attack Surface**: IT/OT connectivity expands the attack surface, exposing OT environments to threats originating from IT networks, such as ransomware and malware attacks.
5. **Lack of Visibility**: Many organizations struggle to maintain a comprehensive inventory of their OT assets and are often unaware of what assets are deployed in their OT environment. This lack of visibility makes it difficult to assess vulnerabilities and implement appropriate protections.

Building a Robust OT Cybersecurity Posture

Navigating the OT cybersecurity journey requires a strategic approach that addresses the unique challenges of industrial environments. Here are key steps organizations should consider:

1. Asset Discovery and Inventory

The first step in securing an OT environment is knowing what needs to be protected. Organizations should implement tools and processes to discover their inventory of all OT assets, including legacy systems. This inventory should be continuously updated to reflect changes in the environment.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

2. Risk Assessment

With a comprehensive asset inventory, organizations can conduct thorough risk assessments. This process should identify critical assets, potential vulnerabilities, and the potential impact of a successful attack on each asset.

3. Implement a Layered Security Approach

Protecting OT environments requires a multi-layered security strategy that addresses vulnerabilities at various levels of the industrial network architecture. While network segmentation is crucial for protecting Level 3 (operations systems) and Level 4 (IT network / logistics systems), it's not sufficient on its own. Organizations must extend protection to lower levels, implementing secure remote access solutions with granular controls and multi-factor authentication. Critically, this layered approach should include Level 1 protection for devices like PLCs, which are often the last line of defense against cyber threats. By securing these foundational components, organizations can prevent unauthorized changes and maintain the integrity of their most critical operational assets, even if other security measures are compromised.

4. Comprehensive Visibility and Asset Management

Implementing solutions that provide comprehensive visibility into actions taken on critical assets is crucial for OT security. These solutions should offer real-time monitoring of all activities and live management of sessions. This includes tracking who is accessing OT devices, logging actions taken, and the ability to terminate unauthorized sessions. Such visibility allows organizations to quickly identify and respond to potential threats, reducing the risk of both malicious attacks and unintended operational disruptions. t

5. Incident Response Planning

Developing and regularly testing an incident response plan is critical. This plan should be tailored to the unique challenges of OT environments and should involve both IT and OT teams. A crucial component of incident response is maintaining a proper backup and recovery strategy that enables rapid rollback to known-secure system states. This allows organizations to quickly restore critical OT systems to their last verified configuration in case of a security incident, minimizing operational downtime and reducing potential damage to industrial processes.

6. Human Factors and Operational Risk

Human error remains one of the biggest cybersecurity risks in OT environments. This includes unintentional misconfigurations, accidental system changes, or improper handling of critical operational equipment. These inadvertent actions can lead to significant disruptions in industrial processes or create security vulnerabilities. Hence it is important to implement solutions that allow for a robust credential repository, and proper password management.

7. Governance and Policy Development

Establishing clear governance structures and developing comprehensive policies and procedures for OT security is essential. These should align with industry standards and best practices while addressing the specific needs of the organization.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The Road Ahead

The journey to OT cybersecurity maturity is ongoing and complex. CISOs often struggle with this journey, noting "This is not an easy path... it can take two plus years to get to the point where IT and OT departments work together effectively."

Organizations must recognize that achieving OT cybersecurity is not a one-time project but a continuous process of improvement and adaptation. It requires commitment from the organization's leadership, collaboration between IT and OT teams, and a willingness to invest in both technology and people.

As the IT and OT convergence grows in industrial and manufacturing environments, the importance of OT cybersecurity will only increase. Those who successfully navigate this journey will not only protect their operations from cyber threats but also position themselves to fully leverage the benefits of digital transformation in the industrial world.

About the Authors

Doug Barnes, OT Cyber Security Consultant



Doug Barnes has over 30 years of IT/OT technical experience in a variety of industries. The last 11 years were spent at both GE & Whirlpool, where he had a variety of OT Technology design and OT Cybersecurity roles within both companies. While at GE Aviation he designed the architecture of the Network & Data security models for the GE Proficy MES system, which was rolled out to 10+ sites. At GE Power he defined the OT network design and segmentation, DMZ OT design, and implemented OT threat monitoring (World Tech – GE Product). While at Whirlpool, he designed the global DMZ & OT network segmentation template, created the global OT governance policies which utilize both NIST SP 800 R83 & IEC 62443 (parts 2 & 3), in conjunction with designing and rolling out the initial OT cybersecurity template utilizing Claroty, Rockwell FactoryTalk Asset Center, and Octoplant.

Doug can be reached online at https://www.linkedin.com/in/douglas-barnes-138b46

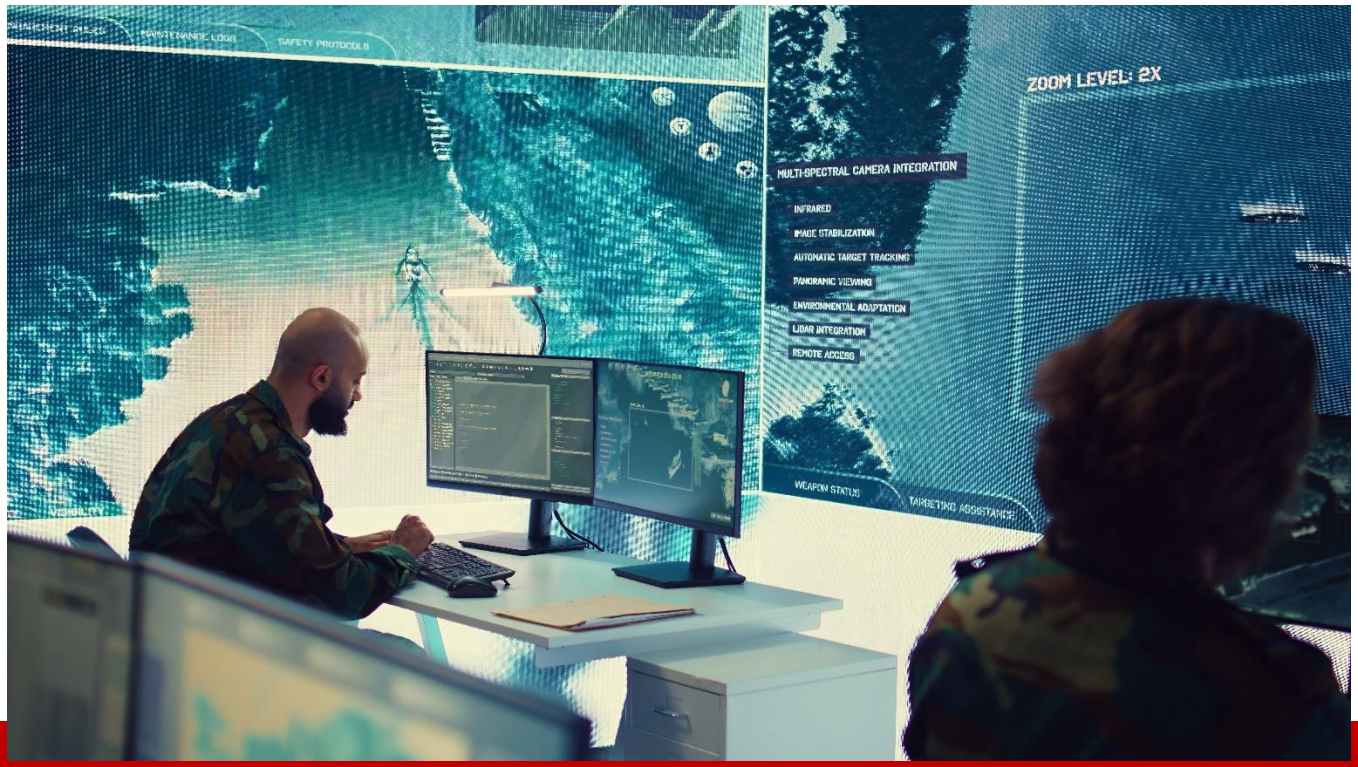
Jay Smylik VP Global Sales at NanoLock Security



Jay Smilyk has over two decades of experience in sales leadership and technology sales. Jay has held executive positions and sales management roles and has served as CRO of Tripleblind and Sepio Systems. Before that, he was the Eastern Regional Director of Sales for Vectra Networks. Jay also previously served as VP of Sales at Safend, where he built a team of security professionals to bring endpoint data protection solutions to the US market.

Jay can be reached online at https://www.linkedin.com/in/jsmilyk/ or via email at jays@nanolocksec.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Raising Cybersecurity Awareness in The Age of AI And Cyber Warfare

By Neal Quinn, head of Radware's cloud security services business

The start of a new year presents a valuable opportunity for organizations and individuals alike to reassess the ever-evolving cyber threats shaping our world. Among the most impactful trends poised to define 2025 are the rapid rise of Artificial Intelligence (AI) and the growing democratization of DDoS attacks as tools of cyber warfare.

Experts from Radware weigh in on these pressing challenges and offer guidance for identifying and dealing with each.

AI: A Double-Edged Sword

Howard Taylor, Radware's CISO, highlights that AI has become a central player in the cybersecurity field, both as a defense tool and as a growing risk. "You can't think about raising cybersecurity awareness without keeping an eye on AI," he says. "While AI has improved incident detection and response capabilities, it has also opened new doors for cybercriminals."

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Applications like ChatGPT and CoPilot have been weaponized by bad actors to not only create more realistic and convincing deepfakes and automated phishing scams and influence campaigns but also launch them more easily at scale. The rapid adoption of these technologies has also created compliance risks that, without proper oversight, can expose companies to legal and financial troubles. “In the absence of proactive monitoring, companies risk overlooking important issues that should have been identified, resolved, and reported,” Taylor warns.

Moreover, AI has complicated the legal landscape, sparking what Taylor refers to as “cyber lawfare” and the increasing business threat of fines, lawsuits, and potential imprisonment. AI applications may unknowingly pull copyrighted material into AI-generated text. Lawfare hunters have tools to identify these breaches and attempt to extract payment from the “copyright violator.” CEOs and boards must now consider this growing regulatory risk as an additional cost of doing business.

Cyber Warfare and the Democratization of DDoS Attacks

Like AI, cyber warfare has played a significant role in reshaping the threat landscape. “You can’t address cybersecurity awareness without addressing the reality of cyber warfare,” Pascal Geenens, Radware’s director of threat intelligence explains. “With more than two years of illegal attacks left unprosecuted following Russia’s invasion of Ukraine and the surge in hacktivism, the threshold into a life of cybercrime has reached a new low. Putting DDoS attacks within the reach of the everyday person is not just for video games. The IT Army of the Ukraine used a similar strategy.”

The group successfully built upon the collective power of volunteers across the globe and in the process became a pioneering force in the democratization of DDoS attacks. “At the same time, they have set the stage for future cyber warfare strategies and reframed what it will take to secure our world going forward,” Geenens added.

As these types of tactics gain traction, future cyber warfare strategies will become even more decentralized and accessible, presenting new challenges for global security.

Critical Infrastructure at Risk

Critical infrastructure has become a top target for malicious DDoS campaigns waged by hacktivists with political and religious motivations. “Organizations must pay special attention to the heightened risks to critical infrastructure,” says Travis Volk, Radware’s senior vice president of global service providers. “Part of raising cybersecurity awareness is being reminded of a rapidly evolving threat landscape, where critical infrastructure is increasingly targeted by foreign adversaries.”

From internet service providers (ISPs) to large telecoms, these entities represent high-value targets for cybercriminals due to the vast amounts of sensitive data they handle and their access to downstream customers. With AI accelerating the speed and sophistication of attacks—ranging from UDP floods to web, bot, and API business logic attacks—companies need to adopt a proactive, agile approach to

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

resilience planning and rapid response. As Volk puts it, "Securing our world from attacks in the future means we must be prepared to evolve alongside them."

AI in Security: A Crucial Investment

Finally, John Eisenbarger, Radware's vice president for U.S. carriers and service providers, emphasizes that the growing complexity of cyber threats is pushing more organizations toward managed security services, with AI playing a crucial role in accelerating this transition. "Now is a good time for all organizations to evaluate their AI investment and the critical role AI can play in enhancing their security measures," Eisenbarger advises.

As the cybersecurity talent gap widens and attacks become more aggressive, AI can serve as a critical force multiplier, allowing organizations to stay competitive against cybercriminals who are already exploiting the technology to their advantage. "Cybercriminals are certainly not waiting to make the most of AI. Industry will need to keep pace," Eisenbarger adds.

A Call to Action

The rise of AI, the democratization of DDoS attacks, and the threat to critical infrastructure require immediate attention not just during Cybersecurity Awareness Month but throughout the year. It is important to recognize that cybersecurity success hinges on the ability of organizations to quickly evolve their defenses alongside these emerging threats. As AI continues to blur the lines between defense and risk, organizations must be resigned to stay vigilant, adaptable, and proactive.

About the Author



Neal Quinn is Head of Cloud Security, North America at Radware. Neal has over 20 years of experience in the architecture and operation of managed cloud security services and cloud DDoS mitigation. Prior to Radware, Neal was VP of Networks at Akamai, leading the global capacity planning organization and later in his tenure the countermeasures engineering teams for the Security Business Unit, in addition to leading large global capacity buildout programs for the DDoS mitigation scrubbing centers. Prior to its acquisition by Akamai, Neal was the CTO at Prolexic Technologies, leading the SOC, Engineering, Architecture and SERT teams. Neal has extensive experience consulting with large enterprise accounts and facilitating tactical security responses in complex organizations.

Neal can be reached online at https://www.linkedin.com/company/radware and at our company website https://www.radware.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Why Medical Device Manufacturers Need MedTech Experts for SBOM Management

By Ken Zalevsky, MedTech Expert & CEO, Vigilant Ops

The medical device industry operates at the intersection of innovation and responsibility, where safeguarding patient lives and ensuring compliance with stringent regulations are equally critical. Effective Software Bill of Materials (SBOM) management has emerged as an essential strategy for navigating cybersecurity and regulatory challenges in this high-stakes environment.

Unique Challenges Facing Medical Device Manufacturers

Medical device manufacturers face challenges: evolving regulations, complex supply chains, and maintaining stakeholder confidence.

The Shifting Regulatory Horizon

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Regulatory bodies, including the FDA, increasingly emphasize transparency and robust lifecycle management of SBOMs. New requirements demand precision and agility, and failure to comply could lead to delays, denied approvals, or even recalls. Without effective SBOM management practices, organizations risk regulatory penalties and damage to their reputations.

Elevated Risk of Compromise

Medical device organizations face a significantly higher risk of cyber compromise compared to other healthcare sectors. According to SecurityScorecard's 2024 "The Cyber Risk Landscape of the U.S. Healthcare Industry" report, **medical device and equipment companies scored 2-3 points lower in security ratings than the overall healthcare sample**. These organizations also experienced a **16% higher rate of reported breaches and compromised machines**. This underscores the urgency for tailored cybersecurity solutions to mitigate risks and maintain trust.

Complex Supply Chains

Medical devices often depend on a vast ecosystem of suppliers, legacy components, and third-party software. Managing vulnerabilities across this intricate supply chain is vital to ensure both security and compliance. A single overlooked vulnerability could compromise device functionality, patient safety, and trust.

Maintaining Stakeholder Confidence

Trust is the foundation of the medical device industry. Manufacturers must demonstrate to regulators, healthcare providers, and patients that their devices remain secure throughout their lifecycle. Achieving this requires proactive and transparent software supply chain risk management.

The Case for MedTech Expertise

Generic cybersecurity solutions often fall short of addressing the specific needs of medical device manufacturers. MedTech expertise brings critical advantages, including:

- **Specialized Knowledge:** A deep understanding of the interplay between compliance, safety, and innovation ensures that SBOM management practices align with regulatory and industry demands.
- **Tailored Approaches:** Customized solutions that meet manufacturers where they are—whether implementing SBOM practices for the first time or optimizing mature vulnerability management processes—allow for greater adaptability and effectiveness.

Best Practices for SBOM Lifecycle Management

To navigate these challenges effectively, medical device manufacturers should adopt strategies that ensure comprehensive SBOM management:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

- **Automating Compliance:** Streamlining the creation and management of SBOMs to align with FDA requirements and global standards minimizes friction and accelerates time to market.
- **Integrating Deployed and Build SBOMs:** Combining these elements provides a complete view of vulnerabilities across the software supply chain, enabling informed, proactive decision-making.
- **Fostering Stakeholder Confidence:** A proactive approach to supply chain risk management builds trust among regulators, healthcare providers, and patients, solidifying the manufacturer's reputation.

Setting a New Standard for SBOM Cybersecurity

The regulatory and threat landscape will continue to evolve, demanding a forward-thinking approach to SBOM management. MedTech expertise is no longer optional but critical in ensuring patient safety, regulatory compliance, and operational excellence. By embracing comprehensive SBOM practices, medical device manufacturers can safeguard their products, protect their patients, and set new benchmarks for security and trust in the industry.

About the Author



Ken Zalevsky is the CEO of Vigilant Ops, Inc. He is a passionate advocate for the application of advanced technology to improve cybersecurity across all industries.

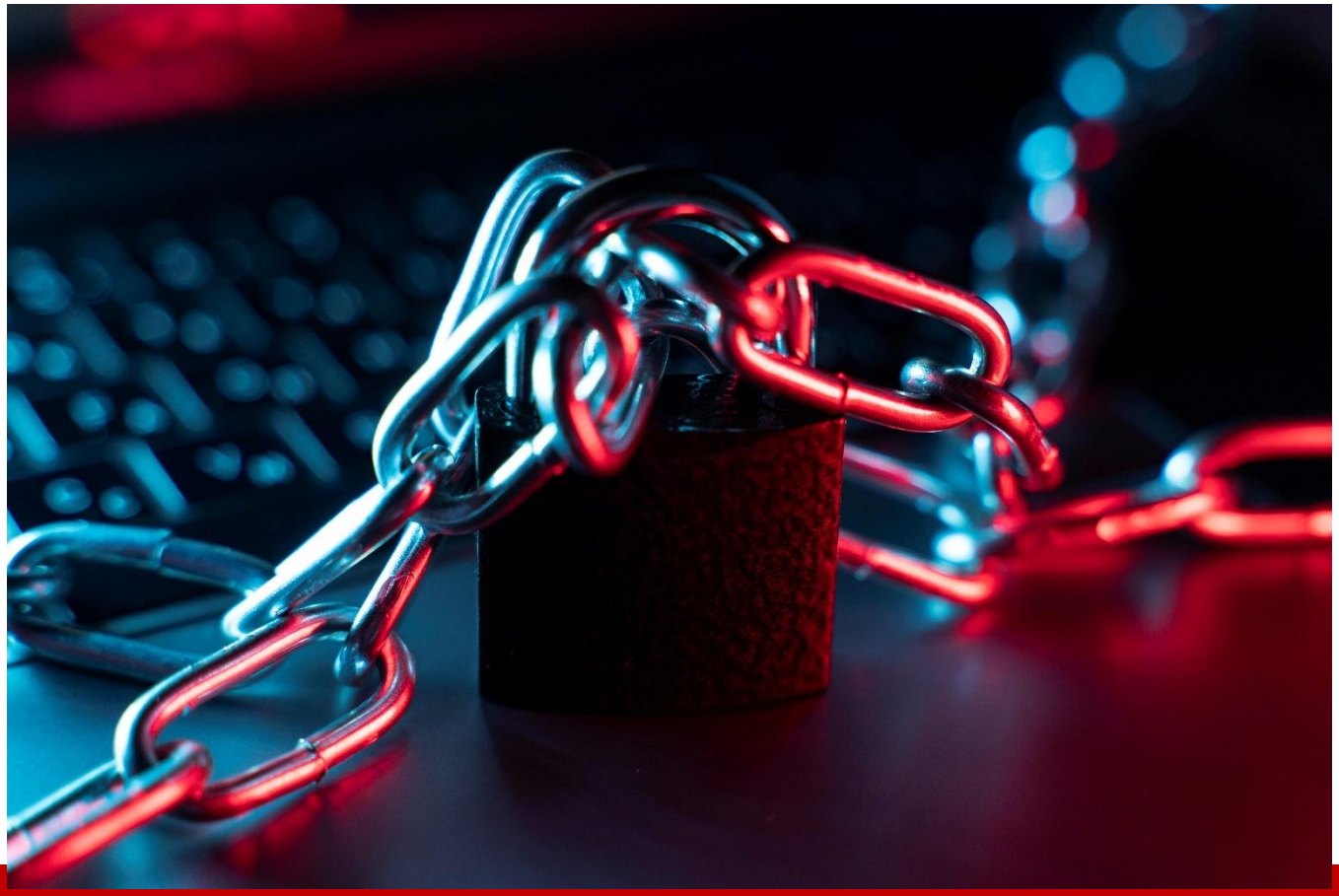
He has collaborated with the United States Food and Drug Administration, US Department of Homeland Security, and the National Telecommunications and Information Administration (NTIA) on various cybersecurity initiatives, including cyber simulation exercises, industry guidance documents, and most recently, SBOM initiatives.

Ken has been a featured speaker at numerous cybersecurity conferences over the years and actively participates on various cybersecurity industry working groups. He has authored numerous cybersecurity whitepapers, blogs, magazine articles, and his work has been published in various industry journals, where he has advised medical device manufacturers on cybersecurity best practices and coached hospitals as they continually struggle with record numbers of breaches.

Ken is a certified Cybersecurity Leader from the School of Computer Science at Carnegie Mellon University and earned an undergraduate degree in Applied Math and a graduate degree in Business Management, both from Carnegie Mellon University. Ken also attended the Executive Education program at Harvard Business School

Ken can be reached online at ken.zalevsky@vigilant-ops.com and at our company website www.vigilant-ops.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Beyond The Breach

Rethinking Backup Strategies for Resilience

By Jon Fielding, Managing Director, EMEA, Apricorn

Data breaches are an unavoidable reality, growing in both sophistication and impact. For organisations, the ability to recover quickly from a breach is critical to maintaining operations and avoiding significant financial and reputational damage. Yet, new research reveals troubling gaps in backup strategies that undermine this capability. As businesses face rising threats, they must rethink their approach to backups, ensuring a more resilient and comprehensive strategy that can withstand even the most severe cyberattacks.

The backup conundrum

Recent findings from Apricorn's annual survey indicate that while many organisations recognise the importance of backups, their practices leave much to be desired. Among IT decision-makers who experienced a breach and needed to recover data, only 50% were able to fully restore their information.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

A concerning 25% managed only partial recovery, and 8% failed entirely due to inadequate backup systems.

These shortcomings highlight a widespread overconfidence in existing measures. While only 9% of respondents admitted their backup systems were not robust enough for rapid recovery, this confidence is clearly misplaced given the prevalence of incomplete recoveries. This disconnect points to a critical need for businesses to reassess their backup strategies and address vulnerabilities.

Overreliance on cloud solutions

The UK Government's Cyber Security Breaches Survey 2024 revealed that 71% of businesses rely solely on cloud service providers (CSPs) for their backups. While the cloud offers scalability and convenience, it is not immune to risks. Cloud breaches, misconfigurations, and ransomware attacks targeting CSP infrastructure can compromise vast amounts of data.

The Microsoft Azure breach, for instance, exposed vulnerabilities in cloud architecture, highlighting the potential for significant disruption when cloud services are compromised. Businesses that place all their data in one digital basket risk devastating consequences.

Organisations must diversify their backup approaches by supplementing cloud storage with offline, encrypted backups on removable devices. A portable encrypted hard drive stored securely offline provides an additional layer of defence against ransomware and other cyber threats.

The power of diversification

A robust backup strategy must avoid single points of failure. The widely endorsed "3-2-1 rule" provides a blueprint for resilience: organisations should maintain at least three copies of their data, stored on at least two different types of media, with at least one copy kept offsite. This multi-layered approach ensures that even if one backup fails, others remain accessible.

Encouragingly, Apricorn's survey revealed progress in diversification, with 30% of respondents automating backups to both central and personal repositories, up from 19% in 2023. Automated backups reduce reliance on manual processes, ensuring critical data is saved regularly and consistently without human error.

Backup failures and cyber insurance

The importance of robust backups extends beyond recovery; they are now a key factor in cyber insurance compliance. Insurers increasingly require demonstrable backup policies as a condition for coverage. According to Apricorn, 46% of IT decision-makers recognise the link between backup strategies and cyber insurance requirements, up from 28% the previous year.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Failing to meet these requirements can leave businesses uninsured and financially exposed after a breach. Conversely, organisations with strong backup systems are better positioned to recover quickly and demonstrate to insurers their commitment to minimising risk.

A culture of preparedness

Backup strategies are only part of the equation. A broader culture of cybersecurity preparedness is essential. This includes employee training, robust access controls, and aligning backup practices with established frameworks such as the UK's National Cyber Security Centre's (NCSC) "10 Steps to Cyber Security." Testing recovery processes in simulated breach scenarios can also reveal hidden vulnerabilities and enhance response readiness.

In a world of escalating cyber threats, a robust backup strategy is non-negotiable. Businesses that rely solely on the cloud or fail to test their recovery systems are gambling with their future. As breaches become more sophisticated and the stakes grow higher, organisations must invest in resilient, multi-layered backup systems to protect their data and operations.

By adopting best practices and embracing a diversified approach to backups, businesses can mitigate risks, ensure compliance with insurance requirements, and safeguard their reputation in an increasingly hostile digital landscape. Cyber resilience starts with reliable backups because when a breach happens, recovery is everything.

About the Author



Jon Fielding is the Managing Director of Apricorn in EMEA and has extensive experience in growing companies in the EMEA market. Jon is responsible for the sales & operations strategy, driving revenue growth and establishing the channel network in the region.

Jon is CISSP certified and has been focused on Information Security for the past 18 years, working with a variety of organisations from IBM to security start-ups such as Valicert and Tumbleweed.

Jon joined Apricorn from IronKey where he worked exclusively in the secure USB market having established the Ironkey office in EMEA 8 years ago as the first in the region. During his tenure, Ironkey was acquired by Imation and then by Kingston.

Jon can be reached online at linkedin.com/in/jon-fielding-290662 and at our company website www.apricorn.com

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Advancing Technologies in The Year Ahead Make Digital Trust More Essential

Navigating AI And Quantum Computing Advances: Strengthening Digital Trust In 2025

By Tim Hollebeek, VP Industry Standards, DigiCert

The past year will be remembered for major developments in two emerging technologies: AI and quantum computing. Generative AI was all over the headlines in 2024, appearing in new desktop and mobile products from Apple and other industry heavyweights, shaking up social media interactions, and transforming enterprise processes in every sector. Quantum computing made massive strides as well, with new chips reaching breakthrough performance.

These technologies offer big potential benefits, but they also introduce distinct security and identity challenges for device manufacturers and enterprise organizations. In a recent blog, DigiCert predicted the cybersecurity challenges and opportunities expected in the year ahead.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Post-quantum cryptography will come off the drawing board and into production

Quantum computing will change everything when it comes to digital trust. The same technology that's capable of solving massive, data-intensive problems will also be capable of breaking the cryptography and public key infrastructures that we depend on.

The good news is that industry and government groups are taking aggressive steps to help enterprises strengthen their cryptography to prepare for new threats. The National Institute of Standards and Technology (NIST) has recently finalized a set of Post-Quantum Cryptography (PQC) standards designed to withstand quantum computing attacks. These new standards are poised to roll out as part of operational solutions.

The first steps of putting PQC into production are happening now, as the U.S. National Security Agency (NSA) prepares to announce post-quantum updates to it's the Commercial National Security Algorithm Suite (CNSA). These new CNSA 2.0 algorithms will provide protection for critical national security systems (***NSS***) networks.

More manufacturers and enterprise organizations will rapidly deploy PQC algorithms, incorporating them into business processes, applications, hardware security modules (HSMs), and other devices. Crypto-agility, including certificate automation, will play an important role in deploying out these new algorithms at scale.

Global industry organizations are also making quantum-resistant cryptography a top priority. For example, the Quantum Safe Financial Forum, a consortium of financial institutions, has been organized to drive a coordinated approach to the transition to PQC in the financial sector. We'll also see PQC evolve to become a regulatory standards imperative.

Content Provenance and Authenticity (C2PA) standard will become commonplace

To strengthen digital trust and confidence in the wake of new AI deepfakes and other challenges, DigiCert also predicts that content provenance standards will also rise to the forefront.

In an era where we can't be sure of the authenticity of photographs, video, and other media, it's more important than ever to be able to verify the source of content. The C2PA standard aims to do just that, utilizing a Content Credentials icon to identify authentic content.

Based on PKI, the C2PA standard produces a tamper-evident record that helps media consumers distinguish between real and fake content. If content is altered or edited, the content changes are recorded, which makes it easier to spot manipulated content such as AI deepfakes. Online images will soon carry the C2PA icon, making it easier for consumers and content creators to confirm the authenticity of content.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Change driven from the top

New standards will play a key role in helping organizations meet new challenges, but ultimately digital trust will need to be encouraged by the people within companies. In the coming year, Chief Trust Officers (CTrOs) will become more prevalent in organizations looking to make transparency and digital trust a top business imperative.

Organizations across every industry are digitally transforming the way they work and interact with customers. That means trust has become a key component in customer relationships and business processes. A CTrOs is responsible for making secure digital experiences, data privacy, and ethical use of AI a part of the company culture.

CTrOs help build and sustain trust with customers, regulatory organizations and business partners. They help ensure that their organizations not only comply with regulatory standards but also promote trust as a fundamental business value and asset. The importance of executives who understand the need to align security, technology, and transparency will only grow.

Proactive planning is key

We're seeing new challenges from quantum computing and AI springing up fast, but it's not too late for organizations to get out in front of the new challenges they bring. By taking a close look at how and where all cryptographic assets are used within your organization, you can better understand potential risks—and start taking steps to mitigate them.

About the Author

Tim Hollebeek, VP of Industry Standards at DigiCert Timothy Hollebeek has 20+ years of computer security experience, including eight years working on innovative security research funded by the Defense Advanced Research Projects Agency. He remains heavily involved as DigiCert's primary representative in multiple industry standards bodies, including the CA/Browser Forum, striving for improved information security practices that work with real-world implementations. A mathematician by trade, Tim spends a lot of time considering security approaches to quantum computing. Tim can be reached at tim.hollebeek@digicert.com and at our company website www.digicert.com



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Risk of Identity Attack Paths: 10 Stats Everyone Must Know

Most organizations are at risk of this threat that has persisted for decades

By Jared Atkinson, Chief Strategist, SpecterOps

The threat of identity-based attack paths – the chains of abusable privileges and user behaviors that create connections between computers and users – has persisted for decades. Most organizations are at risk, whether they know it or not.

The threat applies to all organizations using identity and access management platforms, in particular Microsoft Active Directory (AD) and Microsoft Entra ID (formerly Azure Active Directory). These are favorite targets among attackers and can deliver unmatched payoff. These platforms are widely used among enterprises, with approximately 95% relying on AD. Gaining control of them means attackers can obtain full control of all users, systems, and data in that organization.

Complicating matters, attack paths are often unseen and unmanaged problems. IT environments undergo constant change in both size and complexity. This constant change, combined with the variable of user behavior, creates more attack paths daily. An enterprise can easily have thousands of users and

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

tens of thousands of networked devices. At this scale, it's easy for attack paths to escape notice, especially because AD makes it difficult to analyze user permissions. Finding an attack path is virtually guaranteed for those who seek it.

To defend against this threat, organizations and end users must arm themselves with as much knowledge as possible about the threat they face. Below, we walk through 10 stats everyone needs to know about identity attack paths.

1. **100% of environments have an attack path to Tier Zero and complete environment takeover.** Tier Zero refers to an organization's most privileged assets and accounts in its IT environment. If a threat actor compromises a Tier Zero account, they can gain control of enterprise identities and their security dependencies. They can then do extensive damage to the organization's operations and reputation. Security teams must take preventive measures to secure their Tier Zero assets from attack paths.
2. **90% of breaches that cybersecurity firm Mandiant investigated recently involved AD (where attack paths live) in some form.** AD presents a vast attack surface for adversaries with numerous moving parts, giving threat actors much room to perform malicious activities. Cyber defenders must be aware of this security challenge and adopt a proactive approach in their threat hunting instead of merely reacting to threats that emerge.
3. **On average, over 70% of users in an AD domain have at least one attack path to Tier Zero and control over the enterprise.** Many organizations take steps to enact the principle of least privilege, or the concept that limits access to only those required to perform a task. But unfortunately, least privilege is often out of reach for a variety of reasons. Organizations often struggle to find the balance between security and usability. As a result, privileges that are given for otherwise practical reasons can create attack paths linking every user and computer in the organization's environment to the most highly sensitive systems and highly privileged principals.
4. **On average, AD Certificate Services misconfigurations allow over 50% of users to take over the enterprise in one attack.** The security ramifications of misconfigured certificate service instances are extensive and serious. Certificate abuse can enable an attacker to conduct user credential theft and maintain continuous access to the AD environment across password changes, restarts, and changed credentials, giving them an alarming level of access.
5. **Analysis of 2 billion abusable relationships showed that most attacks can be mitigated by fixing the 0.02% of misconfigurations that connect attackers to Tier Zero.** Attack paths often funnel through a few "choke points," or locations where multiple attack paths converge on sensitive data, that lead to Tier Zero. There are a few common misconfigurations that create them. A relatively small amount of work to fix these misconfigurations can eliminate a significant number of critical attack paths, reducing the risk your organization faces considerably.
6. **On average, cutting one attack path choke point severs 17,000 attack paths.** Large organizations will have too many attack paths to remove all of them, but focusing strategically on choke points to assess and remediate can reduce risk significantly without requiring an insurmountable workload. You can eliminate the threat of thousands of downstream misconfigurations and take away an adversary's attempt to control your organization.
7. **Mapping an AD or Azure tenant is about as complex as mapping all the roads and cities in the United States.** Attack paths are everywhere in part because AD and Azure environments are so large and complicated. For instance, the U.S. includes 20,000 cities connected by nearly 5

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

million roads. Comparatively, an average AD domain or Azure tenant contains 130,000 identities (users and computers) and resources (servers, storage volumes, printers) connected by 3.5 million abusable relationships.

8. **A random sampling by cybersecurity company SpecterOps found synced privileged roles in 100% of AD environments.** Microsoft specifically recommends not syncing privileged users between on-prem and Azure AD because doing so allows adversaries to bypass identity safeguards and enhanced security controls like multifactor authentication (MFA) and conditional access. However, many organizations are not adhering to this guidance, likely due to the challenge of balancing security with usability effectively.
9. **70% of IT environments randomly sampled synced regular on-premise user accounts to Tier Zero roles like Global Administrator.** In doing so, these organizations significantly increase the risks they face, eliminating a layer of protection and making it easier for adversaries to gain the keys to their kingdom.
10. **Organizations employing an attack path management solution can experience an average 35% reduction of risk.** An attack path management solution can help unite and empower an organization's IT and security teams to proactively sever attack paths without disrupting operations. These solutions can enable continuous attack path mapping, quantify identity attack path choke points in AD environments, and provide precise remediation guidance, resulting in improving an organization's security posture.

The threat of identity attack paths will persist as long as organizations rely on AD. To combat this threat effectively, organizations must know the risk they face. They can employ an attack path management methodology, which enables continuous discovery, mapping, and risk assessment of AD attack path choke points. Taking these steps will help organizations eliminate, mitigate, and manage the attack paths they face and keep their keys to the kingdom in the right hands.

About the Author

Jared Atkinson is the Chief Strategist at SpecterOps. He is a security researcher who specializes in Digital Forensics and Incident Response. Recently, he has been building and leading private sector Hunt Operations capabilities. In his previous life, Jared led incident response missions for the U.S. Air Force Hunt Team, detecting and removing Advanced Persistent Threats on Air Force and DoD networks. Passionate about PowerShell and the open-source community, Jared is the lead developer of PowerForensics, Uproot, and maintains a DFIR focused blog at www.invoke-ir.com. You can follow Jared on X @jaredcatkinson and via the SpecterOps company website at https://specterops.io/.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Attacks Against Networks and VPN Infrastructure Surged in The Last 12 Months – Preparing for The Road Ahead

Implementing Next-Gen VPN Measures, Adopting Zero-Trust Strategies to Strengthen Defenses Against Emerging and Post-Quantum Threats.

By Lawrence Pingree, VP of Technical Marketing, Dispersive

In 2024, we saw a major rise in attacks targeting networks and VPN infrastructure, exploiting vulnerabilities, and employing sophisticated techniques to compromise sensitive data and disrupt operations.

Over the next 12 months, look for increased sophistication in these attacks, with threat actors continually refining techniques, and employing strategies and advanced tools to exploit vulnerabilities and bypass security measures. AI and machine learning techniques will automate attacks and make them more effective.

Unfortunately, VPNs will continue to be a prime target, since they offer access to sensitive data and systems. We'll likely see more attacks aimed at exploiting VPN vulnerabilities and compromising user credentials. Once inside a network, hackers will of course work for lateral movement, seeking to gain access to additional systems and data. This could involve techniques such as privilege escalation and credential theft.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

This means that Zero Trust Network Access and technologies such as stealth networking become essential to combat these and other emerging threats.

The ultimate goal of many attacks will be to exfiltrate sensitive data such as customer information, financial records, patient health records, and intellectual property via malware, phishing, and social engineering.

Attackers may also seek to disrupt business operations, triggering downtime and financial losses. This could involve launching denial-of-service attacks or deploying ransomware to cripple critical systems.

Events and insights from the last 12 months demonstrate some of what we can expect ahead, such as:

- The Check Point Quantum Gateway vulnerability (CVE-2024-24919) highlights the importance of patching vulnerabilities but also upgrading to VPN technologies that eliminate the attack surfaces exposed promptly.
- The rise of AI and machine learning in cyberattacks poses a significant challenge for security professionals, and is expected to continue in 2025, but be increasingly multi-dimensional powered by AI.
- Organizations need to adopt a multi-layered approach to security, combining technology with strong policies and employee education, and focus on preemptive cyber defense technologies instead of being so reliant on detection and response.

Prioritizing cybersecurity and investing in robust defenses is the only way to protect organizational data and systems. Here are 10 best practices to help minimize risk and create a powerful cybersecurity framework:

1. Prioritize VPN security: 56% of organizations experience VPN-related cyberattacks and 91% share concerns about VPN security. Implementing robust next-generation VPN security measures is imperative. Specifically, consider stealth networking – the adage “you can’t hack what you can’t see” has never been more relevant than it is today.

It’s a given that traditional perimeters and boundaries and the legacy technologies that guarded them are no longer able to deliver either the security or the efficiency needed.

This is driving the emergence of stealth networking as the means to remove the common attack surface that exists in traditional network IPSEC and SSL VPNs. It eliminates the attackable surfaces that are often exposed in traditional IPSEC and SSL-based VPNs which come with multi-function firewalls, SD-WAN and standalone VPN gateway solutions.

2. Adopt zero-trust strategies: 78% of organizations plan to implement zero-trust strategies, and this is an ideal opportunity for practitioners to adopt a more secure approach by verifying the identity of all users and devices before granting access to sensitive resources.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

3. Monitor for ransomware attacks: Ransomware remains one of the top threats exploiting VPN vulnerabilities (42%). Staying vigilant in monitoring networks for signs of ransomware activity, such as unusual network traffic or suspicious user behavior, is essential.

4. Schedule and conduct audits and penetration testing: The threat landscape is growing, as the 30% increase in malware attacks between 2023 and 2024 indicates. Security audits and penetration testing can help identify vulnerabilities before they are exploited by attackers.

5. Review and update incident response plans: With over 7 billion records exposed in data breaches, a robust incident response plan is essential for minimizing breach "blast zones" and impacts.

6. Implement security measures to prevent DDoS attacks: DDoS attacks are another top threat exploiting VPN vulnerabilities (30%), and implementing security measures such as rate limiting and IP blocking can mitigate these types of attacks.

7. Monitor data breaches closely: The average cost of a data breach in 2024 was $4.88 million, highlighting the importance of monitoring for signs of data breaches and taking swift action when they occur.

8. Keep up to date with security patches and updates: With an increase in malware attacks between 2023 and 2024 (30%), it is essential to stay current with the latest security patches and updates for all systems, including the latest generation of preemptive defense VPNs that Dispersive provides, to reduce the attack surface and prevent exploitation of known vulnerabilities.

9. Educate users about phishing threats: Phishing continues to be the primary cause of data breaches (80-95%). It's essential that your users know how to recognize and avoid phishing attacks, including those that are launched through VPNs – a common gap in organizational security.

10. Develop a comprehensive cybersecurity strategy: By recognizing these statistics and implementing robust security measures, organizations can reduce their risk exposure and protect against diverse types of cyber threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Lawrence Pingree is VP of Technical Marketing, Dispersive. As a renowned expert and former Vice President at Gartner's Technology and Service Provider research practice, Lawrence Pingree has been instrumental in shaping the future of security innovation. With over 300 published research notes on cybersecurity, he has helped thousands of businesses and society as a whole evolve by accelerating IT security innovation and enabling its positive impact. As a thought leader in emerging security technologies and trends, Mr. Pingree's insights have guided organizations through the complexities of modern cybersecurity, introducing key concepts such as Security As a Service/Software as a service (SaaS), Software Defined WAN (SDWAN), Content Disarm and Reconstruction (CDR), Endpoint Detection and Response (EDR), Network Traffic Analysis (NTA), Cloud Workload Protection (CWP), Cloud Incident Response Automation (CIRA), Generative Runtime Defense (GARD), and Secure Internet Gateways (SIG). As Dispersive Vice President of Technical Marketing, with his expertise spanning cloud security, endpoint security, generative security, and disinformation security, Mr. Pingree enables businesses to stay ahead of threats and capitalize on new market opportunities, making him a highly respected voice in the industry dedicated to accelerating information technology security innovation and its positive impact on business and society. Lawrence can be reached online at info@dispersive.io, @DispersiveHold, and at our company website https://dispersive.io/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Cryptography and Modern IT: A Digital Innovation Blind Spot

By Dr. Marc Manzano, General Manager, Cybersecurity at SandboxAQ

It goes without saying that data privacy is important for businesses, so why is cryptography management so often left out of the cybersecurity innovation conversation? As businesses grow, there's usually more sensitive data to protect, the pace of which, given the pace of innovation, can be hard to keep up with. However, cryptography is undeniably a pivotal part of IT security, particularly as regulations and data privacy needs surge. Yet, due to a lack of modernization and automation, organizations often struggle to understand their risk of poorly managed cryptography and effectively manage their cryptographic protocols. As a result, the industry has found itself at a crossroads: the digital innovation blind spot.

Modern IT: How Cryptography Got Left Behind (and Why That's a Bad Thing)

For a multitude of reasons, over the past decades, cybersecurity solutions have evolved keeping up with innovation trends in IT. We have seen the creation of new cybersecurity markets tackling security gaps that are now covered. However, this evolution has left behind a crucial factor underpinning an organization's cybersecurity posture: cryptography. The worry? Outdated cryptography processes cannot keep up with the complexity of modern IT. Unmanaged cryptographic artefacts can cause critical application outages too. Essentially, unmanaged cryptography is a (costly) grenade.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Outdated cryptography is a significant financial burden, a legal liability, and a significant security risk, in the same way that an outdated legacy device on a network can be. Whereas cryptography gets left out of the conversation, the security of physical legacy devices on a network are a constant bone of contention. Crucially, both should be regarded as potent cybersecurity risks.

Compliance and Cryptography

Compliance wise, however, cryptography remains a crucial element of security for many organizations. Good cryptography management is often a requisite of industry compliance, especially in the finance and healthcare sectors. PCI DSS, for the payment card industry, for example, mandates strong encryption for data transmission and storage, as well as specifies cryptographic protocols and management practices.

However, these compliance standards often fall short of well managed and maintained cryptography, leaving many organizations at risk. Compliance does not mean secure. Cryptographic compliance often relies on outdated processes that do not meet management or auditor expectations. However, cryptography management requires a specific skill set that many IT professionals do not possess, leading to data protection or key management policies being ignored. A lack of understanding and skill in this area further alienates it from the mainstream discussion of cybersecurity.

Switching Cryptographic Standards

Cryptography standards are the established guidelines that the cybersecurity industry utilizes at large-scale to ensure the secure transmission and storage of sensitive information, digitally. These standards encompass a wide range of constructions. Adhering to cryptography standards means that organizations can feel confident in the security and robustness of cryptographic algorithms and protocols being used.

When it comes from switching from one cryptographic standard to another, the whole organization may be left without an established solution to handle the migration efficiently. For example, it took some organizations up to 10 years to migrate away from SHA-1.

The Future? Quantum Computing and Cryptography

One thing is for certain: the digital world will continue to innovate. Whether cryptography gets left behind (and therefore too hard to retroactively manage later on) is another question. Quantum computers will break modern day public key cryptography. The looming threat of quantum computers puts the c-suite in a tough position: quantum is not happening now, but if you don't secure cryptography for the future promptly, it will be too late. As a result, sensitive data is vulnerable to 'store now, decrypt later' cyberattacks, which cybercriminals steal and store large encrypted datasets with the intention of decrypting in the future. As we get closer to accessible quantum computing these attacks will no doubt increase.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Governing bodies are waking up to the very real threat of quantum computing and modern cryptography though. The US National Institute of Standards and Technology (NIST) recently released 3 quantum-resistant algorithms, with another one coming soon. It is crucial that business leaders take note of this and proactively protect against the future.

But Why Now? Moving Away from *What If, Why* and *When?*

With budgets tight and spending justification a crucial element of security in today's business landscape, we must focus on the immediate risks. AI, for example, poses a significant threat to organizations today, from adversarial machine learning (AI can be used to manipulate training data, leading to models that make incorrect predictions or classifications, for example) to sophisticated phishing campaigns.

There's an opportunity for organizations to get ahead of the curve to have more resources available to focus on the most pressing AI-augmented threats. Automated cryptography management enables security teams to be more efficient and be able to focus on the never-ending new threats. It is essential to gain a comprehensive understanding of its risk posture, keep up with migration processes to new protocols, and understand that cryptography is an essential part of the digital IT landscape today.

About the Author



Dr. Marc Manzano is General Manager, Cybersecurity at SandboxAQ, where he leads the cybersecurity group. His current research interests include post-quantum cryptography, lightweight cryptography, fully-homomorphic encryption, the intersection between machine learning and cryptanalysis, performance optimizations of cryptographic implementations on a wide range of architectures, and quantum algorithms. He has presented more than 25 articles at international conferences, published more than ten journal papers, and collaborated on several scientific books related to cryptography and computer networks security.

Over the past ten years, Dr. Manzano has led the development of many secure cryptographic libraries and protocols. Dr. Manzano was formerly a Senior Staff Software Engineer at Google, and before that, he was the Vice President of the Cryptography Research Centre at the Technology Innovation Institute, a UAE-based scientific research center. Prior to that, he held several positions where he was responsible for implementing pivotal cryptographic components of a variety of secure communication products, including an electronic voting platform.

Dr. Manzano holds a Ph.D. in Computers Network Security, which he earned under the supervision of the University of Girona (Spain) and Kansas State University (United States). He earned an MSc in Computer Science from the University of Girona (Spain), while he did research stays at UC3M (Spain) and at DTU (Denmark). He initiated his research career while finalizing his BSc in Computer Engineering at Strathclyde University (UK).

Dr. Manzano can be reached on X at https://x.com/marcmanzano?lang=en and on our company website at https://www.sandboxaq.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Securing GenAI Data Requires Sophisticated, Disciplined Practices

By Cloud Storage Security

Since the earliest days of computer science, the concept of garbage in, garbage out (GIGO) has shown the need for data quality. The idea that data output can only be as accurate as the data input continues to be a fundamental tenet of code development. It's become even more important in the world of generative AI (GenAI), which is playing an increasingly significant role in business operations around the world.

Enterprises are scrambling to harness the power of GenAI in hopes of streamlining operations, enhancing customer engagement, and reducing personnel costs. In the rush to adopt a game-changing technology like GenAI, enterprises may be unaware of security risks like data poisoning, hallucination, and even more traditional threats like malware and ransomware targeted at GenAI, which can play havoc with a business. These—and many other threats—require serious attention at the CSO and CISO level before adopting new technology like GenAI. The challenge is how to ensure that security moves at the pace of

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

the business. For most businesses out there today, the focus is on how GenAI can accelerate business, but at a pace that doesn't circumvent security and privacy practices already in place for compliance.

GenAI Basics

GenAI uses huge amounts of data to create and train foundational models that can help to create off-the-shelf applications. Some common uses of GenAI services for enterprises include interactive and personalized customer service systems, content generation for marketing, software development, and individual digital assistants for employees.

These powerful platforms rely on large language models (LLMs) to enable the creation of accurate outputs in response to user prompts. The greatest value from LLMs comes from crafting custom prompts for specific outcomes such as enterprise specific scenarios, customized software platforms or code, or highly specialized writing.

GenAI can also create unique models to perform specific and often complex functions for business or development purposes. These models are regularly trained using proprietary datasets, product information, trade secrets, private or personal data, as well as generally available data. The higher the value of data used to train the model, the better outputs you'll see from your GenAI application – this is where quality in, quality out (QIQO) resonates. Since the outcomes can be highly beneficial, enterprises should consider two important security elements of the process: ensuring the integrity and privacy of output data; and not inheriting any risk from public datasets.

Is Stored Data Clean and Safe to Use?

Threat actors have become successful in finding ways to embed malware into datasets. This malicious code is often designed to remain inactive until it has access to compute resources, opening the door for propagation into secure environments or access to valuable information. Reports of embedded malware discoveries have included code to exfiltrate data, search of personally identifiable information (PII) and other confidential information that could be used for future ransomware or extortion threats. Embedded malware has also been used to alter GenAI outputs, threatening the validity of AI-powered insights and analysis. These threats are real and happening today across platforms that house massive datasets available to GenAI systems and developers.

To complicate this challenge, almost all cloud service providers (CSP) are now introducing GenAI services alongside their infrastructure services. And this makes perfect sense as the cloud is exactly where many developers are building new applications. So, providers like Amazon Web Services (AWS) and Microsoft Azure embed GenAI services into their platform. That is exactly what makes these platforms the perfect target – where else would you be tempted to rapidly adopt a new technology without setting up the proper security guardrails? This is why cloud plus GenAI is increasingly becoming a target - it is where the opportunities lie.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Any enterprise not taking precautions to ensure inputs into LLMs and datasets are clean, and outputs are producing the desired outcome, are putting themselves at risk. And these risks are real and well documented. For further reading, the eBook Securing Gen AI Models: Mitigating Risks and Protecting Your Business discusses GenAI and its data security risks in detail. We believe the proliferation of datasets from GenAI and other business applications is creating another requirement for Zero Trust - this time for data.

Zero Trust, an established practice for network security is based on the premise that you cannot trust any network connection - even from inside your perimeter. Security professionals follow zero trust networking principles by using time-bound credentials, hardware tokens, and enforcing private access even when devices are located in your office, give an additional layer of protection when you can't trust devices. GenAI is now forcing an evolution of that methodology to data.

It all begins with the assumption that any stored data is compromised at some level. Therefore, all data must be scanned for malicious code at every stage or interaction. Every enterprise should take a stance of scanning data, images, objects from all cloud repositories, 3rd party platforms, even off-the-shelf LLMs. And the reverse is true after extracting value from that data. There must be high confidence that any chat-bot, application output, or data feeding into another application, does not contain any sensitive data that should not be exposed. Taking a zero-trust position on all data, regardless of its trajectory to archive or live application, is a crucial step to reduce or even eliminate security threats.

Is Sensitive Data Being Exposed?

In addition to identifying malicious code, you should have high confidence in data content. Data Loss Prevention (DLP) has been considered just an endpoint solution for some time, but similar functions and tools that can scale to the network core and storage systems are available to help to maintain the integrity of confidential information. Loss of control or disclosure of sensitive data can cause regulatory compliance issues as well as placing companies at competitive disadvantages when customer secrets are revealed. These are the headlines every CISO dreads – 'our chat-bot leaked sensitive data that we didn't verify'.

While the search for PII and secrets has been a favorite activity by threat actors for a long time, GenAI increases the risk of exposing sensitive information. If proprietary or sensitive information is included in training data, it is highly likely that it will find its way into derived outputs. Predicting how and where this information could be utilized or exposed would be nearly unachievable, and once it is incorporated into an LLM, it would be impossible to root out and eliminate the threat.

DLP scanning of training data is a critical step in maintaining control of sensitive information. Organizations should consider whether sensitive data should be filtered out of the dataset before training models and as a final precaution, outputs from a GenAI system should always be scanned for sensitive data before they are delivered to end users. Details on how this works can be found in this technical article from Cloud Storage Security.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

A Secure Safety Net

Enterprises should look carefully at GenAI applications alongside their public cloud services to implement a comprehensive safety net for data inputs and outputs. Ensuring that data is clean before it crosses your cloud infrastructure or enters your GenAI pipeline is essential, and securing sensitive information through seamless categorization scans of training data and outputs is crucial to preventing inadvertent disclosures. GenAI should be seen as an awesome business accelerator; not another thing for you to worry about for potential hackers. Before using any business data to justify using GenAI for enhanced returns, make sure the data on the input and output side of the GenAI application is safe by not trusting any of it.

About the Author



Cloud Storage Security (CSS) protects data in the cloud and on premises so that businesses can move forward freely and fearlessly. Its robust malware detection and data loss prevention solutions are born from a singular focus on, and dedication to, securing the world's data, everywhere. Serving a diverse clientele spanning commercial, regulated, and public sector organizations worldwide, the company solves security and compliance challenges by identifying and eliminating threats, while reducing risk and human error. CSS's modern, cloud-native solutions are streamlined and flexibly designed to seamlessly integrate into a wide range of use cases and workflows, while complementing and bolstering existing infrastructure and security frameworks. CSS holds certifications including SOC2, AWS Public Sector Partner with an AWS Qualified Software offering, AWS Security competency, and AWS Authority to Operate.

Find CSS on LinkedIn and YouTube.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Cybersecurity's Shift from Defense to Resilience Against Evolving Threats

By Engin Kirda, Program Co-Chair, ACM CCS 2024, and Northeastern University Professor

As our digital world grows increasingly interconnected, so too do the challenges of maintaining robust cybersecurity. High-profile incidents, such as the CrowdStrike event during the summer of 2024, have illuminated critical vulnerabilities in technology infrastructure and underscored the urgent need for organizations to evolve their approaches. Cybersecurity is no longer solely about defense—it is about building resilience to adapt to and recover from an ever-changing threat landscape.

Drawing on my experience as a researcher and educator in cybersecurity, I've seen firsthand how the complexity of modern digital ecosystems demands innovative and proactive solutions. In this Q&A, I'll share insights into critical issues shaping cybersecurity today, from preventing technological failures and combating ransomware to navigating the ethical challenges of AI-powered defense systems. Through this discussion, I hope to provide actionable guidance on how organizations can strengthen their resilience and remain ahead of evolving threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

1. The CrowdStrike incident brought attention to key technological vulnerabilities in cybersecurity infrastructure. What lessons can organizations draw from this event, and what practices should they implement to safeguard against similar risks?

The CrowdStrike incident demonstrated the importance of researching topics such as secure software updates and the general problem of having homogeneous systems. That is, if many people are using the same solution for a task such as security, and that system fails, everyone may become vulnerable or unavailable at the same time. The CrowdStrike incident was not a security breach, but it did demonstrate how much damage future attacks may create where a product is serving thousands of high-profile customers. For instance, many organizations are highly dependent on cloud services such as GMail or Microsoft Office 365. Hence, if these products were to fail in some way in the future, millions of users and thousands of organizations would be affected. One practice that one could envision here would be to focus on architectures that are more fault tolerant and fail safe in case something catastrophic happens. Software updates should be tested for robustness before deployment, and the dependency between different software products and how they can adversely influence each other should be automatically analyzed. As our computer, software and network systems continue to become embedded into critical infrastructures, all systems should be kept up to date with the latest security patches. This practice will not only protect against cybersecurity threats, but will also maintain reliable performance.

2. Given the increasing frequency and sophistication of ransomware attacks, what do you predict will be the most effective defense strategies in 2025, and how might organizations need to shift their approaches to stay ahead?

Resilient backup strategies remain one of the most effective defenses against ransomware. Offline or air-gapped backups ensure that even if attackers compromise an organization's systems, critical data remains secure and recoverable. But it's not enough to have backups – organizations need to plan for worst-case scenarios by regularly testing their recovery processes. Simulations that assess how quickly systems can be restored after an attack are essential for identifying gaps and ensuring preparedness.

Employee education also plays a critical role in ransomware defense. Most attacks begin with social engineering, such as phishing emails, that exploit human error. Training employees to recognize these threats and understand how they originate is one of the simplest and most effective ways to strengthen security. It only takes one person falling for a phishing attempt to compromise an entire organization. This is why widespread awareness can make a significant difference without adding extra back-end work.

Advances in AI are adding another layer of defense by enhancing detection capabilities. AI systems can analyze data in real-time to identify suspicious activity or ransomware installation attempts, allowing organizations to act before significant damage occurs. By combining resilient backups, proactive planning, employee training, and cutting-edge AI tools, organizations can stay ahead of increasingly sophisticated ransomware threats and build stronger, more adaptive defenses.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

3. As organizations adopt more resilient cybersecurity strategies, what ethical considerations and governance standards do you think will be necessary to guide these efforts, particularly when implementing AI and decentralized systems?

It is clear that we will need answers for AI-based security systems very soon. AI can be great for finding out if a system has been compromised, or if there is a vulnerability in a system that is known, or unknown. However, we will need some humans in the loop to determine if the actions that AI suggests or takes are indeed correct and ethical. For example, imagine if an AI or decentralized system decides, based on its analysis, that a certain country is risky, and in turn cuts off all that country's users. Is this ethical? Also, could this analysis be a false positive because the AI system had a dataset that was incorrect? The overall cybersecurity and technology industry will need to think hard about these questions. In the near future, regulations and governance standards will play an important role in these discussions.

4. Artificial intelligence is quickly becoming a valuable tool in threat detection and prevention. How can AI-powered systems be integrated effectively into existing cybersecurity strategies without becoming overly reliant on them? Are there any potential risks these technologies might introduce?

AI-powered systems have revolutionized cybersecurity by automating the detection of threats and anomalies at a scale and speed that humans simply can't match. However, effective integration of AI into cybersecurity strategies requires balance. While AI can handle much of the heavy lifting, humans must remain involved in the decision-making process to ensure the accuracy and integrity of critical actions.

This doesn't mean organizations need hundreds of people monitoring every AI system at all times. Instead, it's about maintaining strategic oversight – allowing AI to automate routine tasks and flag potential issues, while human experts step in to review and act on high-stakes decisions. This hybrid approach ensures that the system remains both efficient and accountable.

One of the key risks of over-reliance on AI is that it's only as good as the data it's trained on. If the data is biased or incomplete, the system might make flawed decisions, leading to missed threats or false positives. Additionally, cybercriminals are increasingly targeting AI systems, looking to manipulate their algorithms or exploit vulnerabilities.

To mitigate these risks, organizations must focus on regular validation and auditing of AI systems to ensure they operate as intended. Clear protocols should be in place for when and how human oversight is applied, ensuring that critical actions remain grounded in both technological precision and human judgment. By integrating AI as an enhancement rather than a replacement, organizations can harness its full potential while avoiding pitfalls.

5. With modern digital ecosystems becoming more complex, how can organizations identify and address interdependencies in their systems to prevent failures?

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

To stay ahead, organizations need to actively look for these interdependencies by running regular “war game” type of simulations that can show how a failure in one area might cascade through the system and help teams plan for worst-case scenarios.

It’s also important to think about interdependencies from the start, building systems with redundancy and fail-safes baked in. Regularly testing these systems and making adjustments as they evolve can prevent small issues from becoming big problems.

The key here is to make this kind of testing and planning a regular part of operations – not something you only think about after an issue arises. By being proactive, organizations can build resilience into their systems and reduce the risks that come with today’s interconnected digital world.

About the Author



Engin Kirda is a Program Co-Chair of ACM CCS 2024. He is also a professor at the Khoury College of Computer Sciences and the Department of Electrical and Computer Engineering at Northeastern University in Boston. Previously, he was tenured faculty at Institute Eurecom (Graduate School and Research Center) in the French Riviera. Prior to that, he was faculty at the Technical University of Vienna where he co-founded the Secure Systems Lab. The lab has now become international and is distributed over nine institutions and geographical locations.

Engin’s current research interests are in systems, software and network security (with focus on Web security, binary analysis, and malware detection). Before that, he was mainly interested in distributed systems, software engineering and software architectures. Engin can be reached online at ek@ccs.neu.edu and at ACM’s website https://www.acm.org/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Ensuring Security in the Cloud: The Importance of Choosing a FedRAMP-Validated Cloud Service Provider

By Emil Sturniolo, Chief Security Officer at ETHERFAX

In today's digital world, government agencies face increasing pressure to modernize their operations while safeguarding sensitive information. With data breaches, ransomware attacks, and other cybersecurity threats dominating the headlines, maintaining trust and security has never been more critical.

For agencies migrating to a cloud-based solution, selecting a Cloud Service Provider (CSP) with the proper certifications is essential for protecting confidential data and maintaining compliance with federal regulations. The Federal Risk and Authorization Management Program (FedRAMP) has emerged as a cornerstone of cloud security for government organizations, offering a standardized framework to evaluate and authorize Cloud Service Offerings (CSOs).

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

For government organizations, the benefits of choosing a provider that meets FedRAMP requirements extends far beyond compliance. From enhanced security to streamlined processes, FedRAMP offers agencies the confidence they need to embrace modern CSOs without compromising data protection.

Understanding FedRAMP

FedRAMP is a government-wide program created to standardize the security assessment, authorization, and continuous monitoring of cloud products and services. It was established to help government agencies adopt cloud-based products while ensuring that these services meet stringent security requirements.

Achieving FedRAMP compliance is a demanding process for CSPs. CSPs must implement rigorous security controls within each CSO, which includes data encryption, access controls, vulnerability scanning, and continuous monitoring. These controls are evaluated against a stringent set of criteria defined by the National Institute of Standards and Technology (NIST), ensuring that CSPs meet the highest standards of security and reliability (see that latest version of NIST special publication 800-53).

Maintaining FedRAMP compliance is not just a one-time achievement; it requires continuous monitoring and reassessment of the services being provided. This active security posture ensures that CSPs stay ahead of emerging cybersecurity threats as well as evolving federal standards.

The Growing Need for FedRAMP

The shift by government agencies toward cloud adoption has brought unparalleled efficiency and scalability to operations. However, it has also introduced new security challenges. Cyberattacks targeting government agencies are becoming increasingly sophisticated, with adversaries seeking to exploit vulnerabilities in cloud environments that may expose Confidential but Unclassified Information (CUI) and/or disrupt critical operations. FedRAMP was designed to address these challenges by providing a comprehensive framework that reduces risks to manageable levels and ensures agencies can safely leverage CSOs.

FedRAMP also helps eliminate redundancy in security assessments. Without this standardized approach, each agency would have to independently and extensively evaluate the security capabilities of each cloud service provider and their offered solutions — a process that would be very time-consuming, expensive, and inconsistent. By establishing a unified approach, FedRAMP streamlines the adoption of cloud-based solutions across government agencies.

Key Benefits of FedRAMP-Certified Cloud Fax Solutions

For government organizations, selecting a FedRAMP-compliant CSO delivers several critical benefits:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

1. Enhanced Security

A CSO that meets FedRAMP criteria must implement comprehensive security measures that protect against data breaches, unauthorized access, and other cyber threats. These measures include advanced encryption, strict access controls, as well as ongoing vulnerability scans to identify and address potential and emerging risks. Therefore, FedRAMP adoption by CSPs offers assurances to agencies that the selected CSPs prioritize the security and privacy of CUI.

2. Standardized Compliance

FedRAMP establishes a standardized framework for evaluating CSPs, eliminating the need for individual agencies to develop detailed security assessments of each CSO under consideration for use. This standardization not only saves time and resources by minimizing the duplication of effort, but also ensures a consistent baseline level of security across for all government agencies.

3. Increased Trust and Transparency

FedRAMP fosters a higher level of trust between government agencies and CSPs. Cloud service offerings that are certified by an approved independent third-party assessment organization (3PAO) to meet FedRAMP requirements demonstrates that the CSP has undergone rigorous scrutiny and is committed to maintaining the highest security standards.

This trust extends beyond individual agencies to the broader public, as citizens rely on government organizations to protect their data. Working with FedRAMP complaint providers demonstrates a commitment to transparency and accountability in handling CUI.

4. Proactive Threat Mitigation

FedRAMP's emphasis on continuous monitoring ensures that CSPs are always vigilant against emerging cybersecurity threats. This proactive approach helps agencies stay ahead of adversaries and maintain a strong security posture in the face of evolving risks. Continuous monitoring also provides agencies with real-time insights into their cloud environments, enabling them to quickly detect and respond to potential vulnerabilities or incidents.

5. Cost and Resource Efficiency

By standardizing security assessments, FedRAMP significantly reduces the costs and resources typically required to evaluate cloud service providers and their offerings. This streamlined approach eliminates redundant evaluations, allowing agencies to adopt CSOs quickly and efficiently. By minimizing the administrative burden, government organizations can allocate more time and resources to their core missions, driving greater focus on delivering services to the public.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Overall, FedRAMP has become the gold standard for evaluating and adopting cloud service providers, offering a comprehensive framework that prioritizes security, trust, and efficiency. When selecting a cloud-based secure document exchange solution, FedRAMP compliance enables agencies to confidently embrace modern technologies while maintaining the highest standards of security and reliability.

About The Author

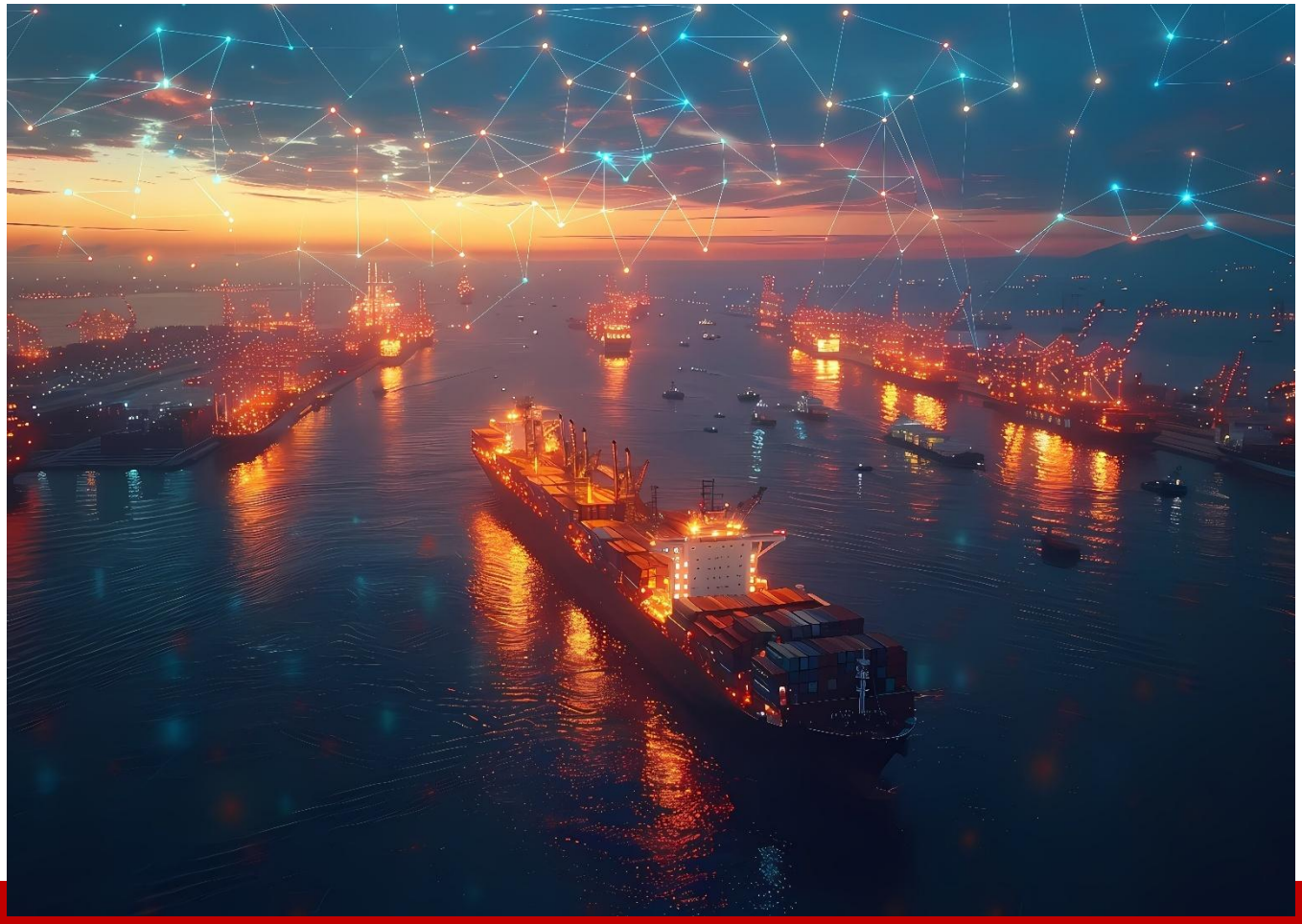


As Chief Security Officer at ETHERFAX, Emil Sturniolo is responsible for managing ETHERFAX's security risks as well as ensuring compliance with industry security standards and best practices. This includes helping ETHERFAX achieve and maintain its PCI DSS, HITRUST and FedRAMP certifications, thus providing ETHERFAX's customers with the confidence that their data will be handled with the utmost care.

Emil is a recognized and respected authority on Internet-based networking and security technologies as he began developing Internet / communications-based solutions in 1981 and worked with many of the original members of the Internet Engineering Task Force (IETF) to develop the Internet into the worldwide computer network it is today. Emil holds over 50 patents related to communications, security, and cryptography, with many more domestic and international applications still pending. Emil's additional responsibilities include overseeing ETHERFAX's Intellectual Property portfolio.

Emil can be reached on LinkedIn and on ETHERFAX's website: https://www.etherfax.net/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Establishing a Cybersecure Maritime Ecosystem

By Sandro Delucia, Product Director, Speedcast

Cyber-attacks happen across all sectors and industries every day. In fact, they are a growth industry expanding 400-500% in the past five years alone. When these attackers succeed, the results can be critical and costly to businesses. A network breach can quickly shut down operations, resulting in millions of dollars in lost revenue and repair work. In 2023, the average cost of a successful cyber-attack was a hefty $4.45 million and total global costs per year are estimated to reach an astonishing $15.63 trillion by 2029.

Anything from a cargo ship to an oil rig can find itself the focal point of a cyber-attack, because hackers will leave no stone unturned in their quest to access a network. Shipping and maritime assets and operations are valuable targets not only because of the value of the cargo onboard, but because of their critical position within an overall supply chain.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

The vulnerabilities in your networks

After years of growing cyber-attacks, most businesses have become adept at protecting 'the front door' of their networks – but all too often, the remote sites used in maritime and other operations are overlooked. For many businesses, these sites represent the Achillies' heel in their overall security make-up. Currently, 24% of business security professionals report concerns about access to their sensitive data through remote sites.

By compromising remote sites, attackers can tunnel straight into the heart of a company's network and gain access to a gold mine of potentially sensitive data. Few remote sites will have IT staff on the premises, which means they are completely dependent on the cybersecurity processes put in place by the wider business.

The critical role of endpoint security

Protecting these remote sites requires *endpoint security*. The endpoints are the laptops, mobile phones and other devices where network flows end. As companies increasingly interconnect their operations, the number of endpoints multiplies.

Protecting these devices is critical because they represent a back door with authorization to access the organization's most sensitive data. Knowledgeable hackers will attack anything from Very Small Aperture Terminals (VSAT) to Wi-Fi, mobile, or fiber connections. Good endpoint security also addresses the human factor that is the hacker's primary target: an employee who accidentally downloads a malicious file onto a device, for example, where it can sit unnoticed as it collects private information before reporting back to an unauthorized user.

Endpoint security is a key part of what cybersecurity experts call 'defence in depth.' It is the opposite of "set it and forget it," where businesses hope a single service will ensure all the necessary protections. It involves real-time protective monitoring and threat mitigation as well as centralised, near-time reporting.

Cybersecurity as a service

The challenge for businesses is to understand which solutions will meet their needs. It is a challenge made more difficult by the constant influx of security products into an already flush market. With so many options, businesses run the risk of selecting a flashy product that doesn't cover all their vulnerabilities through a procurement process that can be both difficult and costly.

The best-of-breed solution today is to use sector-specific solutions that offer cybersecurity as a service. In the maritime sector, for example, we're now seeing smart network management platforms on the market, such as Speedcast SIGMA, which incorporates secure, next-generation firewalls and security policies, while giving users total oversight to what each user has access. These solutions empower businesses with a cost-effective solution which can be used to establish and maintain strong security positioning, even though its main function is to provide seamless, reliable connectivity for their networks.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Designed specifically for remote sites, smart management solutions are enabling operators to ensure the safety and security of their workforce and data flows without the need for stand-alone, cybersecurity-focused products. An industry-leading application like Cydome, for example, can be incorporated into the connectivity management system to enable real-time detection and protection, alongside managed security operations center (SOC) services. These applications run both onboard and at a fleet's headquarters, or in customer-managed virtual machines. The best provides a single dashboard that generates risk scores for each vessel and risk and compliance scores for the fleet. They can also drill down to specific vessel alerts, events, and informational and operational technology (IT/OT) assets.

When applied to smart management platforms, these applications offer that critical defence in depth, including real-time, fleet-wide monitoring; AI-based threat detection, continuous vulnerability scanning, and the latest security information and event management (SIEM) technologies for incident management.

Complying with regulatory requirements

Cybersecurity as a service is also an effective answer to the rise of cybersecurity requirements across the globe. Management teams, insurers, and regulatory bodies are now considering cyber threats with increased seriousness. This has led organizations such as the International Association of Classification Societies (IACS) to launch new and revised regulations, with the aim of tackling cyber-attacks across the shipping and maritime industries.

Take IACS UR 256/257. As of July 2024, these revised regulations require all newly constructed ships, commercial ships of more than 500 gross tonnage, passenger vessels carrying more than 12 people, self-propelled units and drilling rigs working offshore to adhere to new, stringent regulations.

UR E26 focuses on providing a minimum set of requirements for the cyber resilience of the ships themselves. It means vessel inventories must be updated and administered in detail, alongside an analysis of access control across systems. Alarms and testing must also be evident across vessels in order to adhere to the new requirements, representing a significant security enhancement of onboard systems.

IACS UR E27 specifically covers 41 security capabilities relating to onboard device systems and equipment. Some of the main security features that must be implemented include multi-factor authentication, cryptographic algorithms and regular audits. This will ensure a strong line of defence against potential cyber-attacks.

Non-compliance with any of the proceedings outlined by UR E26/27 will result in significant financial and legal penalties, as enforced by another recently revised European Union regulation, the NIS-2 Directive. Companies will be subject to fines up to a maximum of €10 million or 2% of their global annual revenue if deemed to be neglecting these regulations.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Greater vigilance, reduced vulnerability

As harsh as the regulations and penalties may appear, their aim is to create a state-of-the-art cybersecure maritime ecosystem. Decision makers must now find the best way to ensure compliance while balancing the investment cost and benefit.

The maritime industry has been considered a soft target for hackers, where remote devices were weakly defended from external attack and offered an open road into the enterprise network. Cyber risks once seemed limitless, daunting, and without a cure. But in reality, they are much like the risks of every voyage: manageable, as long as vigilance never ceases.

About the Author



Sandro Delucia is a Product Director at Speedcast. He has over twenty years of international experience in Telco and Satellite Communications and has worked extensively in the sphere of Product Management on complex MSS and VSAT projects and solutions. He is actively engaged in driving Speedcast's standard, and bespoke solutions with an emphasis on driving intelligent edge, operational and cloud solutions, and is continuously seeking innovative ways to enhance customer experience and value derived from customized IT and connectivity solutions.

Sandro can be reached on LinkedIn at https://www.linkedin.com/in/sandro-delucia-b3566a1/ and at our company website https://www.speedcast.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Prevent Cyber Attacks with Deepfake Detection Technology - A Complete Guide

By Ryan Jason, Facia.ai

Today, we live in a technologically controlled world where organizations employ digital services for everyday operations. Now, companies onboard users and partners remotely through an online process. They utilize digital processes and allow remote access to the platforms. Digital processes made it easy to have streamlined working operations. However, they also made organizations vulnerable to criminal attacks. With the help of machine learning technology, fraudsters generate spoofed data to utilize for bypassing securities. Neural networks allow them to generate deepfakes that are difficult to identify through the human eye. Hence, there is a need for the most appropriate solution, such as deepfake detection technology, to secure organizations from cybercrimes.

What are Deepfakes? - An Overview

Deepfakes are complex media that are generated with the help of neural networks and machine learning technology. It is difficult to identify deepfakes with simple security methods. Cybercriminals utilize complex and advanced strategies such as deepfakes to perform illicit activities. Many scammers contact higher-level firms with deep fake audio and videos that cannot be identified without advanced security

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

protocols. Deepfake detection technology is another side of artificial intelligence that is used as a preservative and security from the same technical problems such as spoofed data and fake videos.

Nowadays, companies establish remote partnerships and onboard customers digitally. They often fall prey to cyber criminals for using weak security. Fraudsters have learned to dodge security methods. They reach out to organizations for data breaches, financial terrorism, and money laundering. Hence, there is a need for appropriate technology to prevent fraud attacks within the organizations.

How Do Criminals Generate Deepfakes?

Deepfake creation is simple, but it is the product of complex techniques that involve artificial intelligence and neural networks. Initially, a large amount of data is collected from individuals, which has to be replicated. This data involves images, videos, and the voices of a specific person. Then, algorithms are trained and commanded to replicate the identity of an individual. A synthetic media is generated with the help of artificial intelligence. This media can be in the form of audio, videos, and images.

Criminals generate a deepfake of well-known business owners and use them to approach various organizations in the name of investments and partnerships. Companies that do not utilize up-to-date security measures are vulnerable to cyber crimes.

Why is Deepfake Detection technology Necessary to Utilize?

Deepfake detection technology is necessary to combat prevailing fraud attacks. It is necessary to have up-to-date security methods to identify various kinds of synthetic data. Without deepfake detection technology, companies cannot identify fake audio and videos that are generated through artificial intelligence. There are various examples of cyber-attacks which are the result of deepfake generation.

In 2018, US President Barack Obama underwent deepfake attacks. His video came in from which he was delivering a message that he never said. Later, with the help of detection technology, it was determined that it was a fake video. It was a deepfake video that was created by actor Jordan Peele in collaboration with BuzzFeed CEO of BuzzFeed.

The above example showed that even political celebrities are not secure from deepfake attacks. Once, a company got a voice call from its CEO to share a specific amount to a specific bank account. Later on, they identified that his CEO had not called, but it was a deepfake. This is how scammers utilize deep fake technology for cyber attacks.

Many criminals utilize deepfake technology to generate videos of big investor companies' CEOs. They use these videos for video interviews and discussions to reach networks for heavy financial losses.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

What are Deepfake Detection Solutions?

There are various deepfake detection solutions that companies use to prevent cyber attacks. However, there is a complete service designed for deepfake prevention, and it is deepfake detection technology. It involves the usage of biometric face verification technology and various other interrelated steps to validate data before onboarding specific entities. The face verification process within the deepfake detection technology involves machine learning technology to verify facial data. It verifies the complex facial nodes, including muscle stretching, skin patterns, and various other features, to identify the nature of the media presented.

Companies can utilize automated deepfake detection technology to verify entries in real time for a secure business landscape. It helps to eliminate cyber attacks and prevent fraud in organizations.

Final Words

Deep Fake detection technology is necessary to utilize for a secure business landscape. It works through neural networks and verifies user IDs for real-time security from cyber attacks. This technology involves automated checks and various steps to identify the nature of data. Hence, organizations utilize biometric face verification services as deepfake prevention solution. However, a complete process of deepfake detection technology involves facial verification along with other steps to identify the nature of data.

About the Author



Ryan Jason is a Technical Content Writer who's been writing about Cyber Security, Blockchain and Cryptocurrencies for over 3 years. His mission is to draw people closer to cyberspace by providing them with actionable and helpful content. He has a wide variety of writing experience in the Artificial intelligence, Blockchain, BigData, FinTech, Crypto, DeFi, Ethereum, and Cybersecurity sector.

Ryan can be reached online at ryanjasonn191@gmail.com and https://www.linkedin.com/in/ryan-jason-a87b381b7

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Cybersecurity Changes Companies Should Be Considering for 2025

By Marcelo Barros, Director of Global Operations — Hacker Rangers

As companies develop their goals for 2025, they should definitely include “improve our cybersecurity framework” at the top of the list. Considering the rate at which attacks are increasing, this should be a priority. Recent reports reveal that ransomware attacks in North America grew by 15 percent in 2024, with 60 percent of businesses saying they were targeted by such attacks.

The good news for businesses is that a few simple steps can significantly improve their security stance. The following are the primary steps businesses should consider taking.

Enforce multi-factor authentication

As it became clear that traditional passwords were no longer enough to keep networks safe, multi-factor authentication (MFA) was promoted as the next level of security. MFA is “password plus,” adding additional steps to the verification process.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

While most companies acknowledge MFA as an essential part of an effective security framework, requiring consistent use is less common. Reports suggest companies are hesitant to mandate MFA because of productivity concerns, with one from CoreView finding that even "78 percent of Microsoft 365 admins don't use MFA" and are "unmindful of security and data governance protocols and lack basic security protections."

Completing the MFA process takes extra time and typically requires having a second device, such as a mobile phone, on hand. Yet even when employees understand its importance, organizations must actively encourage and guide them to enable it.

Another issue frustrating MFA implementation is the ever-increasing use of third-party platform providers. As companies rely more on these providers, they limit themselves to the security measures they are provided with.

Companies that have communicated the value of MFA without requiring it should consider making it mandatory in 2025. This could involve training employees on the topic, encouraging them to implement it, and guiding them through the steps that enable it. It's also essential to require third-party vendors to implement MFA within their systems, ensuring consistent security standards across all aspects.

Provide human-centric cyber hygiene training

Keeping cybersecurity systems healthy requires regular, comprehensive cyber hygiene. Starting 2025 with refresher training on cyber hygiene will help employees remember the role they play, the practices that are important, and the consequences of letting cybersecurity slip.

The following are some key elements to include in cyber hygiene training:

- Update passwords regularly and ensure a strong combination of numbers, letters, and symbols that are unique for each platform.
- Stay up-to-date on the latest attack schemes.
- Use secure connections, especially for remote workers and those who access work networks from public locations.
- Conduct regular backups to minimize the impact of malware attacks and other breaches that threaten to steal companies' critical data.
- Alert security departments immediately if you suspect an attack is occurring.

To optimize the impact of training, companies should ensure programs are human-centric. Taking a "one-size-fits-all" approach won't give employees the motivation or the information they need to effectively play their part in security efforts. Instead, companies should consider the unique needs and activities of all of their employees when developing training.

Human-centric systems consider skill level as well as function when presenting training. They also strive to make training more user-friendly. Leveraging simulations, gamification, and role-playing exercises can

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

make training more user-friendly and engaging and help companies identify knowledge gaps they need to address.

Ensure the security of software and systems

In many ways, cybersecurity is a contest between black-hat hackers and software developers to see who can identify system vulnerabilities first. When developers win, they issue security patches to address the vulnerabilities. When criminals win, they exploit the vulnerabilities to gain unauthorized access.

That said, businesses can only benefit from developers' work to address vulnerabilities if they focus on updating software and systems as often as possible. By deploying new security patches as soon as they become available, businesses ensure they have the most substantial security framework available.

A "security-by-design" approach to software development significantly improves this area of cybersecurity. This approach addresses security concerns during each phase of software development and support rather than treating it as an afterthought or add-on. Companies seeking to leverage "security-by-design" software should look for platforms with secure coding practices, threat modeling, and continuous security testing.

"Security-by-design" can also guide a company's overall cybersecurity strategy. Consideration of cybersecurity as a key to all of a company's processes, from onboarding to vendor selection to change management and more, maximizes its effectiveness. The most secure companies will have a "security-by-design" culture that all employees understand, value, and support.

Adopt a proactive approach to cybersecurity

Cybersecurity statistics clearly show today's cyber attackers are tireless and relentless. Some studies suggest, for example, that 3.4 billion phishing emails are sent daily. To stay safe, companies must take a proactive approach that anticipates and addresses the ongoing barrage of attacks.

A recent study found that human risks are involved in 74 percent of data breaches. Identifying and mitigating human risks is central to shifting to a proactive stance, as it involves exploring how employees interact with systems and the vulnerabilities they may be inadvertently creating. Mitigating risks requires building a strong security culture that promotes security awareness and fosters open communication about security concerns.

Cyber attacks are an operational risk that today's companies must prepare for, regardless of their size or industry. By taking a proactive approach that puts security at the center of operations and effectively equips all employees to play a role, companies can increase their chances of repelling attacks and avoiding costly consequences.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



Marcelo Barros is Director of Global Operations of Hacker Rangers, and an IT veteran who has played an instrumental role in delivering cutting-edge cybersecurity solutions and services to clients around the world. His passion for cybersecurity led him to join the team at Hacker Rangers, a leading gamification company that makes cyber awareness fun and engaging for organizations worldwide.

Marcelo can be reached online at https://www.linkedin.com/in/marcelonunesbarros/ and at our company website https://hackerrangers.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Silent But Deadly

The True Impact of Unknown & Unmanaged Assets on Network Security

By Wes Hutcherson, Global Technology Evangelist, runZero

The global average cost of a data breach in 2024 stood at an all-time high of around $4.88 million, an alarming figure expected to grow this year in line with the 10% annual increase seen last year. As well as the ensuing expenditure needed to rectify the organizational impact of an attack, the true cost of a security breach extends far beyond the financial toll. With threats proliferating, costs of a breach rising, and the regulatory environment tightening in turn, organizations must understand how to pivot if they are to adapt and thrive in a volatile cybersecurity threat landscape. In order to do so and ensure all bases are covered, comprehensive infrastructure visibility is vital. As the old adage goes, you can't protect what you can't see.

With over 60% of connected devices invisible to defenders and unmanaged assets being linked to 7 out of 10 breaches last year, unknown assets pose a considerable hurdle to achieving complete levels of visibility and network security. These latent devices—ranging from decentralized IT systems to IoT and OT devices— are extremely hard to identify and secure and can't be picked up by traditional discovery

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

and vulnerability scanning tools. This gap in coverage then creates blind spots, making it difficult for security teams to see the full picture and detect and respond to threats effectively. Here's how serious it is getting at the highest level:

- Flax Typhoon (China) hijacked 200,000 IP cameras for their campaigns.
- Sandworm (Russia) manipulates industrial control systems with precision.
- Elfin (Iran) targets industrial systems to disrupt operations and gather intel
- Lazarus Group (North Korea) zeroes in on IoT and OT to exploit vulnerabilities

In IoT and OT environments, the prevalence of unmanaged and unknown assets is higher than traditional IT infrastructure due to the nature of these systems. Many IoT devices, such as smart thermostats, medical devices, and industrial control systems, are often deployed without proper security measures and can be difficult to manage and monitor, creating a larger attack surface and extending the likelihood of cyberattacks. With the increasing convergence of these systems with enterprise networks, IoT and OT devices serve as ideal jumping-off points to other parts of the network, allowing attackers to act fast as soon as weaknesses are identified – 72% can find and exploit a vulnerability in a single day. Once inside, attackers are often able to evade detection due to an organizations' limited visibility, allowing them to bide their time and strike when the opportunity to steal sensitive information and demand hefty ransomware payments presents itself.

In order to fortify their networks, security teams must develop strategies specifically tailored to discovering and securing unmanaged assets within their respective environments and establish a thorough understanding of the attack surface as a whole—every single device, system, and asset attackers could use to get in.

A larger portion of the IT budget must be allocated to identifying and cataloguing all IoT and OT devices—including those unknown or unmanaged that may be hidden within the network. This approach will enable CISOs to gain a clearer understanding of their attack surface through knowing what they have and where it's vulnerable, allowing organizations to take informed, focused action.

Even as security awareness training and controls improve, no system is impenetrable, but a clear picture of the entire environment is an invaluable asset when establishing a comprehensive risk management framework. This process begins with detailed discovery. Traditional discovery tools are simply not built for these environments. They rely on aggressive scanning techniques or authenticated access, which can destabilize sensitive devices or miss them entirely, especially since the network status of IoT and OT fluctuates with regularity.

What organizations need is a careful, continuous discovery process—one that's sensitive enough not to disrupt operations but robust enough to provide a complete picture of the environment. This consists of identifying all connected assets, uncovering vulnerabilities, and remaining alert to new assets or changes that might threaten an IT framework. CISOs must then evaluate the precision and speed at which they can address emerging risks by mapping potential lateral movements of attackers across the network. This includes prioritizing fixes based on the criticality and exposure of systems, and establishing a clear view of the network to enhance segmentation and detect suspicious communication patterns

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Discovery is only the first step. It has to be an ongoing process of not just identifying the devices, but understanding their exposures, connections, and convergence points between IT, OT, and IoT systems in detail. These devices often serve as jumping-off points for more sophisticated attacks, so prioritizing based on their criticality and connectivity is absolutely essential.

Organizations need to move away from fragmented approaches. Sprawl is overwhelming security teams—too many tools, too many integrations, and too much noise. While integrations are useful, they're often just stitching together disparate systems, which can subsequently lead to duplication of data, discrepancies, and missed insights. What's really needed is a consolidated approach that combines discovery and exposure management in one platform, with native capabilities that reduce complexity and provide actionable insights.

It's not just about stopping the attacker at the front door anymore—it's about knowing what they could target, blocking them from getting a foothold, and shutting down their pathways if they are successful in their attempts to slide in. In the event of a breach, attack surface visibility helps teams respond faster. With detailed asset data, organizations can pinpoint compromised systems, track how the attacker got in, and shut it all down before things get worse. Knowing where they might go—and exhausting all options to ensure they can't get there—is critical to safeguarding the network.

About the Author

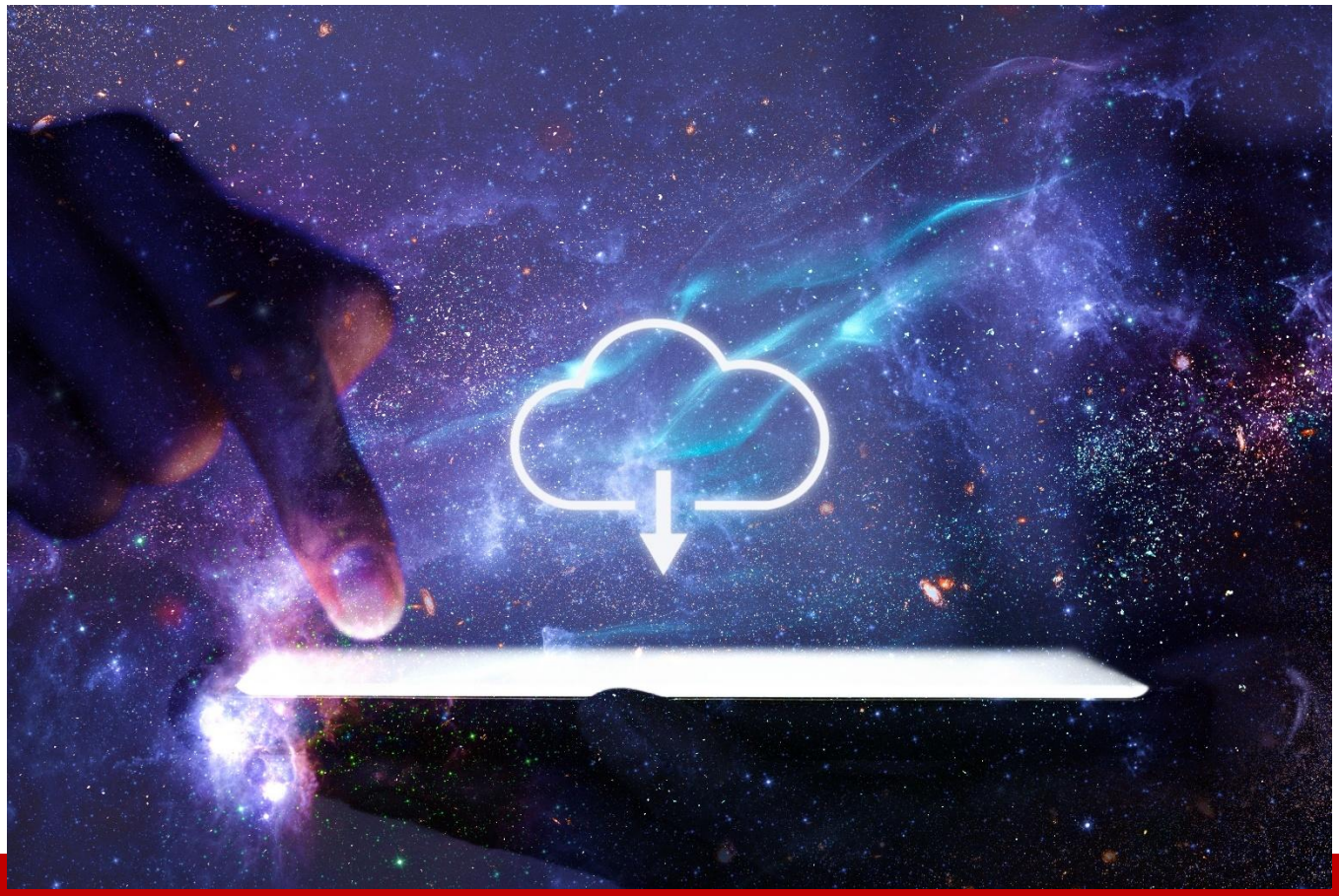


Wes Hutcherson is the Global Technology Evangelist at runZero.

With 16 years of experience in the technology and cybersecurity landscape, Wes has established himself as a seasoned expert in Total Attack Surface & Exposure Management. Wes's deep expertise extends to Managed Detection and Response, and Offensive Security, areas where he has not only excelled but also shared his knowledge through public speeches, educational series, and published articles and studies.

Wes Hutcherson can be reached online via LinkedIn and at https://www.runzero.com/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Cloud Security Playbook Safeguarding Data in The Digital Era

By Hardik Shah, Software Engineer, Microsoft Corporation

As organizations increasingly rely on cloud apps and services and store more data, implementing proper practices and processes is essential to mitigate risks such as unauthorized access, data leaks, and compliance violations. Organizations can help avoid these challenges by adopting several best practices, including data encryption, zero-trust architecture (ZTA), regular compliance and security audits, scheduled backups, ongoing training and education, third-party checks, and dedicated maintenance.

As technology evolves, so does the sophistication of hackers. Today, if a company's security is breached, those with a great deal of financial or personal user information are more prone to ransomware if robust security practices are not already in place. This is why regulations such as the California Code of Civil Procedure (CCP) and the General Data Protection Regulation (GDPR) require many companies to protect users' data better, and if they don't, they are subject to heavy fines. In addition, customers are likely to stop trusting an organization, particularly financial institutions or healthcare organizations, with sensitive, personal data once its system has been breached.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

According to the Hiscox Group 2024 Cyber Readiness Report, nearly half (47 percent) of affected businesses reported difficulties attracting new customers following a cyberattack, more than double the rate reported the previous year (20 percent). Additionally, 43 percent of companies lost existing customers (up from 21 percent), and 38 percent suffered negative publicity (up from 25 percent). “Businesses invest years and significant resources to build their reputations, only to see them compromised within minutes during a cyber-attack,” said Hiscox Chief Information and Security Officer Eddie Lamb. “Continuous cyber education and awareness across all levels of an organization are essential to maintaining security.”

To maintain trust with customers and stakeholders, it’s crucial for companies to safeguard data integrity. While no system is 100 percent foolproof, recognizing some of the main ways hackers can access data is the first step in correcting them. Methods include accessing systems through stolen credentials, non-compliance with GDPR or CCPA regulations, insufficient encryption, weak passwords, and vulnerabilities in third-party integrations. Today’s hackers can even track keystrokes to access data.

One issue that has wreaked havoc in companies is leaks due to weak authentication because of misconfigured cloud storage or apps that have allowed hackers to retrieve company data through access to admin privileges. This huge vulnerability was made evident in March 2019, when Capital One Bank was the victim of a significant cloud data breach due to misconfiguration, and the company was hacked by a former Amazon Web Services (AWS) employee. The institution was forced to pay out $190 million to customers whose data was stolen and an $80 million fine for not undertaking a thorough risk assessment before moving its operations to the cloud and not rectifying the issues promptly.

Similar breaches occurred at other major companies that were found to be negligent when securing their cloud storage, including T-Mobile in 2021 and Apple also in 2019. These breaches highlight the need for more robust security guardrails, particularly as a Gartner survey predicted that more than 95 percent of digital workloads will be deployed in cloud computing environments by 2025.

A proactive approach

While these examples are disconcerting, on the positive side, there are several approaches companies can use to shore up their security and proactively identify potential vulnerabilities. Various third-party vendors or services can help companies look at their infrastructure and how they handle their security. They provide audits and compliance reports, delineating what new systems should be implemented, what needs to be improved, and what is outdated. For smaller companies, Amazon Web Services (AWS) security hub and inspector and Microsoft Azure’s (MSFT) defender for cloud have built-in tools to detect potential security issues that can be run internally through a company’s IT department.

There are also a variety of monitoring systems, including intrusion detection systems (IDS), security information and event management (SIEM), and data loss prevention (DLP). These programs log access into systems and allow companies to reverse engineer breaches to discover what credentials were utilized in the hack and potentially determine which people were involved.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Never trust, always verify

The tools employed by each company are necessarily driven by the organization's size, budget, and sensitivity of information in its possession. A robust system employing ZTA is key. Working on the premise "Never trust, always verify," ZTA ensures that no company's systems or workers are automatically trusted. ZTA demands continuous evaluation and verification through various protocols, including implementing multifactor authentication for identity verification through Identity and Access Management (IAM). This allows companies to determine which employees have permission for specific functions and ensures that nobody can access everything by default. Additionally, IAM can create timed permissions that can be set to expire every few months or even every few days. Organizations can also ensure they use real-time backup solutions that incorporate disaster recovery with encrypted data at rest using programs such as the advanced encryption cipher (AES)-256 and in transit using a protocol like transport layer security (TLS), so the data is always protected.

One of the most cost-effective methods to secure data is employee training via in-person sessions or training videos that address best practices, including reminding workers not to share data. Companies can also use practical methods with workers by sending a simulated phishing attack to see which employees fall for them and then explain how to spot these in advance. In that vein, companies can also ensure they are using sophisticated email clients with built-in phishing detectors.

With the rise in hackers accessing entire security systems, it's crucial for employee training to be one of the first and strongest lines of defense. Companies can address potential breaches by determining which employees have access to which data and training them on what to monitor. Vigilance and adoption of ever-sophisticated tools will assist companies in thwarting hackers and quickly determining when their systems have been hacked and how to prevent further issues.

Disclaimer: The views expressed in this article are those of the author and may not represent the opinions of his employer.

About the Author



Hardik Shah is a Software Engineer at Microsoft Corporation, where he works in research and development for Microsoft OneDrive Sync. He is responsible for developing and maintaining sync algorithms using *C*++ and led a project to migrate 300M+ live users by developing migration sync algorithms, ensuring data integrity and security. Hardik holds patents in the space and has also contributed to the development of MyCase Drive. He holds a bachelor's degree in computer engineering from the University of Mumbai, India, and a master's in computer science from Northeastern University in Boston, Massachusetts. Hardik can be reached at shardik95@gmail.com on LinkedIn and www.microsoft.com.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Strengthening Cyber Crisis Response Through AI

By Haris Pylarinos, Founder and CEO of Hack the Box

The evolution of the threat landscape means the nature of cyber resilience is shifting. Attacks are becoming more sophisticated, and more frequent. This requires greater coordination across an entire organization to remain sharp and adaptive to successfully mitigate and respond.

October's NCSC Annual Review 2024 from the UK outlined the significant opportunities presented by AI, but equally the role that the technology has in transforming cyber threat. We're likely to see 2025 follow a similar path. A core channel for effectively managing escalating risk is to assess organizational preparedness.

Budget constraints and time constraints, coupled with a lack of realism and intensity, limit the effectiveness of traditional assessment formats, including tabletop exercises (TTXs), in handling bad actors' complex tactics. It's no longer sufficient to solely be reactive.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

To progress, we must unite disparate business units as one, arming the C-suite alongside technical front-line teams with proactive training around real world scenarios. Here we can boost cyber agility and response for entire organizations.

AI-powered upskilling, including modern TTXs, can enhance preparedness across entire organizations and strengthen control of businesses throughout the full cyber crisis cycle.

Traditional limitations

Tabletop exercises have been a staple in cybersecurity crisis preparedness for decades. They provide a controlled environment where teams can come together and walk through breach scenarios, practice their responses, and develop crisis management plans.

However, these exercises are inherently limited. They are time-consuming to produce, resource-intensive, and static in nature, often failing to replicate the true chaos of a live cyberattack. They also fail to account for the latest attack methods, including those most likely cause a breach, and to be tailored to the specific needs of an industry or organization.

Facilitator and participant bias and a narrow focus further constrain their effectiveness, leaving critical gaps in crisis preparedness.

In today's threat landscape, where attackers are able to innovate rapidly, the need for a more dynamic and scalable solution is evident. Crisis management must encompass the full spectrum of an organization's workforce, from technical specialists to non-technical teams and decision-makers, to ensure preparedness at every level.

AI-Powered Simulations

The next evolution in cyber crisis preparedness is the integration of AI-powered simulations. These simulations, in contrast to standard generative AI models, are purpose built to enable the creation of real-time, highly tailored scenarios. They adapt dynamically to deliver an unparalleled level of realism and complexity.

By analyzing vast datasets of historical cyber incidents, AI generates scenarios tailored to an organization's specific risks, infrastructure, and industry challenges.

Unlike traditional exercises, these simulations are action-based and evolve in real-time, introducing shifting attack vectors, sudden failures, and external threats. This forces teams to adapt under pressure, strengthening prioritization, decision-making, and cross-departmental collaboration.

AI not only enhances realism but also customizes training to suit varying skill levels within an organization. From entry-level employees to senior executives, each participant engages with challenges calibrated to their expertise, fostering a unified response capability.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

In this format, AI acts as a force multiplier, sharpening an organization's resilience and keeping teams ahead of increasingly sophisticated adversaries.

Learnings Beyond the Table

AI-powered crisis simulations have a shelf life far beyond the exercise itself. Post-simulation debriefs and analyses provide actionable insights that highlight strengths, identify weaknesses, and offer tailored recommendations for improvement, aligned with industry-leading standards and the latest threat landscape.

This feedback loop drives continuous learning. By tracking trends in team performance, AI identifies patterns and informs broader strategies, ensuring that lessons from each simulation are embedded in future planning.

The result is not only better crisis response but also a proactive approach to long-term resilience. The debrief process considers an organization's unique dynamics, such as communication structures and cross-functional alignment.

This ensures that the insights gained are directly applicable, empowering businesses to refine their strategies and enhance collaboration across all levels of the organization.

Addressing the Skills Gap Through Leadership

The UK government's recent cyber security skills report identified persistent skills gap in cybersecurity remains a prevalent challenge for cyber resilience. Organizations continue to face barriers in recruiting professionals capable of addressing the increasingly complex nature of cyber threats.

However, this gap isn't confined to technical expertise. It extends to leadership, where decision-makers are often unprepared for the high-stakes demands of crisis response. Bridging this divide requires cohesive leadership and a proactive investment in workforce development plans.

The C-suite must champion cybersecurity as a core business priority, aligning technical expertise with strategic decision-making. AI-powered simulations offer a unique advantage here, providing scalable, role-specific upskilling that integrates technical teams with leadership.

These simulations bridge the gap for hands-on learning, by sharpening technical skills while enhancing strategic decision-making. This dual focus equips businesses to address the challenges of both immediate cyber crises and long-term resilience.

By embedding cybersecurity into every facet of the organization, from frontline teams to the boardroom, businesses can develop a culture of continuous upskilling and adaptability.

This unified approach not only strengthens response capabilities but also ensures organizations are future-ready in an era of escalating cyber risks.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author



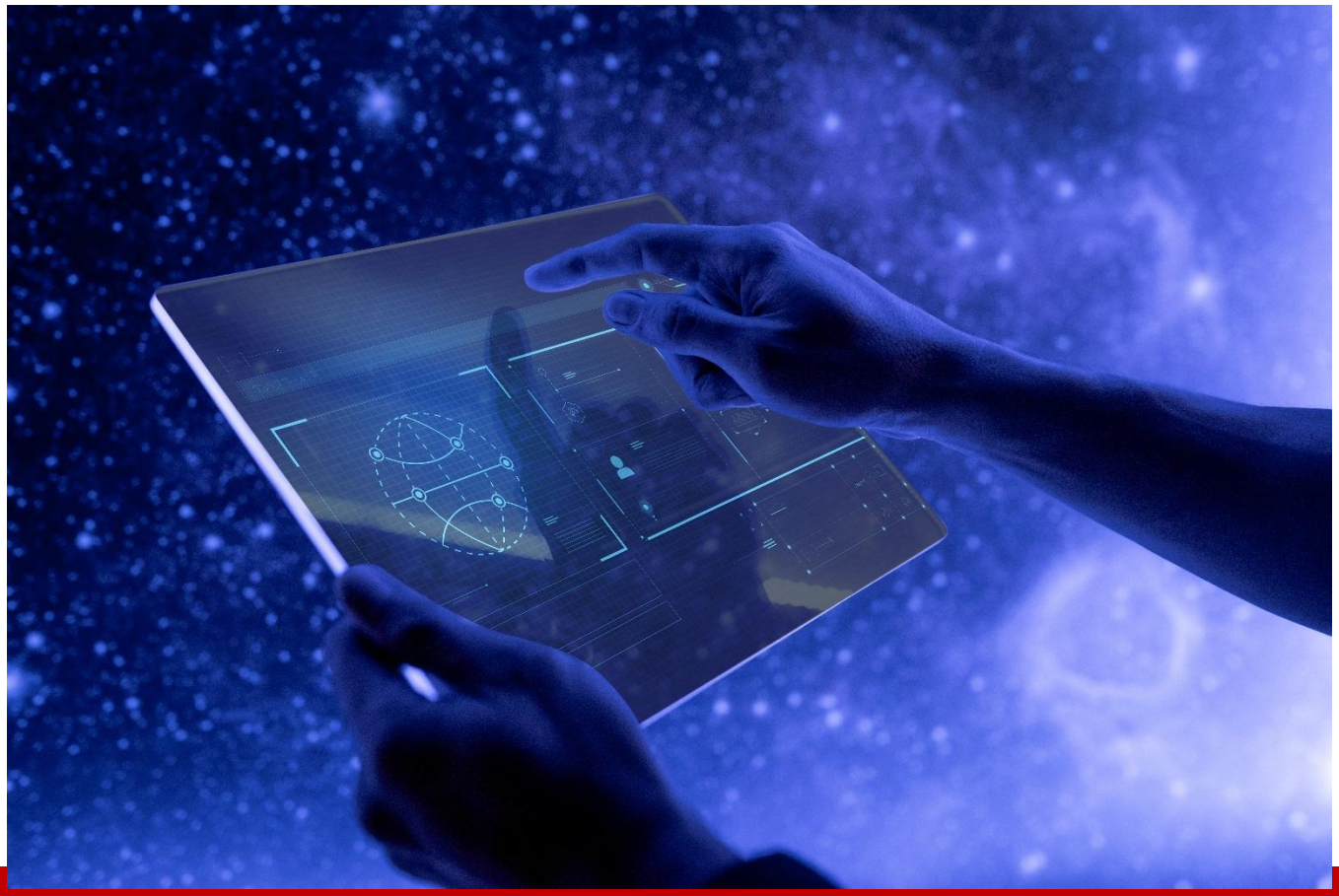
Haris Pylarinos is the Founder and CEO of Hack The Box. With a vision to connect and upskill the cybersecurity community worldwide, Haris disrupted the industry by introducing Hack The Box to the world, and its innovative holistic 360º approach to cyber workforce development, assessment, and recruitment.

Leading the company's expansion worldwide, Haris has been managing to grow Hack The Box exponentially. Under his leadership, the team scaled to over 260 employees and over 3 million platform members since its launch in 2017.

In addition to his role at Hack The Box, Haris has over 15 years of experience and expertise in cybersecurity and systems engineering. He also possessed a strong background in Networking and Software Architecture.

Haris can be reached online at https://www.linkedin.com/in/hpylarinos/ and at our company website https://www.hackthebox.com/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Three Emerging Cybersecurity Trends Shaping 2025

Exploring the Three Trends That Could Prepare Your Organization for the Next Cyber Attack

By Adam Finkelstein, SVP of Global Client Leadership at Sygnia

Stepping into the first months of 2025 has made it abundantly clear that preparation is the key to mitigating the impact of a cyber attack. The previous year highlighted how threat actors have become increasingly bold, leveraging new technologies and methods to exfiltrate, disrupt, and take financial advantage of organizations from all industry verticals. In fact, the average financial cost associated with data breaches in 2024 was the highest on record at $4.88M.

Attacks from the likes of Velvet Ant and Salt Typhoon have shown how vulnerable organizations are to a cyber attack. As data breaches, phishing campaigns, ransomware attacks and more continue to dominate headlines, we asked experts across Sygnia to share their key observations defining the cyber threat landscape, the tactical challenges and how organizations can address emerging threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

AI is Redefining the Cyber Threat Landscape and Demanding Organizational Readiness

The rise and accessibility of AI solutions enables threat actors to develop new attack methods and refine existing approaches. Over the next two years, the National Cyber Security Centre expects AI solutions to increase the volume and impact of cyber attacks.

“Ransomware threat actors can now craft compelling operational campaigns at the push of a button to dupe the more cyber-savvy individuals,” said Karin Lagziel, Director of Cybersecurity Services at Sygnia. “From phishing, smishing and quishing tactics through to deepfake videos and audio, threat actors are deploying far more evasive techniques to attack and cripple organizations.”

Additionally, rapid adoption of complex AI models without proper understanding of the security implications has expanded attack surface and vulnerabilities. Furthermore, with more than 60 elections in 2024 alone, the misuse of AI was rife and is expected to continue to be used by nation-state threat actors as a way to disrupt political narratives. Looking ahead, organizations will need to increase their visibility and ability to detect AI threats, secure their AI models, and train their workforce to navigate this evolving threat landscape.

Navigating the Fine Line on Intrusive Security Tools

For many organizations, intrusive security tools have become a cornerstone to their cyber preparedness and protection strategy, but they can also present complications with the potential to compromise and inhibit critical IT infrastructure. Recent service disruptions, such as the CrowdStrike incident that impacted organizations across the globe, accent the risks associated with tools that require deep levels of access to your IT infrastructure. This is particularly noteworthy for operational technology (OT) environments where uptime is crucial.

“In 2025, organizations will begin to re-evaluate and address this challenge through several strategies,” said Ilia Rabinovich, VP Cyber Security Consulting at Sygnia. “Helpful implementations that strengthen cybersecurity posture with intrusive tools include robust testing, deployment and disaster recovery processes, tailoring security controls to different assets, applying defense-in-depth, and fostering closer collaboration."

Looking ahead, organizations would benefit from identifying their security requirements and how new and existing tools can be leveraged effectively without compromising operational stability or security intrusiveness.

Emerging Threats Will Require Greater Industry Collaboration

The emergence of increasingly complex tools and attack methods highlights the importance of industry cooperation in 2025 and beyond. Recent rule and regulation changes across the

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

cybersecurity ecosystem point toward a commonality – the necessity to build strong partnerships to clearly define global security standards, share key research on emerging threat actors and discuss new strategies to combat the dynamic threat landscape.

“As threat actors leverage new tools and methods to target enterprises to exfiltrate critical data or disrupt services, the cybersecurity community must come together and pool resources to mitigate against the threat of complex cyber-attacks,” said Amir Becker, Senior Vice President of Global Cyber Services at Sygnia. “Organizations must work together to develop standardized frameworks, share compliance tools, and streamline reporting mechanisms to address global regulatory challenges. “

Navigating the year ahead

2025 will test organizations and their cyber security preparedness. As new technologies continue to emerge and shake up both defense and attack strategies, preparing your organization for the next cyber attack will be critical to reducing response time and mitigating the impact of your organization’s reputation and assets. Looking ahead, security strategies will need to adapt, ensuring that both IT teams and decision makers have a comprehensive response strategy, implement the right tools and collaborate among industry peeps to bolster their cyber security posture.

About the Author



Adam Finkelstein serves as the Senior Vice President of Global Client Leadership at Sygnia. With more than two decades of expertise in directing business development and overseeing extensive security initiatives on a global scale, Finkelstein advises clients worldwide, including numerous Fortune 500 and Global 2,000 companies. In his role, he oversees all aspects of Sygnia’s client development, working hand-in-hand to proactively enhance their cyber resilience and thwart attacks within their networks.

Adam can be reached online at LinkedIn and our company website https://www.sygnia.co/

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Next Y2K Is Closer Than You Think

25 years later, software security has a lot to learn

By Paul Davis, Field CISO, JFrog

As we reflect on the 25-year anniversary of Y2K, it's easy to view the lead-up to December 31, 1999, as anti-climactic. Thanks to the hard work of IT professionals and developers, what could have been a global disaster was averted, as we were fortunate to foresee the problem in advance. Yet, 25 years later, some of the lessons learned from that event now need to be applied to software-defined applications.

When you reflect on the 1999 Y2K-scale event, one can see that we are all facing "Y2K" threats nearly every day now - particularly with increasing numbers of critical vulnerabilities exposures and the coming age of AI in the world of software development. In this new environment, it's important to remember the lessons learned from Y2K, and try to anticipate our next major "Y2K-scale" event to implement these learnings.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Years of "Mini-Y2K" Moments

There are tremendous benefits to the software advancements made in the last 25 years. Work flows have improved, device capabilities are rapidly advancing, bugs can be corrected in a matter of hours vs. days or weeks, etc. As such, society has grown almost entirely reliant on properly functioning software to live. Unfortunately, it is that reliance that has the power to bring the world to a standstill if critical software vulnerabilities are exploited.

In the last four years, there have been a couple of notable moments that had the power to replicate what we feared would happen during Y2K including:

- December 2021: Log4J/log4Shell vulnerability
- Month 2024: XZ backdoor attack that could have been disastrous if the community had not responded as quickly as it did.
- July 2024: CrowdStrike outage

Log4J was the first moment that the world realized that a single vulnerability in a major programming application could cripple major software systems if exploited. The CrowdStrike outage, almost three years later, highlighted similar issues – this time with real-life examples of what can happen without the software we take for granted, including grounded flights, banking systems brought offline, and over $5 billion in losses for Fortune 500 companies. XZ Utils was a library that was embedded in multiple operating systems, and a new version all of a sudden included a sophisticated attack that opened an SSH backdoor.

There are countless other lesser-known instances where software vulnerabilities, if not discovered and patched, have the power to take down our critical infrastructure. For example, in July, a leaked Python access token was discovered in DockerHub. Had it fallen into the wrong hands, this access token would give a threat actor administrator access to all of Python's, PyPI's, and the Python Software Foundation's repositories, supposedly making it possible to carry out an extremely large-scale supply chain attack.

The moral of these stories is that we're experiencing more "Y2K's" now, as attackers have realized that compromising a software development lifecycle is a viable way for a malicious user or group to gain unauthorized access to valuable software resources and assets.

Lessons Learned from Y2K and Adaptations for Software

Our infrastructure has changed *a lot* since 1999, most notably through a move away from a hardware-first mentality to a more software-first mentality. Solutions to solve business issues and to provide a competitive edge now rely on virtualized infrastructure, headless servers, microservices and a cross matrix of dependencies.

However, principles learned from the events of Y2K are highly applicable to today's software-defined age in terms of what's required to ensure safety and sustainability:

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

1. IT leaders must have accurate inventories of what should be running in production and how it was built, and automated ways to detect deviations.
2. The need for safer, faster responses with the aid of automation, when a confirmed critical vulnerability or risk is detected.
3. Details matter. Updates for an enhanced user experience are great, but they shouldn't come at the expense of mission critical functionality or system reliability. Losing visibility is a risky proposition and will cause issues.
4. Coordinating and practicing responses across business owners, Dev(Sec)Ops, HR and IT teams in moments of disruption to ensure continuity of mission critical assets and processes.

These lessons and subsequent events that have caused outages and data breaches have fundamentally altered the developer and IT security job functions. More and more is being asked of these professionals, requiring them to have a far more robust skillset than they once did to protect their tech stacks and environments. In the era of Y2K, the IT, security, and developer job functions were well defined but often siloed. Now, the lines are blurred – it is inefficient and dangerous to assume that software development and security are not intrinsically linked.

Luckily, the teams securing our software supply chain have risen to the challenge and adapted accordingly, which is why we are able to talk about recent software-related incidents as "what-ifs" rather than post mortems. The teams are ready to detect, and quickly respond to and mitigate risks when they arise.

The Next "Major" Y2K Moment: The 2038 Problem

While we've explored how recent events were commensurate with the potential scale of Y2K, we are currently on the way to a nearly identical situation set to occur in 2038.

Dubbed the "2038 Problem," it refers to an issue with UNIX time (expressed as UTC) where the Linux operating system will not be able to record time past the date of January 19, 2038. Is it going to matter? UTC is critical for the ability to authorize certificates for devices that run on Linux. Luckily, we have learned from the Y2K event and modern programming languages are designed to overcome this potential weakness. The real problem might occur for those older legacy systems that could suffer an issue. So, we still need to be vigilant and identify them before that impending date because those issues will be complex challenges that won't have a straightforward solution.

How we address these problems in the next 13 years will be paramount. But the good news is that we've learned from the Y2K event and the subsequent software catastrophes. We will still need to improve and effectively strategize with the best minds in the industry to overcome these challenges since they are not going away – this means continuing to remove the barriers that silo developers, security and IT teams and create seamless collaboration with a common goal of securely delivering software to the world.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

About the Author

Paul Davis is Field CISO of the JFrog. He is an experienced IT Security Executive who works to help CISOs, IT execs and security teams, enhance protection of their software supply chain. Additionally, he advises IT security startups, mentors security leaders, and provides guidance on various IT security trends. Paul can be reached on the company website at https://jfrog.com/blog-author/paul-davis/



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Use AI to Enhance Your Patch Management Strategies

By Zac Amos, Features Editor, ReHack

Patch management updates software and systems to fix weaknesses, enhance functionality and ensure seamless operations. It protects businesses from the growing threat of cyberattacks that exploit outdated vulnerabilities.

With the complexity of IT environments, manual updates often fall short, exposing organizations. AI-powered tools can help companies automatically detect vulnerabilities and prioritize based on risk without disrupting workflows. As cyber threats grow more sophisticated, leveraging AI for patch management is necessary to safeguard data and stay ahead of potential risks.

Why Patch Management Is Crucial

Outdated software is a prime target for hackers because it often contains known weaknesses that are easy to exploit. In 2022, malicious actors in the U.S. exploited older software vulnerabilities more

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

frequently than newly disclosed ones, highlighting the dangers of neglecting updates. The 2017 Equifax breach is a sobering example. An outdated vulnerability in Apache Struts exposed sensitive data for 143 million U.S. consumers, 15 million U.K. consumers and 8,000 Canadians.

Beyond security, patch management is vital for maintaining compliance with regulations like GDPR and HIPAA, which require timely fixes to protect data. It also helps businesses avoid costly downtime due to system failure or cyberattack incidents, keeping operations running smoothly. Prioritizing security updates can safeguard organizational systems, protect customer trust and avoid emerging threats.

How AI Can Boost Patch Management

Managing software in a cybersecurity environment can feel like a never-ending battle against vulnerabilities. AI optimizes the process, helping IT teams detect, prioritize and deploy fixes faster and more precisely.

1. Automating Patch Detection and Deployment

AI-driven tools automate the tedious process of scanning systems for vulnerabilities and deploying updates. These tools continuously monitor for weaknesses and analyze risks based on severity, allowing IT teams to tackle the most critical threats first.

Efficiently applying patches can significantly reduce an organization's risk of falling victim to cyberattacks. Updating software ensures users are less likely to encounter exploits or vulnerabilities already fixed in newer versions. With AI handling the heavy lifting, organizations can stay one step ahead of hackers while saving time and resources.

2. Predictive Analysis for Vulnerability Management

AI brings a proactive edge to patch management by predicting high-risk vulnerabilities before they become major threats. Analyzing historical data and real-time threat intelligence allows this tool to identify patterns indicating which weaknesses hackers will most likely exploit.

AI-powered tools take this further by leveraging machine learning models that continuously learn from past activities. This allows them to improve over time, better identify compatibility issues and ensure updates are deployed smoothly. Integrating predictive analysis with machine learning lets companies prioritize critical fixes and minimize the risk of disruptions while staying ahead of emerging threats.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

3. Enhanced Threat Intelligence Integration

AI empowers organizations to stay ahead of cyber threats by analyzing real-time threat data to quickly identify critical patches. Using advanced algorithms, AI monitors global threat intelligence feeds, scanning for emerging attack patterns as they happen.

It then cross-references this data with a software inventory, pinpoints which systems are at risk and prioritizes updates accordingly. This rapid analysis allows businesses to address vulnerabilities faster than traditional methods, which reduces the window of exposure. With AI handling real-time threat detection, companies can act decisively to safeguard their systems before attackers can exploit them.

4. Reduced Downtime with Smart Automation

AI-powered tools ensure seamless patching and don't disrupt business-critical operations. Automating the process allows these programs to schedule updates during off-peak hours. Likewise, it prioritizes fixes that won't interfere with key systems and tests them in virtual environments before deployment. Automation also frees IT teams from time-consuming manual tasks, which allows them to focus on strategic projects.

Additionally, AI tools help organizations comply with regulatory requirements by addressing vulnerabilities promptly. This proactive approach enables businesses to stay ahead of emerging threats rather than constantly playing catch-up, strengthening their overall cybersecurity posture.

Tips for Better Patch Management

Effective management keeps systems secure and operational. With the increasing complexity of IT environments, leveraging the right strategies can make all the difference. Here are some practical tips:

- **Use AI to prioritize vulnerabilities by risk level:** Leverage AI-driven tools to analyze threat data and focus on high-risk patches first.
- **Automate scanning:** Deploy AI-powered tools to continuously scan systems for weaknesses and recommend timely updates.
- **Test patches in virtual environments:** Use AI to simulate deployment and identify potential compatibility issues before applying fixes.
- **Integrate AI with threat intelligence:** Combine real-time threat feeds with AI tools to detect and address emerging risks faster.
- **Schedule updates during low-traffic hours:** Minimize disruption by automating deployment during non-peak times.
- **Track progress with AI dashboards:** Monitor real-time analytics to ensure patches are completed successfully across all devices.
- **Regularly review and refine:** Use insights from AI tools to improve patch management processes over time.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

These tips can help organizations maintain a robust defense against cyber threats and streamline their patching workflows.

Transforming Patch Management with Precision and Efficiency

AI improves patch management by dramatically improving the speed, precision and efficiency of identifying and deploying critical updates. Businesses investing in AI-driven tools can proactively approach cybersecurity, staying ahead of vulnerabilities and protecting their systems from evolving threats.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on Twitter or LinkedIn.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



What Can We Learn from Recent Telecom Hacks?

By Chris Henderson, Senior Director of Threat Operations, Huntress

In early November, it was reported that Singapore telecommunications company, Singtel, had been compromised by Volt Typhoon, a hacking group considered to be backed by the Chinese state. While details about the intrusion remain limited, no data is thought to have been stolen. However, the attack signaled a wider threat to the world, as it was believed to be a trial run for China's cyber capabilities before moving on to other nations.

Unfortunately, numerous reports from the U.S. government at the end of 2024 revealed otherwise. Salt Typhoon, another Chinese state-sponsored hacking group, had already infiltrated U.S. telecommunications networks, in some cases for as long as 18 months. This significant cyber espionage campaign allowed them to gather a vast amount of confidential information, including data on over a million people and communications involving high-ranking officials and key locations like Washington, D.C.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

These incidents raise serious red flags about the security of critical infrastructure and the threat posed by Chinese hacking groups. Telecommunications networks are essential for everyday life—supporting businesses, government operations, and daily communication. For groups like Volt or Salt Typhoon, they are a single entry point that can unlock valuable intelligence, disrupt vital services, and even act as a launchpad for more widespread attacks.

The Escalating Threat Landscape

The attacks by Volt and Salt Typhoon are great examples of recent escalations in state-sponsored attacks. The tactics and determination shown in these incidents highlight a growing pattern in cyber espionage, where state-backed hackers are zeroing in on critical infrastructure to underpin national security and economic stability.

By compromising telecommunications networks, adversaries gain more than just access to sensitive communications; they gain a foothold in systems vital to emergency response, military coordination, and financial transactions. Imagine the consequences if emergency services were disrupted during a natural disaster or if critical military communications were jammed during a conflict. This threat extends far beyond telecommunications. Power grids, water systems, healthcare and transportation are all vulnerable to similar attacks. These sectors share common weaknesses: outdated legacy systems, reliance on third-party vendors and the constant struggle to balance operational needs with robust security.

That being said, securing telecommunications infrastructure presents unique challenges. These networks must remain operational 24/7, which leaves little room for downtime to implement security upgrades or conduct thorough testing. Even encryption, which is vital for protecting data, requires a delicate balance to ensure its effectiveness while complying with regulatory requirements. Additionally, the rapid growth of IoT devices has significantly increased the attack surface, introducing more vulnerabilities that need to be managed. The scale and complexity of these networks also make it extremely difficult to differentiate between legitimate activity and malicious behavior.

How Telecommunications Providers Can Enhance Their Security Posture

These incidents serve as a stark reminder of the urgent need to fortify critical infrastructure against sophisticated threats. Telecommunications providers, in particular, must prioritize proactive and layered defense strategies. Here's how:

- **Comprehensive Monitoring and Threat Detection:** Telecommunications networks are vast and complex, handling enormous volumes of data. Network detection and response tooling that analyzes network activity in real-time are essential. Quickly detecting anomalies in either volume, destination or origin of traffic can make the difference between containing an intrusion and allowing it to escalate into a full-blown breach.
- **Routine Security Audits and Penetration Testing:** Legacy systems, often the backbone of telecommunications infrastructure, are particularly vulnerable. Regular security assessments and

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

penetration testing can uncover weaknesses, like outdated software, misconfigurations, and security control failures before attackers exploit them. These evaluations should extend beyond internal systems to include third-party hardware and software providers. Additionally, security assessments should always include an assessment of staff in addition to the hardware and software. As tradecraft moves to an identity-first approach, ensure your humans are ready to face these threats.

- **Strengthening Resilience Through Redundancy:** Critical systems should be designed with resilience in mind. Implement redundancy by having backup systems and alternate communication pathways to ensure operational continuity in case of compromise. Conduct regular incident response drills to prepare for worst-case scenarios and formulate disaster recovery plans that include both technical and business operations continuity. Identify your organization's critical vendors and processes and establish plans for continued operation even if a supply chain partner becomes unavailable.
- **Securing the Supply Chain:** Telecommunications rely heavily on third-party vendors for hardware and software, creating a sprawling supply chain that adversaries can exploit. To mitigate these risks, rigorous vetting processes, contractual security requirements and ongoing monitoring of supply chain partners need to mature. In addition to evaluating supply chain partners for their cybersecurity resilience, be sure to inspect their preparedness for their own continued operations in the event of an intrusion or supply chain impact.

The Path Forward

The recent attacks on Singtel and U.S. telecommunications networks demonstrate that our adversaries are becoming more capable, persistent and willing to target critical infrastructure. A single company or government entity can’t address this issue. The public and private sectors must collaborate to effectively combat threats like Volt and Salt Typhoon.

Governments bring valuable intelligence, a national security perspective, and regulatory power to the table, while the private sector offers innovation, agility, and deep domain expertise. This collaboration can take many forms, from joint cybersecurity exercises and information sharing centers to public-private partnerships focused on research and development. By sharing threat intelligence, coordinating responses, and jointly developing security solutions, both sectors can combine resources and expertise to proactively address cyber threats and ensure rapid and unified responses to incidents.

Telecommunications providers and other critical industries must also prioritize proactive security measures. This includes continuous monitoring and threat detection, regular security audits and penetration testing, building redundancy into critical systems and securing the supply chain. By investing in these measures, we can enhance the resilience of our critical infrastructure and mitigate the risks posed by sophisticated adversaries.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

While the threat landscape constantly evolves, we have the tools and expertise to defend our critical infrastructure. Through collaboration, innovation and a commitment to continuous improvement, we can stay ahead of our adversaries and ensure the security and stability of our essential services.

About the Author



Chris Henderson is the Senior Director of Threat Operations at Huntress. He has been securing MSPs and their clients for over 10 years through various roles in Software Quality Assurance, Business Intelligence, and Information Security.

Chris can be reached online at https://www.linkedin.com/in/chenderson-cissp/ and at our company website https://www.huntress.com/.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



The Next Security Frontier: Agentic AI

Security teams will need to understand the different stages of how agents work to make sure the use of agents is safe and effective as they become more routinely integrated into business processes.

By Ben Kliger, CEO and Co-Founder, Zenity

Generative AI is quickly moving beyond the capabilities of consumer-focused tools like ChatGPT into the new realm of agentic AI for enterprise use. LLMs can only go so far, and many industry leaders predict that agentic AI is the future of AI advancement for companies looking to become more efficient and transform work processes. In fact, agentic AI took number one on Gartner's list of the top 10 technology trends for 2025.

We're already seeing the burgeoning use of autonomous AI agents, which can be deployed to conduct tasks independently, such as executing sales communications or marketing campaigns. These agents are designed to process information in a new way to make dynamic decisions and even interact with other agents and capabilities. For CIOs, this technology offers enormous potential to reap the benefits of generative AI to increase productivity; agentic AI can essentially perform as a highly competent teammate

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

working almost like a human employee. Like a sports or real estate agent, they make decisions and act on your behalf.

These AI agents have access to a lot of sensitive corporate information and work like human employees, which means they can be unpredictable. Given these tools' widespread access to all manner of sometimes sensitive information, action must be taken quickly to avoid creating a security disaster.

Key security concerns of agentic AI

Any new technology can introduce new vulnerabilities, and that's certainly the case with agentic AI. For example, if an agentic AI system gets compromised, it could make decisions that range from irksome to catastrophic and cause a domino effect of negative impacts.

Allowing an AI agent to roam the web at will, for instance, can have negative results. The AI agent doesn't understand that it can't trust everything it "sees" online. It's built to follow instructions, and that's what it will do. With access to the internet, the agent is perpetually one search away from coming across a site with hidden malicious instructions that lead to its takeover by a bad actor.

Bad actors are using the internet, too, of course. If a cybercriminal manages to compromise your AI agent, they can tell it to search a malicious website they've created. Without a human in the loop, the agent will do as told. What typically happens next is encoding data to be exfiltrated into a parameter. Giving an agent free internet rein enables bad actors to take sensitive data out of a private thread – no approvals necessary.

Making agentic AI more secure

Most companies are looking to effect positive business changes via AI agents. Security teams will need to understand the different stages of how agents work to make sure the use of agents is safe and effective as they become more routinely integrated into business processes:

1. A prompt or trigger comes from a user, like "Summarize my emails" or an automatic prompt—for instance, you build an agent that summarizes all your emails from a given day.

2. The agent performs various retrieval-augmented generation (RAG) steps: calling data, calling other agents, activating applications and so on.

3. The agent then "returns" an action, whether it's an answer to a prompt or something else (such as updating data, creating a chart, answering customer inquiries and so on.

However, organizations need to go beyond just looking at prompts and responses by also incorporating insights into what the agent does behind the scenes. They need to understand how, when and why agents are making decisions to do what they do. By diving deep into the agents' actions, they can uncover issues related to data privacy/protection, interpretation of prompts and governance/compliance.

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Data privacy and protection – One main issue is handling sensitive data. Another is ensuring that business users have control over which data is processed, who has access to it and how the policies are enforced. It's typical for AI agents to process vast quantities of information – and some of it is bound to be sensitive or confidential. Security teams must deploy strong measures to protect data; this includes regular audits, access controls and encryption. This combination will help to block data breaches and unauthorized access to data.

Proper interpretation of prompts – The way that AI agents interpret prompts and triggers is also a key factor in security. If an agent misinterprets a prompt, it could respond or act in unintended ways – which could cause security vulnerabilities or disrupt operations. Security teams must scrupulously test AI agents in various scenarios to ensure they are responding properly and consistently. Also, using guardrails like human-in-the-loop mechanisms can help reduce risk by enabling human oversight and intervention as needed.

Governance and compliance – Organizations must ensure compliance with industry standards and regulations. Legal and compliance departments must collaborate with security teams to institute governance frameworks focusing on the ethical and legal consequences of working with AI agents.

Securing the agentic AI frontier

AI agents are transforming the business world, providing huge benefits with respect to innovation, competitive advantage and efficiency. There are several ways to build AI agents on your own (i.e. tools like Salesforce Agentforce, AWS Bedrock, and Microsoft Copilot Studio), which introduces not only a large volume of these agents but also means that less technical users are building agents. And that means greater security risk – potentially of a severe nature. Use the guidance discussed above to ensure security is in place to enable business while keeping your business safe.

About the Author

Ben Kliger is the CEO and Co-Founder of Zenity, with vast experience in the Cybersecurity industry spanning over 16+ years. His expertise ranges from hands-on cyber security, team building and leadership through business strategy and management. Ben can be reached on LinkedIn or at https://www.zenity.io.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.


EVENTS

ORGANIZED BY

CYSEC GLOBAL

CYSEC QATAR

13TH GLOBAL EDITION

4 FEB 2025

Sheraton Grand Doha Resort & Convention Hotel | Doha, Qatar

Advancing Qatar's Cyber Resilience for Tomorrow

#CYSEC25 / QATAR.CYSECGLOBAL.COM



CYSEC KUWAIT

14TH GLOBAL EDITION

12th FEBRUARY, 2025

CROWNE PLAZA KUWAIT
AL THURAYA CITY, KUWAIT

Navigating the Path to a Cyber Secure Kuwait!

#CYSEC25 / KUWAIT.CYSECGLOBAL.COM



19TH GLOBAL EDITION

CYBERX QATAR

#CyberXQatar



300+
PREQUALIFIED DELEGATES

30+
SOLUTION PROVIDERS

25+
INDUSTRY EXPERTS

10+
HOURS OF SESSIONS

FEBRUARY 5TH 2025

GRAND HYATT DOHA HOTEL & VILLAS
DOHA, QATAR

RESERVE YOUR SPOT
www.cyberxqatar.com

ORGANISED BY

BConnect

AN INITIATIVE BY

CYBERX GLOBAL

عالم الذكاء الاصطناعي
EVERYTHING
— GLOBAL —

4 FEB 2025
AI EVERYTHING SUMMIT
ABU DHABI

5 - 6 FEB 2025
EXHIBITION SHOWCASE
DUBAI

POWERING GLOBAL COLLABORATIONS IN THE NEW AI ECONOMY

15,000+	500+	150+	60+	200+
VISITORS	EXHIBITORS	INVESTORS	COUNTRIES	SPEAKERS



ACCELERATED BY
GITEX GLOBAL

/AiEverythingGLOBAL

aieverythingglobal.com


DGI
GEOSPATIAL INTELLIGENCE FOR DEFENCE AND SECURITY
THE WORLD'S LEADING GEOSPATIAL INTELLIGENCE EVENT
USE CODE:
CDM10
FOR 10% OFF
10 - 12 February, 2025
The QEII Centre, London
900+
Geospatial Intelligence Professionals to Network With
125+
Geospatial Intelligence Experts Sharing Their Practical Insights
60+
Nations Represented from Around the World
15+
Hours of Invaluable Networking Time
3 DAYS
of Insightful Content

FUTURE AI SUMMIT
MALAYSIA

OFFICIAL SUPPORTING PARTNER

MDEC



26 FEBRUARY 2025

KUALA LUMPUR, MALAYSIA

POWER OF AI + DATA

BUILDING NEXT GEN ENTERPRISES

150+ PREQUALIFIED DELEGATES

15+ SOLUTION PROVIDERS

15+ INDUSTRY EXPERTS

10+ HOURS OF SESSIONS

FOR MORE INFORMATION
malaysia.futureaisummit.com

ORGANISED BY BConnect

RegTech Africa Conference

// @REGTECHAFRICA

2025 REGTECHAFRICA CONFERENCE & AWARDS

Theme

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

- HYBRID EVENT
- 2 DAYS
- 1,000+ PARTICIPANTS
- 50+ SPEAKERS
- 10 TRACKS

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

GET A TICKET

WWW.REGTECHAFRICACONFERENCE.COM

ENDORSED BY | LASAA

GITEX EUROPE Berlin

21 – 23 MAY 2025

MESSE BERLIN — GERMANY —

FEATURING

GITEX GREEN IMPACT | SMEDEX SME Digital Economy Expo | AI EVERYTHING EUROPE | NORTH STAR EUROPE

CREATING NEW DIGITAL BUSINESS OPPORTUNITIES IN BERLIN

Europe's #1 Most Dynamic Tech & Startup Metropolis

2,500+ EXHIBITORS

1,500+ STARTUPS

1,000+ INVESTORS

100+ COUNTRIES

SCAN TO GET INVOLVED

ENDORSED BY

BERLIN

Senate Department for Economics, Energy and Public Enterprises

SUPPORTED BY

BERLIN

BERLIN PARTNER for Business and Technology

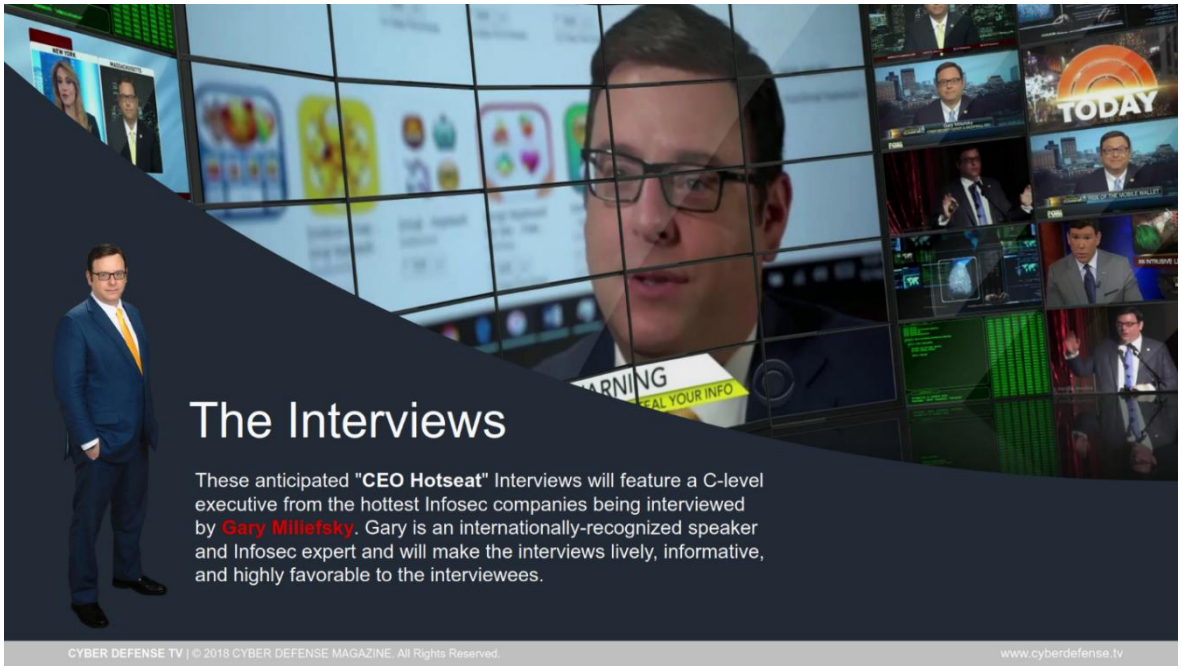
CYBER DEFENSE TV

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.



Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.

Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

Copyright (C) 2025, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com,and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide.
marketing@cyberdefensemagazine.com

All rights reserved worldwide. Copyright © 2025, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

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

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

All rights reserved worldwide.

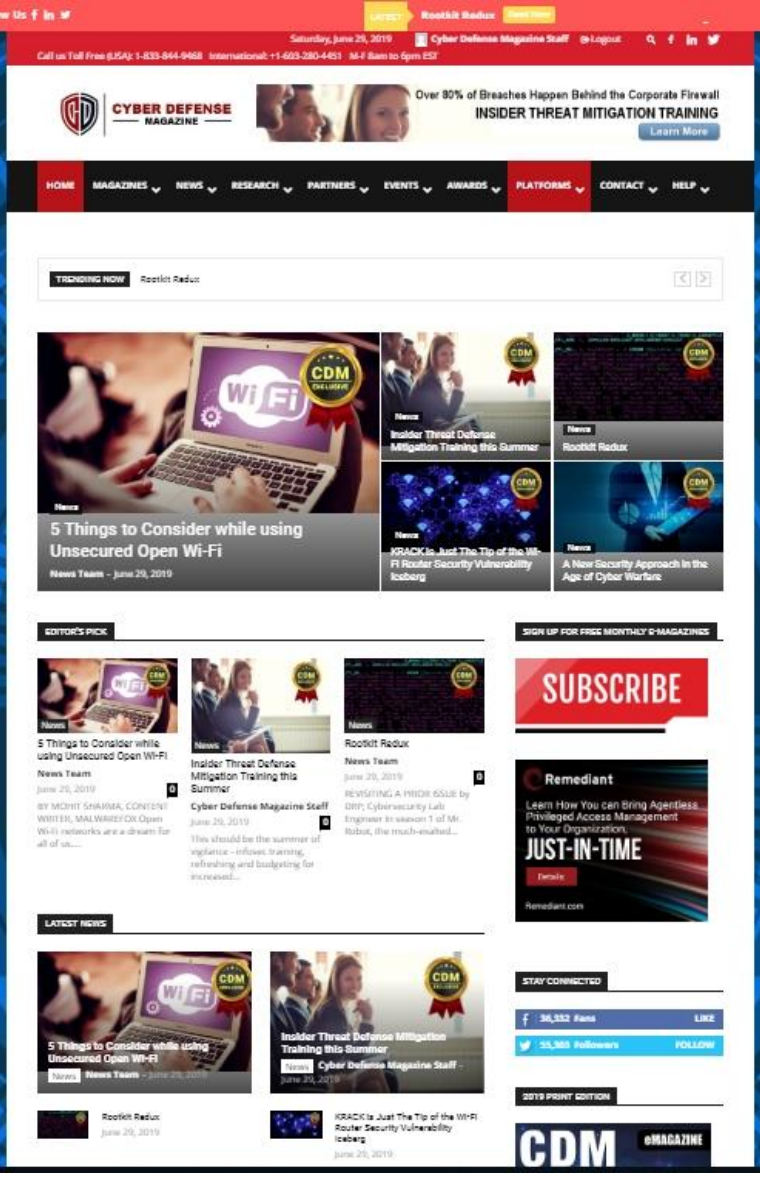
marketing@cyberdefensemagazine.com

https://www.cyberdefensemagazine.com/

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

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 02/03/2025

Copyright © 2025, Cyber Defense Magazine. All rights reserved worldwide.



Books by our Publisher: [Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook : Miliefsky, Gary: Kindle Store,](#) [Kindle Store, Cybersecurity Simplified, with others coming soon...](#)

13 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites. We successfully launched https://cyberdefenseconferences.com/ and our new platform https://cyberdefensewire.com/

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert



ALWAYS FREE
NO STRINGS ATTACHED



CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER



www.cyberdefensewire.com
www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com



Protect Your Defense Business with Cybersecurity Support from NSA.

Small and medium sized defense contractors are frequently targeted by cyber criminals and nation-state threat actors alike. Don't let inadequate security measures put your intellectual property and networks at risk. Our no-cost cybersecurity services can help protect your business from evolving cyber threats.

GET STARTED TODAY

nsa.gov/ccc

RSAConference™2025

San Francisco | April 28 – May 1 | Moscone Center

Many Voices.
One Community.



Together we secure.
Join us at RSA Conference 2025!

Cybersecurity's greatest challenges demand more than one perspective. That's why RSAC 2025 unites thousands of voices from around the world to collaborate, innovate, and secure our digital future.

From April 28 – May 1 you'll hear groundbreaking Keynotes, explore hands-on sessions, and participate in exclusive networking opportunities. This is where the global cybersecurity community connects to share insights and find solutions.

Why Attend?

- Hear from top experts tackling today's toughest challenges in cybersecurity.
- Experience cutting-edge solutions at the Expo that will drive your strategies forward.
- Collaborate with peers to unlock innovative solutions and gain fresh perspectives.
- Expand your network with professionals from every corner of the globe, forging connections that last a lifetime.

Be a part of something bigger. RSAC 2025: **Many Voices. One Community.**

Register now at RSAConference.com/cyberdefense25

#RSAC



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