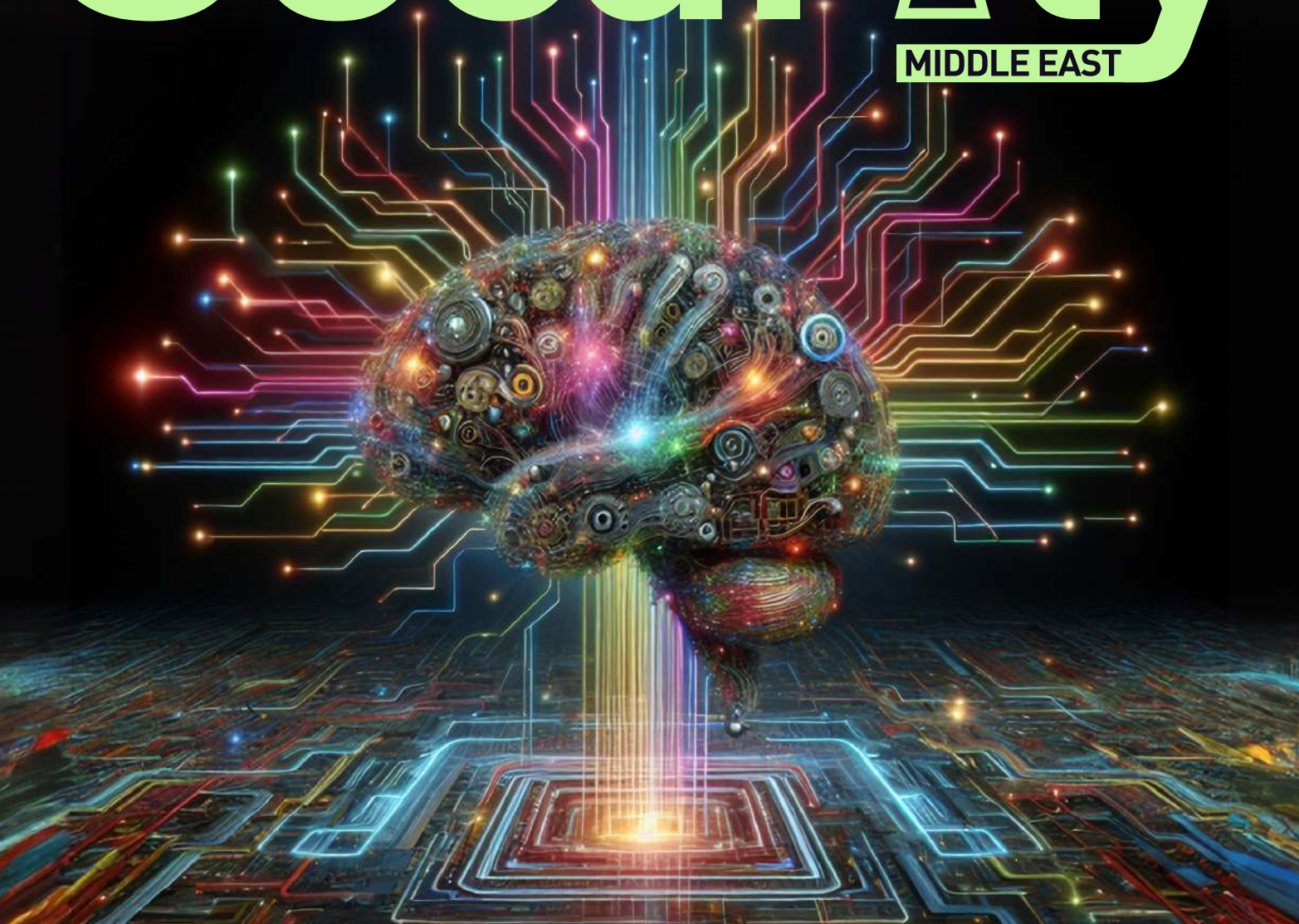


Security

ADVISOR

MIDDLE EAST



AI IN CYBERSECURITY: PROMISE, PERIL, AND THE PATH FORWARD

AI IS NOW CENTRAL TO CYBER DEFENCE, BUT ITS SAFE FUTURE
RESTS ON ETHICS, TRANSPARENCY, AND HUMAN CONTROL.



Delinea

Securing identities at every interaction

Seamless, intelligent, centralized authorization to better secure the modern enterprise



Secure Credentials



Privileged Remote Access



Privilege & Entitlement Elevation



Identity Threat Protection



Identity Governance

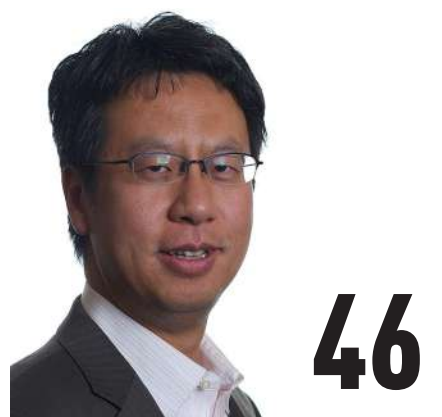
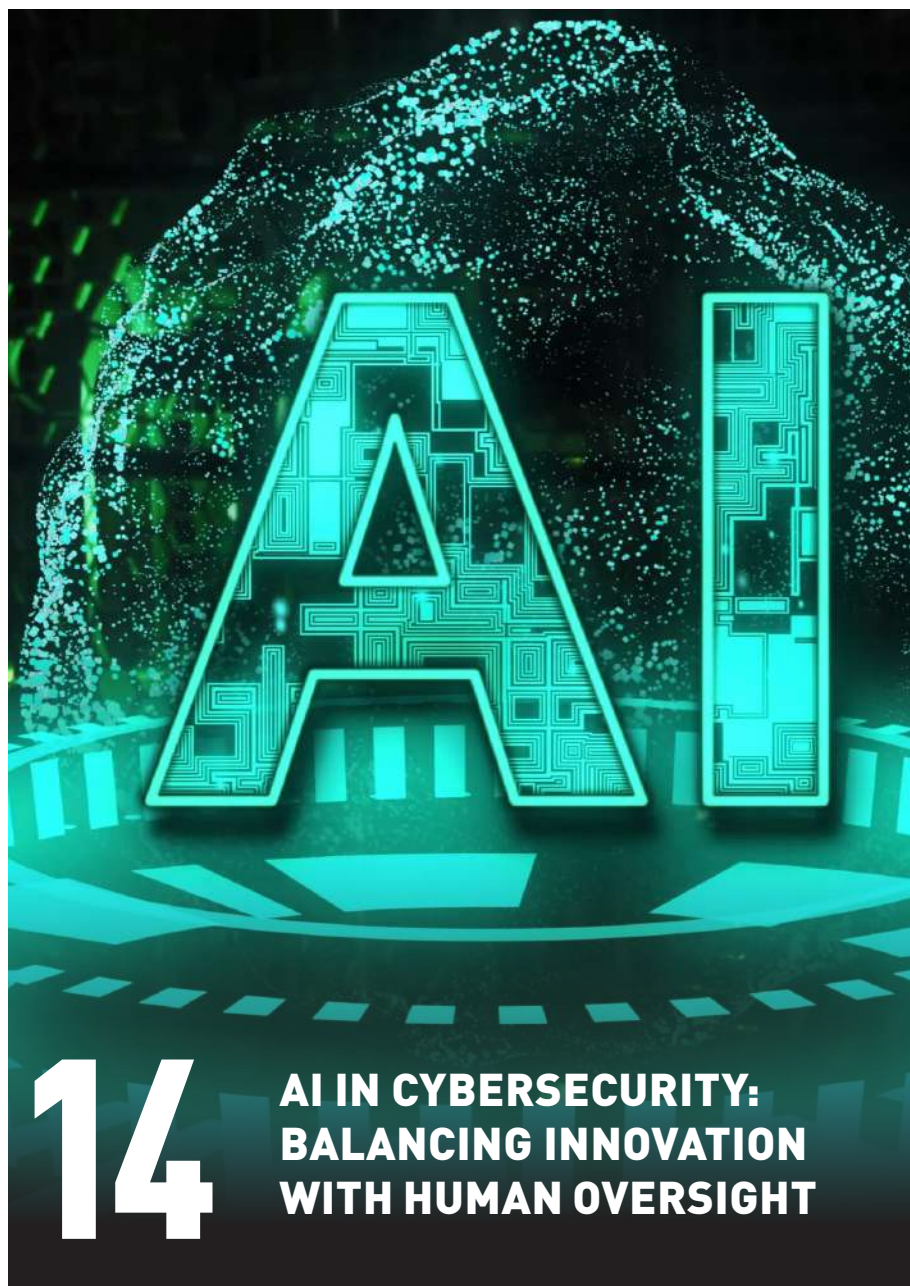


Follow us on



delinea.com





9 SANS Institute brings Cyber Leaders Forum back to Riyadh this August

40 BeyondTrust accelerates identity security innovation and research momentum with launch of Phantom Labs

22 Ransomware in the Crosshairs: Sophos, Halcyon announce new intelligence-sharing and mutual anti-tamper protection initiative

46 Fortinet expands FortiCloud with new identity, storage, and communication services.



CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD
CLEANROOM™ RECOVERY



Visit commvault.com to Learn More

EDITOR'S NOTE



Talk to us:
E-mail:
sandhya.dmello@
cpimediagroup.com

Sandhya DMello
Editor

AI'S PROMISE AND PERIL: WHY SECURITY LEADERS MUST STAY AHEAD

Welcome to the combined July–August 2025 issue of Security Advisor Middle East. This edition captures the accelerating transformation of the cybersecurity landscape — one where artificial intelligence is both an enabler and a threat. As nearly 98% of organisations embed AI into their defences, experts caution that human oversight, ethical governance, and transparency remain critical to navigating its full potential without compromising security or trust.

In our cover story, we examine how CISOs, researchers, and innovators are balancing AI's disruptive capabilities with the need for robust safeguards.

Industry leaders from Fortinet, Sophos, Tenable, and SANS Institute share insights into closing skills gaps, augmenting human creativity, and reinforcing cyber resilience as attacks become faster, smarter, and harder to detect.

Beyond AI, this issue brings you breaking updates and innovations shaping enterprise security:

- Recognition and leadership: SentinelOne secures its fifth consecutive Leader position in Gartner's Magic Quadrant for

EPP, while Vectra AI leads the way in AI-driven NDR.

- Emerging threats: Cloudflare uncovers phishing campaigns exploiting trusted email security tools, and Sophos-Halcyon forge a partnership to outpace ransomware groups.
- Innovation at scale: From Tenable's AI exposure management to HID's next-gen passkey ecosystem, vendors are accelerating solutions designed for hybrid, AI-driven enterprises.
- Regional focus: The SANS Cyber Leaders

Forum returns to Riyadh, spotlighting Saudi Arabia's growing role as a global cybersecurity hub.

With ransomware surging, AI-enabled attacks evolving, and enterprises navigating multi-vendor complexities, this issue is your guide to understanding where the future of cybersecurity is headed — and how to prepare for it.

The lines between innovation and exploitation are blurring faster than ever. Staying ahead requires more than technology; it demands strategic foresight, collaborative intelligence, and an unwavering commitment to securing the digital economy.

DEFENDING INNOVATION WITH INTELLIGENCE

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

ADVERTISING
Group Publishing Director
Kausar Syed
kausar.syed@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

PRODUCTION AND DESIGN
Designer
Prajith Payyapilly
prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES
Web Developer
Adarsh Snehan
webmaster@cpimediagroup.com

Publication licensed by
Dubai Production City, DCCA
PO Box 13700
Dubai, UAE

Tel: +971 4 5682993

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

© Copyright 2025 CPI
All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

ATTACKERS EXPLOIT PROOFPOINT AND INTERMEDIA LINK WRAPPING TO DELIVER PHISHING PAYLOADS, SAYS CLOUDFLARE

From June 2025 through July 2025, the Cloudflare Email Security team has been tracking a cluster of cybercriminal threat activity leveraging Proofpoint and Intermedia link wrapping to mask phishing payloads, exploiting human trust and detection delays to bypass defenses.

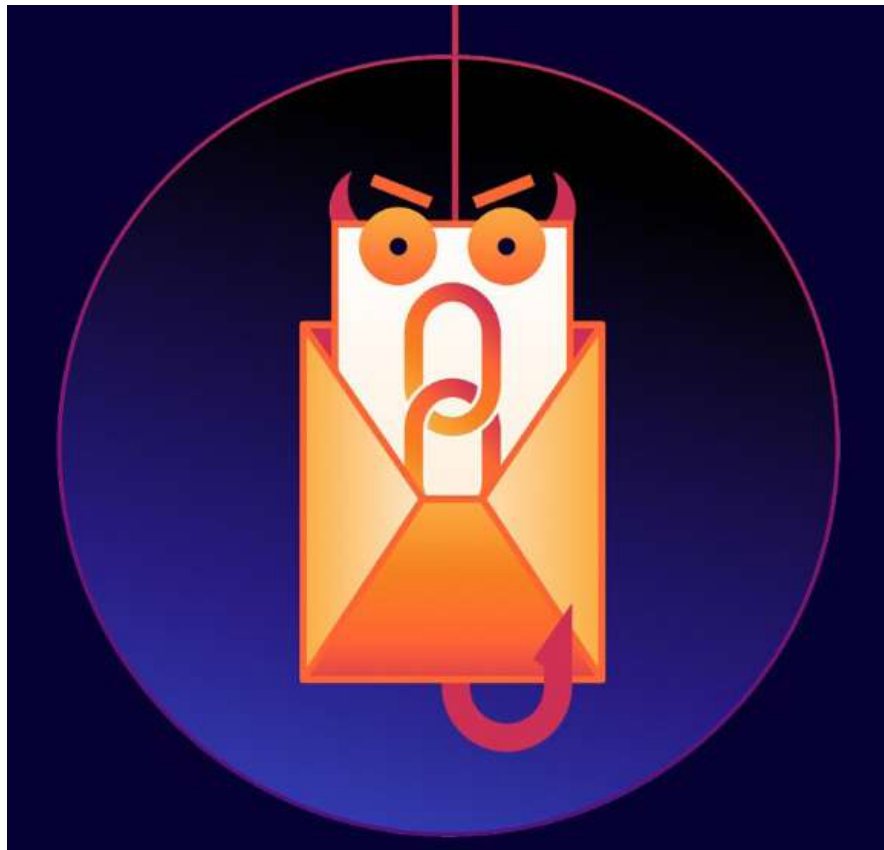
Link wrapping is designed by vendors like Proofpoint to protect users by routing all clicked URLs through a scanning service, allowing them to block known malicious destinations at the moment of click. For example, an email link to `http://malicioussite[.]com` might become `https://urldefense[.]proofpoint[.]com/v2/url?u=http-3A__malicioussite[.]com`. While this is effective against known threats, attacks can still succeed if the wrapped link hasn't been flagged by the scanner at click time.

Recent campaigns observed by the Cloudflare Email Security team reveal how attackers are abusing Proofpoint's and Intermedia's link wrapping features to bypass detection and redirect victims to a variety of Microsoft Office 365 phishing pages. This technique is particularly dangerous as victims are much more likely to click on a 'trusted' Proofpoint or Intermedia URL than an unwrapped phishing link.

Impact

By cloaking malicious destinations with legitimate `urldefense[.]proofpoint[.]com` and `url[.]emailprotection` URLs, these phishing campaigns' abuse of trusted link wrapping services significantly increases the likelihood of a successful attack. Attackers exploit the inherent trust users place in these security tools, which can lead to higher click-through rates and a greater probability of impacts such as:

- **Direct financial loss:** By making fraudulent links appear legitimate, attackers lower user suspicion at the critical moment of click-time, making direct financial loss more



Cloudflare reveals how cybercriminals are manipulating link wrapping to bypass defences and deliver Microsoft 365 phishing attacks

likely. In 2024, email was the method of contact for 25% of fraud reports. Of these, 11% resulted in financial loss, amounting to an aggregate loss of \$502 million and a median loss of \$600 per incident.

- **Compromise of personal accounts leading to identity theft:** Link wrapping could serve as a highly reliable method for harvesting personal data. Phishing campaigns are a primary method for attackers to obtain personal information, contributing to 1.1 million identity theft reports in 2024, with credit card fraud and government benefits fraud being top categories.
- **Significant time burden for victims:** Victims of identity theft, often initiated

through phishing, face substantial time burdens, with tax-related cases averaging over 22 months (676 days) for resolution in Fiscal Year 2024.

- **Phishing as leading breach method:** Comcast research shows 67% of all breaches start with someone clicking on a seemingly safe link.
- **Credential theft via phishing:** The 300% spike in credential theft incidents observed by Picos Security in 2024 can be fueled by more effective phishing techniques like link wrapping.

Mitigation and detection

Because this campaign abuses the trusted domains of security providers, conventional reputation-based URL filtering is ineffective. The following

detections were written by Cloudflare Email Security to protect against phishing campaigns leveraging the link wrapping techniques described. They leverage a variety of signals based on historical campaign data, and incorporate machine learning models trained on messages containing link wrapping URLs.

- SentimentCM.HR.Self_Send.Link_Wrapper.URL

- SentimentCM.Voicemail.Subject.URL_Wrapper.Attachment

“Threat actors are constantly evolving their tactics to exploit even the most trusted layers of email security. What we’re seeing with the abuse of link wrapping is a stark reminder that attackers are not just targeting users — they’re manipulating the very systems meant to protect them. At Cloudflare, our

mission is to stay ahead of these threats with proactive, AI-powered detection and comprehensive visibility across the email attack surface. We’re committed to helping organizations in the Middle East and globally close these blind spots and build a more secure digital environment,” concludes Bashar Bashaireh, AVP Middle East, Türkiye & North Africa at Cloudflare.

NUTANIX NAMED A CHALLENGER IN 2025 GARTNER MAGIC QUADRANT FOR CONTAINER MANAGEMENT

Nutanix, a leader in hybrid multicloud

computing, announced it has been recognised as a Challenger in the 2025 Gartner Magic Quadrant for Container Management. This marks Nutanix’s first recognition in this Magic Quadrant following the launch of its Nutanix Kubernetes Platform (NKP) solution last year.

The company introduced NKP after integrating D2iQ, Inc.’s Kubernetes Platform, allowing Nutanix to deliver a production-ready enterprise solution for managing cloud native applications across diverse environments. Customers can run both modern and traditional applications on the same platform—anywhere from their datacentre and the edge to public clouds—on virtualised underlays, bare metal, or native public cloud Kubernetes® environments.

Lee Caswell, SVP Product and Solutions Marketing at Nutanix, said: “We’re delighted to be recognised as a Challenger in the 2025 Gartner Magic Quadrant for Container Management, which we believe is testament to our relentless focus on product innovation and customer success. Our open and complete NKP solution complements our existing portfolio both architecturally and in go-to-market execution, giving customers a seamless path to modernise their applications while simplifying operations across hybrid multicloud environments.”



Lee Caswell, SVP Product and Solutions Marketing at Nutanix

Nutanix customers worldwide are leveraging NKP to innovate faster with an open, CNCF-compliant cloud native stack that enables platform engineering teams to operate Kubernetes clusters securely and consistently. A leading North American financial services firm, featured in a video case study, highlighted the

platform’s ability to reduce operational complexity by simplifying monitoring and management of containers.

In India, Karnataka Bank is running critical business applications—including mobile and internet banking, fraud and risk management, and loan management—on the Nutanix Cloud

Platform (NCP) with Kubernetes support. The bank also uses NCP for a digital currency application mandated by the Reserve Bank of India. Venkat Krishnan, CIO of Karnataka Bank, said: “Our customers are digitally savvy, so this requires us to quickly roll out and provide cloud native applications that

are easy to use, can be easily updated, and are always available. Nutanix’s platform, ability to support Kubernetes, and professional services enable us to deploy the applications required by the marketplace we serve and regulators.”

Nutanix further expanded its container innovation earlier this year

with the launch of its Cloud Native AOS solution, extending Nutanix’s enterprise storage and advanced data services to hyperscaler Kubernetes services and bare metal cloud native environments—without the need for a hypervisor. Cloud Native AOS is now available globally.

ODC AFRICA AND ME PARTNERS WITH HEDERA AFRICA HACKATHON TO BOOST WEB3 INNOVATION

The Orange Digital Center (ODC)

network in Africa and the Middle East, a key driver of digital inclusion serving young people and entrepreneurs across the region, announces a partnership with the Hedera Africa Hackathon. The hackathon is organised by The Hashgraph Association (THA) and Exponential Science, two non-profit organisations committed to advancing decentralised technologies and innovation, and operated by Dar Blockchain, a leading Pan-African Web3 hub.

Together, these partners aim to foster the adoption of decentralised technologies, education, and innovation through the Hedera Africa Hackathon, a continent-wide competition designed to develop and reward the most promising blockchain solutions, with prizes worth over one million dollars.

Blockchain training at scale

Central to the initiative is a certifying training programme in Hedera technology—deployed across Orange Digital Centers (ODCs) in the Middle East and Africa.

The online course is designed to upskill young professionals and entrepreneurs in Web3 and distributed ledger technologies, providing the technical foundation required to participate in the hackathon.

This effort reflects Orange’s continued commitment to digital inclusion and its long-term vision of empowering the next generation of African tech leaders. The Hashgraph Association, a Swiss non-profit driving adoption of the Hedera network,

and Dar Blockchain, a pan-African Web3 hub, will support the technical and strategic components of the training.

Hybrid hackathon across 16 countries

The Hedera Africa Hackathon will be hosted both virtually and through in-person hubs at Orange Digital Centers. Participants will gain access to physical infrastructure, mentoring support, and networking opportunities with ecosystem experts.



Co-organised with the Exponential Science Foundation, the competition is focused on developing real-world applications using the Hedera network—ranging from digital identity to transparent supply chains and secure financial services.

The organisers emphasise the event’s ambition not only to reward innovation but to build a sustainable pipeline of blockchain talent across Africa and the Middle East.

SANS INSTITUTE BRINGS CYBER LEADERS FORUM BACK TO RIYADH THIS AUGUST

The SANS Institute is set to return

to the Kingdom's capital with the fourth edition of its Cyber Leaders Forum from August 24 to 28, 2025. Taking place at the Hyatt Regency Riyadh Olaya, the event will offer five days of high-impact leadership and technical training, tailored for security managers and SOC leaders facing today's complex cyber threats.

This year's forum builds on Saudi Arabia's rising status as a global cybersecurity frontrunner. In 2025, the Kingdom secured the top position in the IMD World Competitiveness Yearbook's cybersecurity indicator, a milestone achieved through concerted national efforts led by the National Cybersecurity Authority and the Saudi Information Technology Company (SITE). Their strategic initiatives have not only boosted local cyber resilience but have also reinforced international partnerships and technology localisation.

"Saudi Arabia's position as a global cybersecurity leader is no coincidence, it's the result of strategic vision and long-term commitment," said Ned Baltagi, Managing Director, Middle East, Africa, and Turkey at SANS Institute. "At SANS, we're proud to support this progress by bringing world-class training to Riyadh



Ned Baltagi, Managing Director, Middle East, Africa, and Turkey at SANS Institute

through our Cyber Leaders event, helping to develop the next generation of cybersecurity leadership in the Kingdom."

Leadership-focused courses for strategic security professionals

The Riyadh training event will feature specialised courses aligned with the needs of InfoSec leaders. These include:

- **LDR512:** Security Leadership Essentials for Managers, aimed at helping professionals strengthen strategic planning and leadership abilities.
- **LDR514:** Security Strategic Planning,

Policy, and Leadership™, offering tools for building comprehensive cybersecurity plans and policies.

- **LDR551:** Building and Leading Security Operations Centers™, focused on SOC development and aligning operations to enterprise risk profiles.

Each course incorporates 17 hands-on labs and Cyber42 leadership simulations, ensuring participants gain both conceptual knowledge and practical skills. Attendees can join either in person or via live online sessions.

Community Night Talk: Focus on crypto mining threats

As part of the event, the Cyber Leaders Community Night Talk will take place on August 25 from 5:30 PM to 6:30 PM. Delivered by expert instructor Jan D'Herdt, the session will explore the detection of unauthorised cryptocurrency mining in corporate environments—an emerging risk with serious implications for enterprise networks.

This open-access session offers a practical platform for cybersecurity professionals in Saudi Arabia and beyond to enhance their threat detection capabilities. Online attendance is also available through SANS Accounts.

SENTINELONE NAMED LEADER IN GARTNER MAGIC QUADRANT FOR EPP FOR FIFTH CONSECUTIVE YEAR

SentinelOne, a global leader in AI-powered security, has been recognised as a Leader in the 2025 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP). This achievement marks the fifth consecutive year that the company has been positioned in the Leaders Quadrant, underscoring its

continued dominance in autonomous, AI-driven protection across endpoint, cloud, and data environments.

The latest recognition builds on multiple accolades from Gartner, including Customers' Choice honours in the Voice of the Customer for Extended Detection and Response (XDR) in 2025,

Cloud-Native Application Protection Platforms (CNAPP) in 2024, and Managed Detection and Response (MDR) in 2024. SentinelOne was also highlighted as a Strong Performer in Cloud Security Posture Management tools (CSPM), validating the strength of its unified agent and agentless approach.

"We think our fifth consecutive year as a Leader in the Gartner Magic Quadrant reflects our commitment to help customers defend against and outpace today's adversaries by replacing legacy tools with modern AI-native, autonomous protection," said Ric Smith, President and Chief Product & Technology Officer, SentinelOne.

SentinelOne continues to scale by equipping enterprises, government agencies, and service providers with integrated, reliable, and advanced solutions. Its Singularity Platform remains a benchmark in modern security—trusted to prevent breaches, reduce complexity, and secure operations without compromise.

This year, SentinelOne strengthened its vision for the AI-driven SOC with major milestones, including:



Ric Smith, President and Chief Product & Technology Officer at SentinelOne

- A preview of the next generation of Purple AI at RSAC 2025, introducing advanced agentic detection and response.
- Recognition as the Best Endpoint Security Solution at the 2025 SC Awards.
- The launch of Singularity Hyperautomation, delivering no-code, AI-powered workflow automation for security teams.
- Achieving FedRAMP High Authorisation for key offerings, including Purple AI, Singularity Endpoint, Singularity Cloud Security, and Singularity Hyperautomation.

SentinelOne's continued recognition highlights its architectural and reputational advantage, ensuring customers and partners have the most advanced defence against cyber threats while driving business resilience and reducing risk.

RANSOMWARE IN THE CROSSHAIRS: SOPHOS, HALCYON ANNOUNCE NEW INTELLIGENCE-SHARING AND MUTUAL ANTI-TAMPER PROTECTION INITIATIVE

Sophos, a global leader of innovative

security solutions for defeating cyberattacks, today announced a strategic threat intelligence sharing partnership with Halcyon, the leading anti-ransomware solution provider. This collaboration brings together two of the most experienced teams in ransomware defense to accelerate detection, enhance protection, and improve response capabilities for more than 300,000 organisations worldwide.

The collaboration between Sophos and Halcyon will exchange threat intelligence in real time, including indicators of compromise (IOCs), adversary behaviors, and attack patterns, to enhance ransomware prevention and accelerate response time. Following Halcyon's recent announcement of a community-focused Ransomware

Research Center, this data-sharing initiative will inform defenses across both Sophos' and Halcyon's solutions. It will benefit customers using Sophos Endpoint powered by Intercept X, as well as Sophos Managed Detection and Response (MDR), Sophos XDR, Halcyon's Anti-Ransomware Platform, and other joint capabilities.

Halcyon and Sophos will also implement mutual anti-tamper protections that allow each platform to monitor and safeguard the other's agents in customer environments. This helps ensure that organisations using both solutions benefit from added resilience, reducing the risk of ransomware interfering with security defenses and preserving the integrity of their overall protection strategy.

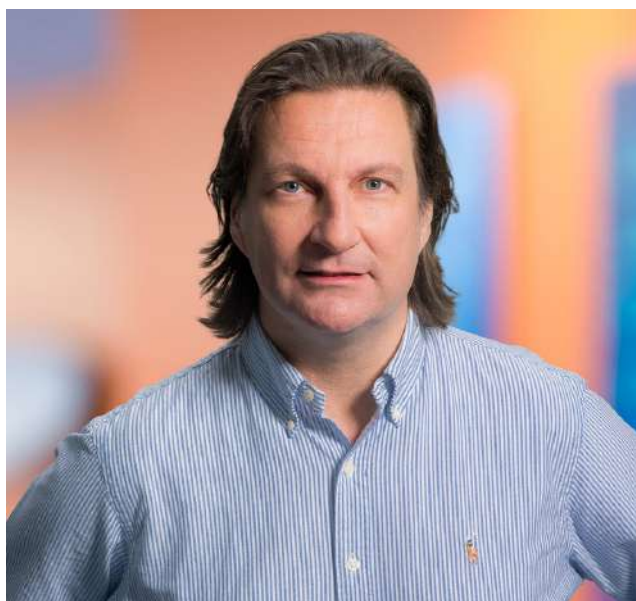
The threat intelligence collaboration is part of Sophos' broader strategy to

expand the reach and speed of its threat response through strategic partnerships. Sophos X-Ops, the company's cross-functional threat intelligence unit, will work closely with Halcyon's research and engineering teams to share and operationalise ransomware-related insights across a wide array of attack surfaces.

"Ransomware tools and tactics are evolving constantly, and the best defense is timely, relevant intelligence that enables defenders to act quickly and with confidence," said Simon Reed, chief research and scientific officer, Sophos. "By sharing insights with Halcyon, we're improving signal fidelity and accelerating detection across our systems, which strengthens protection for all the organisations we serve."

"Halcyon is honored to partner with

Sophos. Over the last four years, based on our telemetry, Sophos has time and time again proven to be one of the most effective endpoint security platforms we have encountered, reliably performing and disrupting attackers at a level that simply outperforms the majority of the players in the next-generation antivirus and endpoint detection and response (EDR) space. Their dedication to innovate and roll out industry-leading and unique features continues to put their customers at an everyday advantage over the most sophisticated attacks affecting enterprises today,” said Jon Miller, CEO and co-founder of Halcyon.



Simon Reed, chief research and scientific officer, Sophos.

Key benefits of the collaboration between Sophos and Halcyon include:

- Real-time ransomware intelligence: Sophos and Halcyon will share timely threat intelligence, including

indicators of compromise (IOCs), attacker behaviours, and tools used in active ransomware campaigns. This intelligence supports earlier detection, broader visibility, and more informed responses.

- Strengthened defences across products and services: Shared intelligence will enhance threat detection models, enrich contextual telemetry, and accelerate protection updates within each company’s solutions, including Sophos Central and Halcyon’s Anti-Ransomware Platform.
- Mutual anti-tamper protections: Each solution actively monitors the other’s agents to prevent tampering or disablement during ransomware attacks, helping ensure that security defences remain intact and effective throughout an incident.

This collaboration highlights Sophos’ and Halcyon’s continued commitment to cybersecurity innovation, industry cooperation, and the mission to defeat cybercriminals. Together, Sophos and Halcyon are delivering the intelligence needed to stay one step ahead of attackers.

TENABLE RECOGNISED MAJOR PLAYER IN IDC MARKETSCOPE FOR CLOUD-NATIVE APPLICATION PROTECTION

Tenable, the exposure management company, has been named a Major Player in the inaugural IDC MarketScape: Worldwide Cloud-Native Application Protection Platform (CNAPP) 2025 Vendor Assessment.

The designation underscores Tenable’s strategic approach to cloud security and its ability to deliver actionable visibility across the modern attack surface. The IDC MarketScape assessment evaluated vendors based on a rigorous framework that considered product capabilities, strategy, and customer feedback.

The report highlights Tenable Cloud Security’s ability to provide critical visibility and actionable insights that



Eric Doerr, Chief Product Officer at Tenable, says the recognition affirms Tenable’s cloud security vision and innovation.

enable organisations to prioritise vulnerabilities and protect sensitive data across multi-cloud environments. The solution integrates seamlessly with Tenable One, delivering a complete CNAPP offering out of the box—spanning infrastructure, workloads, identities, data and AI.

“Tenable Cloud Security provides visibility information tailored to specific cloud providers like AWS, GCP, Azure, and Oracle Cloud,” the report states. “Each cloud risk finding is explained with its context, detailing the criticality level based on impact and likelihood

of exploitation. Specific remediation guidance is provided.”

Through identity-intelligent risk analysis, context-rich prioritisation, and automated remediation workflows, Tenable enables collaboration between security and DevOps teams while eliminating tool sprawl. Fast deployment and unified insights help accelerate risk reduction across both cloud and on-premises environments.

“We believe being named a Major Player in the first-ever IDC MarketScape for CNAPP is a powerful validation of our strategy and our

commitment to helping customers understand and reduce risk across not only their cloud environments, but their entire attack surface,” said Eric Doerr, Chief Product Officer at Tenable. “It’s about providing the context and intelligence that enables organisations to prioritise what matters and proactively remediate flaws before they can be exploited.”

Tenable continues to expand its capabilities in response to growing cloud complexity and the need for integrated, intelligence-driven exposure management.

VECTRA AI NAMED ‘LEADER’ IN FIRST-EVER GARTNER MAGIC QUADRANT FOR NDR

Vectra AI, Inc., the cybersecurity AI

company that protects modern networks from modern attacks, announced it was named a Leader in the 2025 Gartner Magic Quadrant for Network Detection and Response (NDR).

Vectra AI is positioned highest for ability to execute and furthest for completeness of vision, and is the only vendor in the report to be named a leader in both the Gartner Magic Quadrant for NDR and a Customer Choice Winner for NDR in the 2024 Gartner Peer Insights Voice of the Customer.

The Vectra AI Platform is purpose-built to defend modern hybrid environments from identity and network-based attacks. As threats accelerate across cloud, data center, remote, and OT domains, Vectra AI provides comprehensive coverage to reduce attack exposure. Its AI agents continuously triage, correlate, and prioritise real threats in real time – eliminating alert fatigue and accelerating response. With Vectra AI,

defenders gain control to detect, hunt, investigate, and respond to attacks across the full threat landscape, enabling security teams to focus on maturing their security posture.

“Gartner’s decision to publish a Magic Quadrant for NDR reflects just how essential this market has become in modern cyber defense,” said Hitesh Sheth, founder and CEO of Vectra AI.

“Being recognised as a Leader in this inaugural report reinforces Vectra AI’s position at the forefront of this critical space. As organisations grapple with growing complexity, identity-based attacks, and AI-driven threats, the Vectra AI Platform delivers what modern defenders need – coverage that reduces exposure, clarity that cuts through the noise, and control to act with speed and confidence,” added Sheth.

Vectra AI has been recognised by customers for outstanding product performance and support, earning the distinction of Customers’ Choice in the 2024 Gartner Peer Insights Voice of the Customer for Network Detection and Response. As of January 2024, Vectra AI holds a 4.8 out of 5 rating based on 96 reviews, with 96% of customers saying they would recommend the platform. This recognition reflects Vectra AI’s deep commitment to customer success and ongoing innovation in protecting modern networks from modern attacks.





ISACA
UAE Chapter

&
tahawultech.com
presents

INFOSEC & CYBERSECURITY CONGRESS 2025

Securing the Intelligent Age

📅 **16th September 2025**

📍 **VOGO Abu Dhabi Golf Resort & Spa**

🕒 **09:00 AM onwards**

SECURING THE INTELLIGENT AGE: BUILDING CYBER RESILIENCE FOR TOMORROW'S DIGITAL ENTERPRISES

The rise of intelligent technologies, AI-driven systems, and connected infrastructures has transformed cybersecurity into a boardroom priority. Security and risk leaders are now expected to be innovation champions—guiding organizations through complex digital environments while ensuring resilience, trust, and regulatory alignment.

The **Infosec & Cybersecurity Congress 2025**, hosted by **ISACA UAE Chapter** and **Tahawultech.com**, provides a powerful platform for meaningful discussions, real-world case studies, and forward-looking strategies. Industry leaders, CISOs, regulators, and innovators will converge to explore next-gen governance models, risk frameworks, and tech-driven defense mechanisms.

Join us on **16th September 2025** at **VOGO Abu Dhabi Golf Resort & Spa**,
and be part of the movement shaping the future of secure digital transformation.

GOLD SPONSOR

Delinea
Securing identities at every interaction

SILVER SPONSOR

tekSalah

OFFICIAL PUBLICATIONS

cnme
computer news middle east

Reseller MIDDLE EAST
THE VOICE OF THE CHANNEL

Security MIDDLE EAST

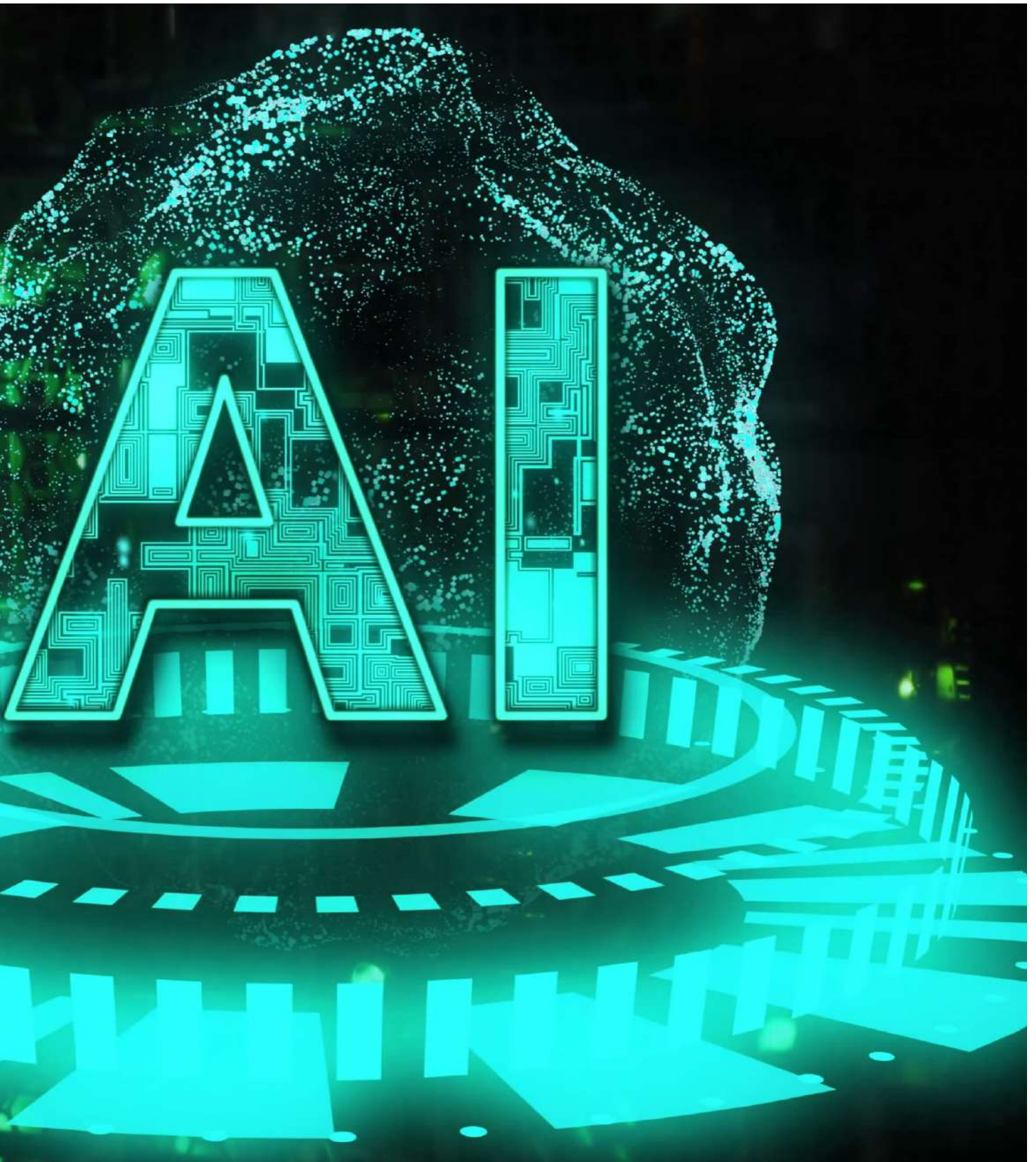
HOSTED BY

tahawultech.com

#infosec&cybersecuritycongress2025 | #tahawultech | #isacauaechapter

AI IN CYBERSECURITY: BALANCING INNOVATION WITH HUMAN OVERSIGHT

AS 98% OF ORGANISATIONS EMBED AI INTO THEIR DEFENCES, LEADERS WARN THAT GENERATIVE AI OFFERS BOTH PROMISE AND PERIL, DEMANDING ACCOUNTABILITY, TRANSPARENCY, AND STRONGER HUMAN-AI COLLABORATION.



Artificial Intelligence (AI) is redefining the rules of cybersecurity, transforming it from a defensive discipline into a race against evolving threats. Cybercriminals are weaponising AI to craft highly sophisticated attacks, putting enterprises under mounting pressure to harness the same technology for defence — but without crossing ethical, regulatory, and operational boundaries.

Shadi Khuffash, Senior Regional Director, South Middle East, Fortinet, said, “AI-driven cybersecurity solutions have quickly moved from a nice to have to necessity as AI is exploited by malevolent actors. We are already seeing the weaponisation of AI with attackers creating sophisticated attacks that can evade traditional cybersecurity measures in addition to exploiting vulnerabilities in AI systems by means such as data poisoning and adversarial attacks that can compromise the integrity and privacy of Large Language Model (LLM) data.

Over the next five years, Khuffash cautions, “we will experience a doubling down on development of AI-powered cybersecurity solutions that focus on proactively defending against emerging threats, enabling rapid detection and response to threats and automating security and network operations”.

Already, AI threads through many systems, from Security Information Management (SIEM), security orchestration, automation and response (SOAR), Security Operations Center, and more, where AI helps to correlate, triage, and report weaknesses and can predict where attackers could hit.



Shadi Khuffash
Senior Regional Director
South Middle East, Fortinet.

Enterprises in the Middle East face the challenge of tackling sophisticated cyberattacks while ensuring ethical and compliant use of AI. This demands cybersecurity partners offering three key pillars: robust defence against known and emerging AI-driven threats, proactive and automated SOC and NOC capabilities to streamline operations, and strong safeguards to secure AI models and prevent LLM data leakage — all while staying aligned with evolving regulations to protect privacy and confidentiality, added Khuffash.

While Khuffash highlights the urgent need for AI-powered defences and structured frameworks, other experts

caution that the rapid adoption of AI also brings its own set of challenges. Rob T. Lee, Chief of Research at the SANS Institute, urges enterprises to look beyond the hype and approach AI solutions with a critical eye. He notes that while AI offers enormous potential, many tools currently marketed as “AI-driven” often fall short of true innovation, and defenders face the added complexity of operating under strict regulatory frameworks — a constraint that attackers, using unrestricted AI, don’t have to contend with.

Lee said, “The technology is still evolving, and its actual benefits require thorough academic research. When implemented effectively, agentic and automation solutions offer significant advantages, although currently many applications focus primarily on logfile aggregation — a task potentially better suited to established machine learning approaches. It is advisable to critically assess vendor claims, as there is a tendency to label products

AI-DRIVEN CYBERSECURITY SOLUTIONS HAVE QUICKLY MOVED FROM A NICE TO HAVE TO NECESSITY AS AI IS EXPLOITED BY MALEVOLENT ACTORS
SHADI KHUFFASH, SENIOR REGIONAL DIRECTOR, SOUTH MIDDLE EAST, FORTINET.

as ‘AI,’ reminiscent of the proliferation of ‘powered by Windows 95’ branding in past decades. Initiatives such as SecGemini are encouraging, yet they necessitate further testing to confirm their efficacy.”

Building on this, Lee highlights a growing imbalance between attackers and defenders. While adversaries freely exploit unrestricted large language models to launch sophisticated, AI-driven attacks, defenders operate under strict rules and evolving privacy regulations like GDPR and NIS2. Such compliance requirements, though vital for safeguarding data and user rights, can limit defenders’ speed and flexibility, ultimately giving attackers a significant tactical edge in the cybersecurity battlefield.

Fresh data from the SANS Institute reinforces Lee’s caution, underscoring how humans remain the weakest link in cybersecurity. Its 10th Security Awareness Report, based on insights

from over 2,700 practitioners worldwide, found that 80% of organisations identify social engineering as the top human-related risk — a threat now amplified by AI-powered phishing, smishing, and vishing attacks. The report also noted a rise in risks linked to mishandling sensitive data, weak passwords, and poor authentication, reflecting how attackers are exploiting human behaviour in more sophisticated ways. Despite progress, security teams continue to face resource and staffing constraints, with the most mature programmes requiring sustained investment and at least 2.8 dedicated staff. Lance Spitzner, Technical Director at SANS, noted that the findings highlight that “human risk is still under-reported, yet it remains one of cybersecurity’s most urgent challenges” in the age of generative AI and deepfakes.

Lee’s concerns about hype and imbalance are echoed in recent data. A Sophos report, “Beyond the Hype: The Business Reality of AI for Cybersecurity,”

found that while 65% of IT leaders have already adopted GenAI, an overwhelming 89% worry flaws in these tools could undermine their security strategies. The survey also revealed that 87% fear accountability gaps and 84% are concerned about headcount reductions due to unrealistic expectations about AI replacing humans. Interestingly, smaller firms valued GenAI for reducing burnout, while larger organisations prioritised stronger protection. This reflects the “double-edged sword” of AI that Mayuresh Kothari, Advisory Solution Principal at Sophos, highlights — an innovation that can empower teams but, without oversight, risks causing more disruption than it prevents.

For Kothari, AI represents a transformative opportunity to empower cybersecurity teams, close critical skills gaps, and free up valuable time by automating repetitive tasks. However, he warns that without proper safeguards like explainable AI, transparency, and

**THE TECHNOLOGY IS
STILL EVOLVING, AND
ITS ACTUAL BENEFITS
REQUIRE THOROUGH
ACADEMIC RESEARCH**

**ROB T. LEE, CHIEF OF
RESEARCH AT THE
SANS INSTITUTE**

Rob T. Lee
Chief of Research at the SANS Institute



SHORTAGE OF SKILLS IS THE BIGGEST GAP THAT AI WILL BE LOOKING TO FIX. I KNOW THIS BRINGS ABOUT FEAR AND PARANOIA THAT THE JOBS WILL BE TAKEN AWAY BY MACHINES, BUT THAT'S NOT ACCURATE ATLEAST FOR NOW
MAYURESH KOTHARI, ADVISORY SOLUTION PRINCIPAL AT SOPHOS

Mayuresh Kothari
Advisory Solution Principal at Sophos



human oversight, the technology could unintentionally cause widespread disruption, including risks to critical infrastructure.

Kothari said, "AI is going to be a double-edged sword in cybersecurity. One of the biggest opportunities for its application in Cyber is the empowerment of the Security Operator. For years now market analysts, IT Leaders and even Security Professionals themselves have been talking about resource crunch. Shortage of skills is the biggest gap that AI will be looking to fix. I know this brings about fear and paranoia that the jobs will be taken away by machines, but that's not accurate atleast for now. All security functions will get augmented by AI, not replaced. It will give back to security professionals a rare commodity, time. However, the flip side of it is that if improperly done, it may cause the most disruption. We all know how big

an impact cyber disruption can have on the real world. Last year's incident is fresh on everyone's mind. Imagine if an unsupervised AI bot were to switch off critical installations such as power plants or water supplies just to protect them. Guard rails for AI such as Explainability, Transparency and Human Oversight are key to making safe and secure deployment. And hasty adoption of AI without these insights would hamper not just in the short term but also in the long term acceptability."

Kothari addresses the growing challenge for enterprises in the Middle East: how to balance the power of generative AI with ethical, transparent, and regulation-compliant deployment. He points out that cybercriminals are using the same AI tools but in unstructured and unregulated ways, giving them a tactical advantage.

Kothari said, "First of all, we need to

remember that threat actors are using the same set of tools as us but in a far more unstructured and unregulated or supervised manner. While the effectiveness of these outcomes are something that only threat actors know, they still work without any hindrance from regulation or oversight. So, defending against such antagonists requires us, the security providers, to step up our game while still ensuring we do it responsibly and ethically. Having said that, organisations need to ensure that they do things right the first time and every time. As mentioned above, Explainable AI is one of the key concepts that has come to the forefront when organisations are adopting and implementing AI in their ecosystems. Just like in the physical world, in the world of AI, trust should be paramount for a seamless integration of agents. Human-in-the-loop also

plays a significant role in ensuring that explainability is maintained while improving efficiency. Not at the cost of it.”

Four critical steps for organisations:

- Empower IT and security teams to actively participate in AI-driven decisions.
- Maintain strict quality controls over datasets used in AI model training.
- Adopt AI within a structured, monitored framework to prevent costly mishaps.
- Treat AI investments like any financial decision — weighing both short-term gains and long-term risks carefully.

Kothari’s emphasis on responsibility and explainability highlights the importance of placing human oversight at the centre of AI adoption. This idea of keeping people in control is echoed by other experts who argue that AI should be seen as an ally to human ingenuity, not a replacement for it.

TO ENSURE HUMAN CREATIVITY AND JUDGMENT REMAIN CRUCIAL AS AI ADVANCES, WE MUST PRIORITISE AI AS A TOOL FOR AUGMENTATION, NOT REPLACEMENT

GAVIN MILLARD, VP OF PRODUCT AT TENABLE

Building on this theme, Gavin Millard, VP of Product at Tenable, stresses that the most effective approach lies in using AI for augmentation — handling repetitive, data-heavy tasks so that security professionals can focus on complex problem-solving, innovation, and ethical decision-making.

Millard said, “To ensure human creativity and judgment remain crucial as AI advances, we must prioritise AI as a tool for augmentation, not replacement. This means designing systems where AI handles repetitive tasks, freeing humans to focus on complex problem-solving, innovation,

and ethical oversight. Educational initiatives should also emphasise critical thinking and adaptability alongside AI literacy. The cyber security threats from AI are multi-faceted, from sophisticated AI generated deep fake content that compels an employee into making a bank transfer, to simplistic AI generated malware to take advantage of known flaws through phishing attacks. The best approach to defend and mitigate these attacks are similar to cyber defense today - including preemptive exposure management to address the flaws attackers favour before they are leveraged and educate



Gavin Millard
VP of Product at Tenable

employees on suspicious requests, no matter how compelling they appear to be.”

AI has seamlessly integrated into our daily lives, transforming how we interact with technology and the world. From personalised recommendations on streaming services and e-commerce to the efficiency of GPS navigation and smart home assistants, AI simplifies countless tasks. It underpins predictive text, spam filters, and even advanced medical diagnostics, enhancing convenience and accuracy.

“In cybersecurity, AI plays a crucial role in analysing vast datasets of threat and activity information, enabling automated distinction between the risky and risk free. Furthermore, agentic AI is proving valuable in automating repetitive tasks to reduce the manual effort required to maintain secure infrastructures,” added Millard.

Millard’s call to treat AI as an augmentation tool rather than a replacement underscores a recurring theme among industry leaders: humans must remain at the heart of cybersecurity decision-making. A similar perspective is shared by Bernard Montel, EMEA Technical Director and Security Strategist at Tenable, who illustrates both the practical benefits and looming risks of AI.

Montel highlights how AI already



Bernard Montel
EMEA Technical Director and Security
Strategist at Tenable

underpins everyday life — from online recommendations to medical diagnostics — and is increasingly vital in cybersecurity for analysing massive datasets and automating defences. Yet, he cautions that the same technology is also being weaponised, powering everything from AI-generated deepfakes to automated phishing campaigns, making proactive exposure management

and continuous employee awareness training more important than ever.

Montel said, “Artificial intelligence has seamlessly integrated into our daily lives, from personalised recommendations and GPS navigation to predictive text and advanced medical diagnostics. In cybersecurity, AI is proving invaluable, analysing vast datasets to distinguish threats and automating repetitive tasks to maintain secure infrastructures. To truly harness the power of AI in our computing environments, organisations must champion AI as a tool for augmentation, not replacement. This means designing systems where AI handles repetitive tasks, freeing humans to focus on complex problem-solving, innovation, and ethical oversight. Prioritising human creativity and judgment is paramount as AI continues

to advance. Alongside AI literacy, educational initiatives should emphasise critical thinking and adaptability.”

The rapid advancement of AI also presents multifaceted cybersecurity threats, points out, Montel. “We’re seeing everything from sophisticated AI-generated deepfakes designed to trick employees into making fraudulent bank transfers to simplistic AI-generated malware leveraging known flaws through phishing attacks. The most effective approach to defending against and mitigating these threats mirrors current cyber defense strategies: preemptive exposure management to address vulnerabilities before they’re exploited, and robust employee education on suspicious requests, no matter how compelling they may seem,” concluded Montel. 📌

IN CYBERSECURITY, AI IS PROVING INVALUABLE, ANALYSING VAST DATASETS TO DISTINGUISH THREATS AND AUTOMATING REPETITIVE TASKS TO MAINTAIN SECURE INFRASTRUCTURES

BERNARD MONTEL, EMEA TECHNICAL DIRECTOR AND SECURITY STRATEGIST AT TENABLE

EXPAND NORTH STAR

12-15 October 2025

Largest
startup
event in
the world

Dubai
Harbour

MEET. PITCH. SCALE.
AT THE WORLD'S
#1 STARTUP-INVESTOR EVENT

INSPIRED BY

HOSTED BY

GITEX
GLOBAL

غرفة دبي
DUBAI CHAMBER
الرقمية DIGITAL

UAE HEALTH SECTOR TARGETED IN SOPHISTICATED RANSOMWARE ATTACK

I MAYURESH KOTHARI OF SOPHOS EXPLAINS HOW A CONTI OFFSHOOT IS EXPLOITING HEALTHCARE NETWORKS — AND WHY PROACTIVE INCIDENT RESPONSE IS ESSENTIAL.

Recent cyberattacks on the UAE's health sector have exposed the growing threat posed by ransomware groups targeting critical infrastructure. The latest incident, linked to the emerging Gunra group—believed to be a reconstitution of the dismantled Conti gang—used double extortion tactics involving the theft and encryption of sensitive personal and medical data. According to Mayuresh Kothari, Advisory Solution Principal at Sophos, the attackers exploited legitimate administrative tools to evade detection and launch a highly disruptive campaign.

In this interview, Kothari explores the threat landscape, the importance of engaging expert incident response teams, and why proactive cybersecurity planning is essential. He also outlines how Sophos is helping organisations in the Middle East improve readiness through integrated solutions and local investment.

Could you provide an overview of the recent cyberattacks targeting the UAE health sector?

Based on publicly available information from X (formerly Twitter) and claims made by the threat group on leak sites,

this incident appears to be a form of double extortion. The threat actor was able to first circumvent the security controls to establish presence in the network before starting to identify critical data, exfiltrate it out and lastly, encrypt. Since the threat actor claims to have stolen millions of records containing PII, PCI, and healthcare data, the potential consequences of this exposure are serious. The ransom demand includes payment for both data decryption and to prevent the public release of the stolen information.

Can you share more information about the threat group responsible?

The threat actor group known as Gunra has been active since early this year. Indicators suggest that this group has emerged from the remains of the Conti

ransomware group, which was recently disrupted by law enforcement agencies. At Secureworks, we have classified Conti under the codename Gold Ulrick. Their modus operandi involves leveraging windows administrator tools to hide malicious activities prior to conducting extortion operations.

What actions should organisations under attack take to effectively mitigate the impact of incidents like these?

This is a complex issue without a simple solution. To begin with, impacted organisations should engage professional incident response (IR) teams with comprehensive expertise in all aspects of managing such incidents. For instance, Secureworks, now part of Sophos, offers specialised services tailored to these needs. When an organisation engages us during an active incident, we begin by identifying the root cause or patient zero of the attack and then remove the threat actor and any associated artifacts. We also provide guidance to prevent future attacks. Our support extends to ransom negotiation, regulatory and communication advice around disclosure or with regulators, and establishing a long-term response program.

CYBERSECURITY IS A CONTINUOUS PROGRAMME — HOPE FOR THE BEST, BUT PREPARE FOR THE WORST.

Is this the only approach, or are there preventative measures organisations can implement today to proactively defend against such threats?

Cybersecurity is a multi-faceted discipline that organisations must approach as an ongoing program, one that is regularly reviewed, tested, improved, and repeated. Numerous frameworks today help assess the maturity and effectiveness of such programs. However, cybersecurity is always a team effort. It cannot be done in isolation. The foundation begins with strong preventative and policy enforcement controls. Take Sophos Endpoint Protection and Firewalls, for example. With nearly 40 years of experience delivering cutting-edge security controls, our approach known as Synchronised Security provides integrated, highly efficient protection. However, prevention is just the starting point. We must always hope for the best but prepare for the worst. That's where detection-based mechanisms become essential such as Vulnerability Management, Endpoint Detection and Response (EDR), and Managed Detection and Response (MDR). And even then, the process isn't complete. As we emphasised earlier, cybersecurity must be treated as a continuous program. This is where our Proactive Incident Response services lead the way, ensuring organisations are not just reacting to threats, but actively preparing for them.

What do you mean by Proactive Incident Response? Isn't incident response typically a reactive process?

Incident Response (IR) is not just the act of responding to a threat after it occurs. It also involves preparing for potential incidents in advance. This means having plans in place, conducting regular testing, and clearly defining the initial steps to be taken in the event of an attack. To put it into perspective, think of how emergency response works in the real world. Many workplaces designate first responders who wear high visibility jackets and helmets so they can be easily identified during an



Mayuresh Kothari
Advisory Solution Principal, Sophos.

emergency. These individuals are trained to use fire extinguishers, guide people to exits, and manage the initial response to a crisis. Cyber IR functions in the same way. Proactive services often delivered through a retainer focuses on this preparedness. It involves training internal first response teams on the actions to take during an incident: how to contain the threat, prevent its spread, and reduce the risk of data exfiltration. Beyond training, proactive retainers help organisations establish and review their incident response plans, define industry-specific playbooks, and conduct both technical and non-technical exercises. These activities help security teams identify gaps in their current processes and improve their overall readiness.

How does Sophos differentiate itself from other vendors offering similar solutions?

We are uniquely positioned to provide end-to-end solutions with tried and test capabilities across endpoint, network, cloud and services. Our secure by design and practice approach has consistently delivered results, and we remain committed to supporting the region through continued investment. Our latest initiative is the launch of a dedicated data center in the UAE, which will enable us to meet local data residency requirements while continuing to provide world-class security solutions tailored to our customers' needs. **i**

AI-DRIVEN CYBERATTACKS DEMAND MACHINE-SPEED DEFENCES, SAYS KITEWORKS CISO

FRANK BALONIS, CISO AND SVP OF OPERATIONS AT KITEWORKS, WARNS THAT COMPLIANCE-LED ORGANISATIONS MUST REPLACE HUMAN-DEPENDENT SECURITY WITH AUTOMATED, AI-ENABLED CONTROLS TO SURVIVE THE NEXT WAVE OF AUTONOMOUS CYBER THREATS.



Frank Balonis, CISO and SVP of Operations at Kiteworks.

AI-driven cyberattacks are reshaping the threat landscape with unprecedented speed, scale, and precision. Frank Balonis, CISO and SVP of Operations at Kiteworks, spoke to Sandhya D'Mello, Technology Editor, CPI Media Group about how traditional compliance frameworks and human-dependent controls are no match for autonomous

adversaries. Organisations must now adopt machine-speed defences, real-time data visibility, and automated enforcement to withstand AI-enabled threats. With regulatory demands increasing and the financial impact of breaches soaring, the path forward demands unified architectures, zero-trust strategies, and AI-powered anomaly detection to ensure both security and compliance.

The recent research demonstrates AI's ability to autonomously execute complex network attacks with alarming precision and scale. How do you see this redefining the cybersecurity threat landscape for compliance-driven organisations?

The convergence of autonomous AI attack capabilities and organisational vulnerability creates an unprecedented compliance crisis. Carnegie Mellon and Anthropic research proves AI can autonomously breach networks with 100% success rates, while 83% of organisations lack basic controls against AI data exposure. This redefines the threat landscape fundamentally. Attacks now operate at machine speed 24/7, systematically exploiting hundreds of vectors simultaneously while, per IBM, shadow AI incidents cost \$670,000 more than standard breaches. With 59 new AI regulations in 2024 and fines exceeding \$100,000 becoming common, compliance-driven organisations face a stark reality: deploying AI-enabled security isn't optional anymore. For healthcare, financial services, and any entity handling sensitive data, machine-speed defenses have become the minimum viable protection against adversaries that never sleep, never forget, and scale infinitely across attack surfaces.

What makes traditional data loss prevention (DLP) and regulatory compliance frameworks ineffective against such AI-driven attacks?

Traditional DLP and compliance frameworks fail against AI-driven attacks because they were designed for predictable, human-speed threats within controlled environments. The research reveals fundamental mismatches. DLP relies on signature-based detection, but AI attackers generate novel attack vectors in real-time that never existed before, rendering pattern databases obsolete. While security teams investigate alert #1, AI has already executed attacks #2 through #50 at machine speed. Most critically, compliance frameworks like GDPR and HIPAA require tracking all data processing activities. Yet, 86% of organisations are blind to their AI data flows. With employees routinely sharing sensitive data through 1,200+ shadow AI applications. The fragmentation compounds failure: organisations average 15,000 ghost users and 176,000 inactive identities that AI can exploit, while disconnected security tools create visibility gaps. Traditional controls – training (40% adoption), policies (10%), and warnings (20%) – provide zero protection against autonomous systems that methodically catalog every vulnerability and execute multistage attacks with surgical precision.

From a compliance standpoint, what immediate controls or policies must be re-evaluated or re-implemented in light of this development?

From a compliance standpoint, organisations must immediately shift from human-dependent controls to

automated technical enforcement. The research proves only 17% of organizations with automated blocking survive AI attacks. Training, policies, and warnings provide zero protection.

Critical re-evaluations are required in regard to:

Access Controls: deploy automated AI-specific blocking, as 97% of breached firms lacked proper controls.

Audit Trails: establish forensic-quality tracking for GDPR/HIPAA compliance, since 60% can't respond to data requests.

Real-time Classification: only 10% have properly labeled files required for compliance.

Unified Governance: consolidate fragmented tools into command centers tracking data lineage through AI processing.

The mandate is clear. Compliance requires machine-speed technical controls, not human measures that fail universally.

What architectural shifts should organisations consider to secure sensitive content when attackers operate at machine speed and scale?

Organisations must architect for machine-speed defense through four fundamental shifts. Unified Command Centers should be used to consolidate fragmented security tools into platforms providing total visibility, as AI exploits blind spots between disconnected systems. Automated Technical Controls should be used to deploy blocking and scanning at machine speed, since only 17% with these controls survive AI attacks while human-dependent measures fail universally. Zero-Trust

Data Architecture implements controls that verify every access in real-time, as AI systematically exploits trust relationships and 15,000 ghost users in typical enterprises. AI-vs-AI Defense Layers includes AI-powered anomaly detection that learns organisational patterns and responds in milliseconds, not hours, matching attacker capabilities.

The architectural imperative here is to shift from perimeter-based human-speed security to data-centric machine-speed protection that follows sensitive information wherever it flows. With forensic-quality audit trails satisfying regulatory requirements while defending against adversaries that operate 24/7 at inhuman precision.

Given the scale and memory capabilities of AI-driven attacks, what practical steps would you recommend to CISOs and compliance heads to strengthen their defence posture and ensure regulatory readiness?

CISOs and compliance heads need three critical defenses against AI's perfect memory and infinite scale.


Immediate (0-30 days): Deploy automated blocking and anomaly detection, as only 17% with these controls survive AI attacks. Establish zero-trust verification for every access since AI catalogs all discovered credentials.

Consolidate (30-90 days): Unify fragmented tools into a single platform eliminating blind spots between 1,200+ shadow applications. Deploy AI-powered defense responding in milliseconds, not hours.

Compliance (90+ days): Implement forensic audit trails for every data movement, automated classification, and real-time reporting. Success metrics: sub-second detection, 100% audit coverage, minutes-to-containment.

The mandate here is to match AI's machine speed and memory with equally capable defenses. Human-dependent measures guarantee failure. **1**

TRADITIONAL CONTROLS – TRAINING (40% ADOPTION), POLICIES (10%), AND WARNINGS (20%) – PROVIDE ZERO PROTECTION AGAINST AUTONOMOUS SYSTEMS THAT METHODICALLY CATALOG EVERY VULNERABILITY AND EXECUTE MULTISTAGE ATTACKS WITH SURGICAL PRECISION.

A portrait of Dr. Víctor Mateu, a man with a beard and short hair, wearing a dark blue blazer over a black t-shirt. He is looking directly at the camera with a slight smile. The background is a dark, textured wall.

Dr. Víctor Mateu
Chief Researcher Cryptography
Research Center at Technology
Innovation Institute.

**GOVERNMENTS AND BUSINESSES CAN NOW
PLAN THEIR TRANSITION TO POST-QUANTUM
CRYPTOGRAPHY (PQC) TO ENSURE LONG-TERM DATA
SECURITY AGAINST QUANTUM-ENABLED THREATS.**

HOW TO NAVIGATE THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

ITENABLE LAUNCHES AI EXPOSURE TO PROVIDE UNIFIED VISIBILITY, RISK MANAGEMENT AND GOVERNANCE FOR GENERATIVE AI TOOLS LIKE CHATGPT ENTERPRISE AND MICROSOFT COPILOT.

Security professionals worldwide are preparing for a major upgrade in the form of a migration to new post-quantum cryptographic standards as the era of quantum computing comes closer to reality.

The U.S. National Institute of Standards and Technology (NIST) has been leading a standardisation process to transition from classical public-key cryptosystems to quantum-resistant alternatives.

Governments and businesses can now plan their transition to post-quantum cryptography (PQC) to ensure long-term data security against quantum-enabled threats.

However, this shift must be approached with caution to avoid unintended vulnerabilities.

Recent research from the Technology Innovation Institute (TII)'s Cryptography Research Center (CRC) in Abu Dhabi and Polytechnic University of Turin highlights a key concern: solutions that rely on variants of computationally hard problems used in the design of PQC algorithms to enhance their performance or to provide added functionalities require additional scrutiny.

An example is the Linear Code Equivalence (LCE), which plays a role in PQC signature schemes.

The study, Don't Use it Twice! Solving Relaxed Linear Code Equivalence

Problems warns that modifying computational problems, even slightly, can significantly change their complexity, sometimes making them solvable with today's technology.

This is a caution to designers of new designs to double-check that tweaks they introduce don't lead to weaker security guarantees than intended.

Lessons from the Linear Code Equivalence Problem

LCE, a computational assumption consisting of two linear codes that are equivalent up to a linear transformation, has been studied by cryptanalysts and is used to construct secure cryptosystems like digital signatures. The research warns against using relaxed versions of LCE in cryptographic applications without rigorous security validation, which could lead to vulnerabilities.

A key takeaway is that even for well-established hard problems, providing additional data, such as multiple instances of a problem that share the same secret, can make it easier for attackers to recover the secret information. This serves as a reminder to designers that seemingly minor adjustments to cryptographic structures can unintentionally reduce security.

While the study highlights potential vulnerabilities, it by no means suggests abandoning PQC development. Instead,

organisations should begin transitioning to quantum-safe cryptography while keeping in mind the importance of careful validation and measured adoption.

For example, security practitioners should focus on rigorous cryptanalysis to assess the long-term security of any PQC scheme built on novel or modified computational problems.

They must also avoid relying on less studied assumptions or at least approach them with skepticism to ensure that relaxations of problems don't introduce unintended vulnerabilities.

The transition to PQC should be a gradual process, informed by ongoing cryptanalysis and contributions from the global cryptographic community. The process will also go through refinements as a natural part of its journey in the coming years.

The Road Ahead

The industry must navigate this shift with an understanding that cryptographic design is inherently iterative. New threats emerge and countermeasures must adapt accordingly.

Governments and organisations embarking on their PQC migration journey must recognise that while PQC is still maturing, it presents an exciting opportunity to build a stronger, more resilient cryptographic foundation for the future. **1**



Mohannad Abuissa
Director of Solutions Engineering and CTO
for Cisco in the Middle East and Africa

FUTURE-PROOFING THE UAE: HOW AI- DRIVEN NETWORKS ARE POWERING INNOVATION, RESILIENCE, AND ECONOMIC GROWTH

The UAE is accelerating its transformation into a global hub for innovation, smart infrastructure, and digital excellence, making reliance

on robust, secure network connectivity more critical than ever. The nation's ambitious investments in artificial intelligence (AI), cloud computing, and cybersecurity are positioning it at the forefront of digital evolution, driving its vision for a knowledge-based economy.

The UAE's focus on innovation and seamless digital operations, from smart cities to tech hubs, means that any disruption carries widespread consequences across critical sectors.

According to Cisco's latest global networking report, insights from over 8,065 senior IT and business leaders worldwide, including more than 250 in the UAE, reveal a stark reality: just one severe network outage per organisation each year can cause a staggering economic loss of billions globally.

Downtime's true cost goes beyond money

While it's easy to consider downtime mainly as a financial loss, its true effects run far deeper. Beneath the numbers lies a more significant problem: each outage erodes trust, hampers productivity, and diminishes future opportunities. When the network fails, supply chains are disrupted, customer service suffers, and the company's reputation can be damaged.

IT leaders in the UAE are already delivering financial value from today's networks – largely by improving customer experiences (59%), boosting efficiency (57%), and enabling innovation (56%). But much of that value is at risk if it comes from infrastructure that hasn't been designed for AI or real-time scale.

To unlock the full growth and savings they expect, leaders have identified critical gaps they must close: siloed or partially integrated systems (64%), incomplete deployments (55%), and reliance on manual oversight (50%). Smarter, more secure, more adaptive



networks are the business case for investment. 96% say improved networks will directly drive revenue, and 97% expect meaningful cost savings – driven by smarter operations, fewer outages, and lower energy use.

AI is transforming networks — and elevating the risks

AI is transforming networks — and raising the stakes. The rise of AI assistants, autonomous AI agents, and data-driven workloads is fundamentally changing how work gets done, but it's also generating network traffic that is more complex, unpredictable, and demanding than ever before. These applications require vast bandwidth and

ultra-low latency to support real-time and near real-time processing.

Our research reveals that 67% of respondents say their current data centres can't fully support AI requirements, and 92% intend to boost capacity—whether on-premises, in the cloud, or both.

This significant investment shift reflects the nation's commitment to becoming a global AI leader. This is not just about managing more data; it's about enabling real-time insights, supporting innovative applications, and driving growth at an unprecedented scale for the UAE economy. The network is no longer just the backbone – it's the engine driving UAE's digital transformation, yet it faces unprecedented pressures from the complexity of AI workloads.

Secure Networking: Essential for Business Growth

With increased complexity comes greater risk. As networks become more dynamic and distribute their vulnerability to cyber threats grows. In the UAE 99% of organisations consider secure networking vital to their operations and growth with 68% viewing it as critical. Additionally, 97% believe that enhancing their network will improve their cybersecurity posture.

We are at a crucial turning point. The traditional view of networks as static and siloed systems is no longer relevant. Modern networks need to be predictive autonomous and secure by design. They must support seamless connectivity for AI workloads remote teams and hybrid cloud environments all while safeguarding data applications and reputation.

At Cisco, we see this as both a challenge and an opportunity. By redesigning networks for greater flexibility, intelligence, and security, organisations can fully realise the advantages of AI, drive efficiency, and gain a sustainable edge in the marketplace.

A pivotal moment — and a chance for growth

The insights from our research indicate that network outages are no longer merely temporary inconveniences; they represent a multi-billion-dollar challenge to global innovation and economic progress. For UAE organisations, this underscores a significant area for consideration. Investing in modernising and securing networks is poised to enable businesses to harness the full potential of AI, drive efficiencies, and maintain a long-term competitive edge. 📌

THE RISE OF AI ASSISTANTS, AUTONOMOUS AI AGENTS, AND DATA-DRIVEN WORKLOADS IS FUNDAMENTALLY CHANGING HOW WORK GETS DONE.

FROM OVERLOAD TO ORCHESTRATION: ENABLING DIGITAL WORKSPACES WITH AN MSP PLATFORM



Nisangan N
Enterprise Evangelist, ManageEngine

Digital employee experience (DEX) is now emerging as a priority alongside cybersecurity and privacy, reshaping the expectations placed on IT infrastructure. Rather than focusing solely on uptime and data protection, modern enterprises now require seamless access, user-first experiences, operational agility, and robust security across distributed and hybrid environments.

To meet these demands truly, IT ecosystems must go the extra mile; supporting orchestration across endpoints and ensuring secure access from anywhere—while also delivering a unified experience at scale. However, with constrained budgets and limited internal resources, many organisations find it difficult to invest in or maintain such capabilities.

That's why a growing number are turning to managed service providers

(MSPs) as their strategic IT partners. Recent reports reveal that 60% of all organisations worldwide rely on MSPs to streamline IT and cloud operations.

For MSPs, however, delivering on these expectations is no small feat. They must manage complex technology layers—from infrastructure and cybersecurity to end-user support and compliance—often as a single unit. To succeed, they increasingly rely on interoperable, lightweight systems that unify service

delivery. These platforms serve as singular delivery channels, reducing tool fatigue, streamlining operations, and empowering MSPs to scale efficiently while maintaining a high standard of client service.

Bridging the gap in a fast-moving world

This growing complexity calls for sharper IT focus and adaptability. As technology continues to evolve rapidly, it often leaves behind a gap that's hard to fill. Not long ago, a digital desk job simply meant having access to a desktop monitor. But today, business environments have expanded far beyond that; embracing thin clients, virtual desktop infrastructures (VDIs), remote work setups, multi-cloud environments, and a diverse mix of operating systems.

Each of these components has its own use case and must be set up, managed, and secured appropriately. That's where the challenge begins: most businesses lack the right expertise or tools to keep pace.

Take the example of cloud adoption. While the world was still adjusting to cloud computing, forward-looking businesses had already jumped into a multi-cloud strategy. Today, over 89% of global organisations run on multi-cloud environments. But in the race to adopt every new capability, many now find themselves in the middle of complex, bloated setups that are difficult to manage and scale.

Not every business is equipped to deal with current demands, let alone what's coming next. That's why many turn to MSPs, expecting them to bring structure, stability, and control to their IT systems.

MSPs step up but face intensifying pressure

MSPs are increasingly becoming the bedrock of digital operations as more businesses delegate IT to service providers. Yet, they shoulder immense responsibility. A recent Canalys report projects global managed services revenue to grow 13% YoY

in 2025, reaching \$595 billion. With this opportunity comes heightened expectations and mounting challenges.

Operationally and strategically, MSPs are stretched thin by external pressures:

1. **AI adoption:** Canalys also reported that 61% of MSPs "still struggle to get AI projects out of the proof-of-concept stage with customers." Due to the rapid growth in the field, MSPs need to stay on top of AI developments to be able to advise on which tools provide ROI, in addition to determining which tools they want to and are able to provide managed services for.
2. **Cybersecurity escalation:** As demand rises for advanced services—like managed and extended detection and response (MDR and XDR), secure access service edge (SASE), and Zero Trust architecture—delivering these offerings stretches internal teams and technology limits.
3. **Regulatory heat:** New mandates (such as DORA and NIS2) and stricter cyber insurance requirements are intensifying compliance workloads.

Beyond external pressures, internal inefficiencies are holding MSPs back. Fragmented tool sets force teams to juggle siloed systems across help desk, patching, compliance, remote monitoring and management (RMM), professional

services automation (PSA), and security. Despite overlapping functions, these tools often fail to integrate, leading to delays, disjointed visibility, and error-prone workflows.

In such an environment, even experienced MSP teams find it hard to maintain quality and pace. The result? More time spent managing tools, less time driving value for clients.

Why MSPs who embrace platforms are better set for growth

With growing responsibilities and limited time, many MSPs struggle to keep services running smoothly while also improving them. When each client brings their own tools, expectations, and environment, internal operations often get stretched too thin.

Disconnected systems slow down technicians, complicate reporting, and increase the risk of error. Over time, this affects service quality and leads to burnout, even among experienced teams.

MSPs who move towards a platform-led model—where critical tools and data are brought under one roof—are far better equipped to stay on top of service delivery without compromising internal efficiency. Moving from multiple tools to a unified platform helps:

1. Reduce tool sprawl and streamline technician workflows.
2. Give full visibility across client environments in a single view.
3. Automate repetitive tasks, reporting, and compliance checks.
4. Improve onboarding and team collaboration.
5. Deliver quick responses while maintaining consistency and control.

Rather than patching together multiple systems, these MSPs build a solid foundation that supports sustainable growth, better client experiences, and faster adaptation to change.

In a world where IT demands are only getting bigger, choosing the right platform is not just an option; it's becoming a strategic advantage. 📌

IN A WORLD WHERE IT DEMANDS ARE ONLY GETTING BIGGER, CHOOSING THE RIGHT PLATFORM IS NOT JUST AN OPTION; IT'S BECOMING A STRATEGIC ADVANTAGE.

CONFIDENT UNTIL CRISIS: ARE ORGANISATIONS PULLING WOOL OVER THEIR OWN EYES WHEN IT COMES TO DATA RESILIENCE?

I WITH CYBERATTACKS ESCALATING, VEEAM'S TIM PFAELZER URGES LEADERS TO DITCH PAPER-BASED PLAYBOOKS AND STRESS-TEST THEIR DATA RESILIENCE FOR REAL-WORLD CRISES.

For too long, business leaders have viewed their organisation's data resilience from afar, relying on theoretical plans and a checklist mindset. This 2D perspective - where technical measures are simply ticked off a to-do list - fails to capture the full, real-world cross-organisational complexity of cyber threats. Ransomware, in particular, cannot be fully simulated on paper.

This mentality has led to a dangerous false sense of security. Veeam research shows that more than 30% of organisations believe they are more resilient than they actually are. While they may have the right pieces in place, unless these elements work together in a rigorously tested, real-world incident response plan, they risk being exposed when a true crisis hits.

With 69% of organisations having faced a ransomware threat in the past year, the time for blind confidence is over. Leaders must remove the wool from their eyes and take meaningful, proactive action.

False Confidence, Real Consequences

Data resilience can be deceptively complex, and gaps often remain

hidden until it's too late. Many organisations fall into the trap of believing they are prepared, only to find out otherwise under attack. Of the organisations that fell victim to ransomware last year, 69% thought they were prepared beforehand. After experiencing an attack, confidence in their preparedness dropped by more than 20%.

Although the majority of organisations had a ransomware playbook, less than half included essential technical components such as backup copies and containment or isolation plans. On the surface, everything may have appeared in order - but a closer inspection revealed significant vulnerabilities.

MORE THAN 30% OF ORGANISATIONS BELIEVE THEY ARE MORE RESILIENT THAN THEY ACTUALLY ARE – IT'S A DANGEROUS ILLUSION.

The consequences of misplaced confidence are severe. Only 10.5% of organisations were able to successfully recover following a ransomware attack last year, leading to major business and operational impacts. The recent M&S ransomware incident is a high-profile example, causing not only service outages for customers but also an estimated £300 million hit to trading profits.

The Evolving Threat Landscape

Some organisations may have hoped that the disruption of major ransomware groups like BlackCat and LockBit by law enforcement would make the threat landscape easier to navigate. In reality, the threat has not diminished - it has evolved. Smaller groups and "lone wolves" have quickly filled the gap, bringing new methods and tactics that further challenge organisational resilience.

From 2D to 3D: The Path to True Resilience

Regardless of how confident an organisation may be in its data resilience, a deeper, more critical examination of its ransomware playbooks is essential. It is no longer

safe to assume that what works on paper will hold up under real-life duress. Leaders must move from a flat, 2D perspective to a dynamic, 3D approach.

Start with the big picture: Do you know what data you need to protect and where it resides? Are the key resilience measures, such as a predefined chain of command and regular backup verifications, in place? Drill down further: Are your security teams up to date on the latest attack trends? With 89% of organisations reporting their backup repositories targeted by threat actors, ensuring redundancy for your backups is now critical.

Plugging the gaps is only the beginning. Organisations must stress-test their incident response plans with real-world simulations. It's not enough to rely on plan A - test plans B, C, D, and beyond, including scenarios where critical staff are unavailable or multiple crises occur simultaneously. This process often exposes blind spots that would go unnoticed in a theoretical plan.

Turning Confidence Into Capability

Leveraging frameworks like the Veeam Data Resilience Maturity Model (DRMM), developed in partnership with McKinsey, can help organisations move beyond blind confidence. Our findings show that organisations with a high degree of data maturity recover from ransomware incidents seven times faster than their less mature counterparts, and experience three times less downtime.

By taking control of data resilience — grounded in rigorous testing, continuous improvement, and collective intelligence — organisations can replace blind confidence with real capability. In the current threat landscape, it's not a question of "if" your organisation will be attacked, but "when". The best time to prepare is now - because in data resilience, only true readiness will make the difference. 🔑



CANON INTRODUCES SUBSCRIPTION SECURITY SERVICES TO PROTECT BUSINESS DEVICES AND DATA

I FLEXIBLE TIERED SERVICES DELIVER END-TO-END SECURITY, SAFEGUARDING PRINT INFRASTRUCTURE AGAINST EVOLVING THREATS

Canon announced the launch of its new Subscription Security Services – a flexible, easy-to-manage service which delivers end to end security protection for businesses – helping to safeguard end point devices, documents and data.

Building on Canon's robust print security offering, the new Subscription Security Services leverage cutting-edge technology and are available in two tiers: 'Enhanced Security' and the more comprehensive 'Premium Security'. Both tiers include robust device hardening, automated firmware updates, data backup, and secure data destruction as standard. The 'Premium Security' tier extends these capabilities with proactive device monitoring and management, real-time threat detection, rapid recovery and detailed security insights.

With the average cost of a data breach sitting at \$4.88 million in 2024, it is more critical than ever for a business

to take action and protect themselves from vulnerabilities to safeguard their organisation for the future.

Security essentials

Canon's Subscription Security Services provide businesses with the foundations for managing and securing their print device fleets. This includes robust device hardening to ensure all print and scan devices on the network are protected under a unified security policy. Establishing consistent governance across all devices is a key step in addressing the often-overlooked area of print infrastructure security.

Automated firmware updates ensure devices are always running the latest software, with patches applied to mitigate against any potential vulnerabilities, minimising the need for manual updates. This proactive approach helps organisations maintain confidence that devices are operating with the highest level of protection, while supporting




business continuity by reducing potential disruption.

Advanced protection

As security risks continue to evolve, protecting large print and scan device fleets can become increasingly complex. The 'Premium Security' tier delivers advanced capabilities tailored for organisations with larger device networks, enabling proactive security management through continuous monitoring and optimisation.

Businesses benefit from enhanced real-time threat detection where security issues are flagged as they occur, enabling quick reaction and the ability to implement the necessary safeguards. Rapid recovery capabilities also allow for fast restoration



Canon launches its new Subscription Security Services with two tiers, Enhanced and Premium, offering advanced protection for business print environments

WITH CANON'S SUBSCRIPTION SECURITY SERVICES, WE'RE PROVIDING COMPREHENSIVE SECURITY CAPABILITIES, REMOVING THE COMPLEXITY OF DEVICE PROTECTION SO BUSINESSES CAN FEEL CONFIDENT THEY'RE RECEIVING THE RIGHT EXPERTISE AND BEST-IN-CLASS SECURITY – REGARDLESS OF THEIR FLEET SIZE.

QUENTYN TAYLOR, DIRECTOR OF INFORMATION SECURITY, CANON EUROPE

of compromised devices, reducing potential downtime. Canon continually tests and refines these services to ensure the appropriate security configurations, aligning these with rigorous guidelines to give businesses confidence in the

protection they receive.

Canon's Subscription Security Services seamlessly integrate with the security features in Canon's existing cloud solutions, such as Cloud Connector and uniFLOW Online. This strengthens end-

to-end security and helps businesses minimise security risk. By adding Subscription Security Services, Canon provides businesses with flexible deployment options to meet their diverse and evolving security needs.

Quentyn Taylor, Director of Information Security at Canon Europe comments: "As security risks evolve and regulation tightens, businesses need a simpler, more effective way to protect their print fleet. With Canon's Subscription Security Services, we're providing comprehensive security capabilities, removing the complexity of device protection so businesses can feel confident they're receiving the right expertise and best-in-class security – regardless of their fleet size." 

CROWDSTRIKE UNVEILS FALCON NEXT-GEN IDENTITY SECURITY TO PROTECT EVERY IDENTITY ACROSS THE ATTACK CHAIN

THE FIRST UNIFIED SOLUTION SECURING HUMAN, NON-HUMAN,
AND AI AGENT IDENTITIES ACROSS HYBRID ENVIRONMENTS



Mike Sentonas, President of CrowdStrike.

CrowdStrike announced CrowdStrike Falcon® Next-Gen Identity Security, the first unified solution to protect every identity – human, non-human, and AI agent – across the full hybrid identity lifecycle and every environment. Delivered today, without delays or integration complexity through the AI-native CrowdStrike Falcon® platform, the new offering protects identities across on-premises, cloud, SaaS, and workloads, removing security blind spots and replacing fragmented controls. CrowdStrike unifies initial access prevention, modern privileged access management (PAM), identity threat detection and response (ITDR), SaaS identity security, and agentic identity protection to stop identity-driven breaches across domains.

“Organisations need trusted identity security now, not months or years from now. CrowdStrike provides what customers need most in a unified platform: modern identity security by design, without architectural trade-offs and integration debt,” said Mike Sentonas, president, CrowdStrike. “Access in today’s enterprise is dynamic and unpredictable, with identities spanning users, machines, and AI agents operating across hybrid environments in real time. The Falcon platform was built to manage this complexity, providing the speed, scale, and precision organisations need to stop modern identity attacks.”

Identity has become the primary path adversaries take to compromise an organisation. Attackers increasingly exploit a broad spectrum of identities that span human users, service accounts (non-human identities), SaaS credentials, and now, autonomous

AI agents. Each agent represents a superhuman identity with persistent access to systems, applications, and sensitive data. These non-human agent identities dramatically increase the size and severity of the attack surface: more identities across more environments, more privileges across more workflows, and more opportunity for adversaries to move faster than defenders can respond. Modern adversaries exploit this access to move seamlessly across domains – endpoint, identity, cloud, and SaaS – leaving organisations that rely on traditional IAM and legacy PAM tools exposed to cross-domain attacks.

Falcon Next-Gen Identity Security closes the gaps that adversaries exploit with a unified solution that delivers continuous protection across identity types (human, non-human and AI agent), environments, and stages of the identity attack chain. From initial access to lateral movement, CrowdStrike protects human, non-human, and AI agents across hybrid environments, including on-prem, cloud, and SaaS. Powered by CrowdStrike’s agentic AI, organisations gain autonomous threat analysis and response that helps them detect, investigate, and stop identity-based attacks in real time, through a single unified platform.

Organisations can immediately strengthen their security posture without waiting for promised integrations, or accepting identity capabilities fragmented across multiple platforms that replicate the same complexity and security gaps as multi-vendor solutions. Delivered through a single lightweight sensor and managed from a single console, CrowdStrike gives defenders real-time visibility, dynamic access enforcement,

and autonomous response across every identity and every domain.

CrowdStrike’s Unified Platform for Securing Every Identity Across Hybrid Environments

Falcon Next-Gen Identity Security unifies four core capabilities to deliver end-to-end visibility, control, and protection of identities, privileges, and risk across the full attack chain in hybrid identity environments:

- **Initial Access Prevention:** Leverages real-time endpoint signals, industry-leading threat intelligence, and AI trained on trillions of events to authenticate trusted identities, dynamically blocking threats before adversaries can gain initial access.
- **Modern Privileged Access Management (PAM):** Enforces just-in-time access and eliminates standing privileges. Dynamically adjusts access based on real-time risk to secure sensitive systems across hybrid and multi-cloud environments.
- **Identity Threat Detection and Response (ITDR):** Detects and stops identity-based attacks in real time. Uses cross-domain telemetry and agentic AI to triage threats, enforce policy, and block lateral movement and privilege escalation.
- **SaaS Identity Security:** Identifies misconfigurations, flags risky behaviors, and governs overprovisioned access – for humans, non-human identities, and AI agents – across cloud-first applications.

Delivered through the CrowdStrike Falcon platform, Falcon Next-Gen Identity Security replaces fragmented tools and disconnected workflows. Security teams gain real-time visibility, dynamic enforcement, and autonomous response across every identity and every domain. With rapid deployment and immediate time-to-value, organisations can strengthen their identity security posture today, without waiting for integrations or accepting security gaps. **1**

ORGANISATIONS NEED TRUSTED IDENTITY SECURITY NOW, NOT MONTHS OR YEARS FROM NOW.

MIKE SENTONAS, PRESIDENT, CROWDSTRIKE

TENABLE EXPANDS EXPOSURE MANAGEMENT PLATFORM TO SECURE ENTERPRISE AI

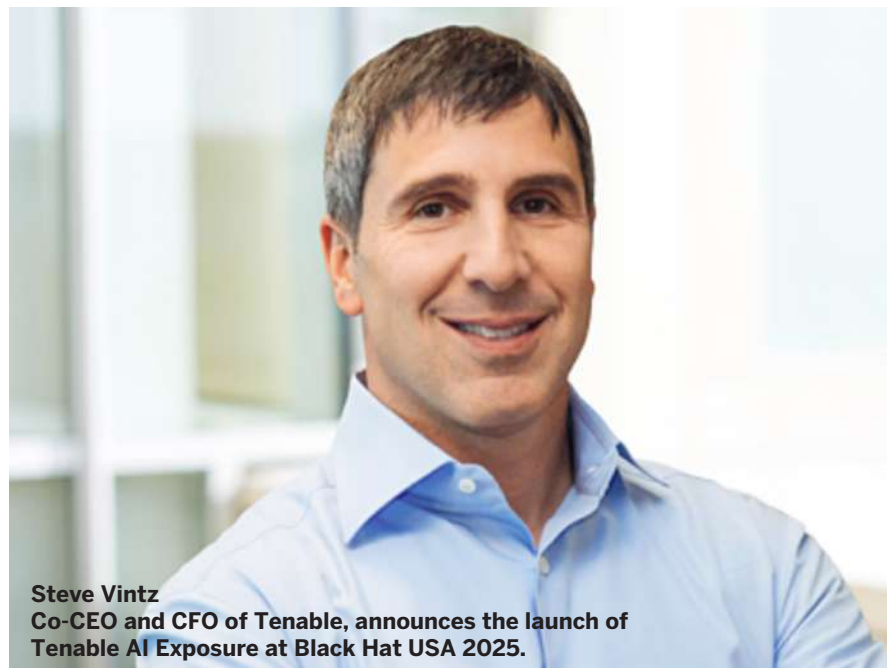
TENABLE LAUNCHES AI EXPOSURE TO PROVIDE UNIFIED VISIBILITY, RISK MANAGEMENT AND GOVERNANCE FOR GENERATIVE AI TOOLS LIKE CHATGPT ENTERPRISE AND MICROSOFT COPILOT.

Tenable, the exposure management company, has announced a major expansion of its Tenable One platform with the launch of Tenable AI Exposure, designed to help organisations discover, manage, and secure risks associated with generative AI. Unveiled at Black Hat USA 2025, the new solution enables enterprises to move beyond discovery to comprehensive risk management and policy enforcement for widely used platforms such as ChatGPT Enterprise and Microsoft Copilot.

The rapid adoption of generative AI is creating an invisible layer of security exposure as businesses embrace productivity gains. Employees are leveraging these tools in ways that may expose sensitive data or open avenues for manipulation by attackers, leaving security teams with limited visibility or control. Tenable AI Exposure addresses this challenge by delivering an end-to-end, unified approach that secures the entire lifecycle of AI usage within enterprise environments.

With agentless deployment, Tenable AI Exposure offers rapid coverage and integrates into the Tenable One platform. Key capabilities include:


- **Comprehensive AI discovery:** Unified insights from Tenable AI Aware and continuous monitoring to map both sanctioned and unsanctioned AI usage, highlighting risks in data flows and user interactions.



- **Exposure management and prioritisation:** AI Security Posture Management (AI-SPM) helps identify, prioritise and manage risks from sensitive data leakage, misconfigurations, and unsafe integrations.
- **Governance and control:** Enforcement of organisational policies and security guardrails to prevent risky behaviours, while defending against threats such as prompt injections, jailbreaks, and malicious outputs.

Steve Vintz, Co-CEO and CFO of Tenable, underlined the significance

of the launch, saying: "With Tenable AI Exposure, we're giving organisations the visibility and control they need to safely embrace the promise of generative AI without introducing unacceptable risk. This is a critical step in the evolution of exposure management."

Tenable AI Exposure is currently available via a private customer preview, with general availability expected by the end of 2025. Visitors to Black Hat USA 2025 can experience a live demo at booth #2440 and attend a session by Tomer Avni, VP of Product Management, titled "Don't Let AI Divide Your Defences: Get it Together for the AI Attack Surface" on August 6. 

GITEX

GLOBAL

13-17
OCT 2025
DUBAI WORLD
TRADE CENTRE

FEATURING

Global
Data
Centres

GQX
GITEX QUANTUM
EXPO

GITEX
DIGI HEALTH
& BIOTECH

GITEX
CYBER
VALLEY

GITEX
GREEN
IMPACT

GLOBAL
DEV
SLAM

THE WORLD'S LARGEST TECH, AI & STARTUP SHOW

200,000

TECH
EXECUTIVES

180

COUNTRIES

40%

OF ATTENDEES
ARE C-LEVEL

6,500

EXHIBITING
COMPANIES

1,733

STARTUPS

400+

GOVERNMENT
ENTITIES

Scan the QR code to

GET INVOLVED



#GITEXGLOBAL
gitex.com



ORGANISED BY



مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

BEYONDTRUST ACCELERATES IDENTITY SECURITY INNOVATION AND RESEARCH MOMENTUM WITH LAUNCH OF PHANTOM LABS



Marc Maiffret, CTO, BeyondTrust.

BeyondTrust, the global leader in identity security protecting Paths to Privilege, has announced the formal launch of its dedicated cybersecurity research team, BeyondTrust Phantom Labs™. The launch of Phantom Labs represents a strategic milestone in BeyondTrust's ongoing mission to advance identity security innovation, uncover emerging threats, foster industry collaboration, and help shape industry standards that empower defenders with actionable insights worldwide.

Building on years of real-world threat analysis, vulnerability disclosures, and identity-focused security innovation, Phantom Labs is tasked with "thinking like an attacker" to expose the ways threat actors escalate access and maintain control. With the addition of new research leadership and specialized hires, Phantom Labs is accelerating the company's ability to help defenders proactively understand, detect, and disrupt identity exploitation in increasingly complex hybrid and cloud environments.

BeyondTrust's expanding research mission is focused on delivering key contributions to the global cybersecurity community:

- Original threat research and vulnerability discovery
- Guidance for defenders, including mitigation playbooks and hardening recommendations
- Collaboration with product teams to drive innovation across the BeyondTrust portfolio

Phantom Labs formalizes the work of BeyondTrust's existing security researchers, whose investigations have uncovered critical vulnerabilities and provided threat intelligence used in real-world incident response, including key intelligence that helped Okta investigate and contain a high-profile breach.

Recent contributions include:

- Discovery of stealth privilege escalation risks in Microsoft Entra guest accounts
- Development of data science-driven detection models to identify session hijacking
- Release of the paths to privilege research framework, now integrated into BeyondTrust's platform
- Ongoing collaboration with the Adventures of Alice & Bob podcast to help educate the market about unknown risks and contribute to the global cybersecurity community.

To further accelerate BeyondTrust's identity security innovation and research momentum, BeyondTrust has made strategic new hires and elevated key internal experts into critical roles:



- **Kinnaird McQuade**, an industry leading expert in cloud identity security, has joined BeyondTrust as Chief Security Architect. McQuade's security research has produced popular open-source tools including Cloudsplaining, which has been downloaded more than 40 million times. This work has helped shape how modern security teams identify and contain attacks like data exfiltration, lateral movement and privilege escalation, particularly in hybrid and cloud environments where identity is the new perimeter.
- **Fletcher Davis**, a leading offensive security researcher and red team specialist, will lead Phantom Labs. Davis brings extensive experience in simulating advanced threat actor behavior, uncovering cross-domain identity risks, and exposing hidden paths to privilege in complex

enterprise environments.

BeyondTrust's research momentum sits under the overall direction of Marc Maiffret, Chief Technology Officer at BeyondTrust and pioneering force in vulnerability research and cybersecurity innovation. With decades of experience in offensive and defensive security, including discovering some of the first major Microsoft vulnerabilities and co-founding one of the earliest vulnerability management platforms, Maiffret provides a uniquely attacker-informed perspective to the company's mission.

"Think like a hacker.' That mindset shaped my first security startup over 25 years ago, where we helped define Vulnerability Management and built one of the first commercial security research teams," says Marc Maiffret, CTO, BeyondTrust.

"Great security products require more than customer insight. They need research teams anticipating threats before they emerge. Traditional PAM solutions lag behind in addressing complex, cross-domain attack paths. And Identity Security isn't a feature you bolt on. It demands a purpose-built platform, led by research. BeyondTrust delivers that with Pathfinder and Phantom Labs—a platform purpose built to secure identities and access, powered by a team uncovering tomorrow's threats today." 📌

THINK LIKE A HACKER.' THAT MINDSET SHAPED MY FIRST SECURITY STARTUP OVER 25 YEARS AGO, WHERE WE HELPED DEFINE VULNERABILITY MANAGEMENT AND BUILT ONE OF THE FIRST COMMERCIAL SECURITY RESEARCH TEAMS, SAYS MARC MAIFFRET, CTO, BEYONDTRUST.

HID UNVEILS NEXT-GENERATION FIDO HARDWARE AND CENTRALISED MANAGEMENT AT SCALE

I THE NEXT GENERATION OF HID'S FIDO PORTFOLIO FEATURES HARDWARE AUTHENTICATORS AND A CENTRALISED MANAGEMENT EXPERIENCE THAT SIMPLIFIES PASSKEY DEPLOYMENT.

H ID, a worldwide leader in trusted identity and access management solutions, has announced a new line of FIDO-certified credentials—now powered by the new Enterprise Passkey Management (EPM) solution— designed to help organisations deploy and manage passkeys at the enterprise scale. New research from FIDO Alliance shows that while 87% of enterprises are adopting passkeys, nearly half of those that are yet to deploy cite complexity and cost concerns as primary barriers. HID's solution streamlines the shift to passwordless authentication.

This next phase of HID's passwordless authentication roadmap gives enterprises choice, flexibility, and speed to deploy FIDO without compromising user experience or security posture. The expanded portfolio delivers phishing-

resistant authentication with enterprise-grade lifecycle management, making scalable passwordless security accessible to organisations of all sizes. The solution works seamlessly across diverse work environments while reducing IT support requirements through centralised visibility and control.

"Phishing-resistant authentication isn't one-size-fits-all. It's a journey, and we're here to help enterprises along the way," said Sean Dyon, Vice President & Head of the Authentication Business Unit at HID. "Rolling out passkeys isn't just about issuing devices, it is about giving security teams the tools to manage them at the enterprise scale, with the same precision as the rest of the identity stack. Our next-generation portfolio delivers both the hardware diversity and FIDO management capabilities organisations need to deploy and manage passkeys at scale."



Unlock Enterprise-Grade Passkey Management – at scale

Rolling out FIDO across the enterprise isn't just about secure hardware—it's about control, continuity, and compliance. HID's new subscription-based solution empowers IT and IAM leaders to drive passwordless adoption at scale—securely, efficiently, and with full administrative oversight.

With HID's Enterprise Passkey Management, you can:

- **Remotely initiate and manage provisioning** — Issue FIDO credentials on behalf of users to reduce manual effort, end user training requirements and accelerate deployment.



ROLLING OUT PASSKEYS ISN'T JUST ABOUT ISSUING DEVICES, IT IS ABOUT GIVING SECURITY TEAMS THE TOOLS TO MANAGE THEM AT THE ENTERPRISE SCALE, WITH THE SAME PRECISION AS THE REST OF THE IDENTITY STACK.

- **Gain full lifecycle visibility** — Manage issuance, revocation and audit trails at scale to support compliance and operational efficiency.

Expanded hardware portfolio for diverse enterprise needs

Through the expanded Crescendo® line, there are three new purpose-built

authenticators designed to meet diverse enterprise requirements:

- **Crescendo Keys** – Redesigned in response to market feedback for improved ergonomics, usability and accessibility. Supports FIDO2, PKI, and OATH with remote PIN reset, perfect for power users and regulated environments.

- **Crescendo Cards** – A single, universal credential—a corporate badge that offers both physical access to facilities and passwordless access to digital enterprise resources. Available as dual interface or contactless cards, with support for FIDO, PKI, OATH, and other key physical access technologies.
- **OMNIKEY 5022 Contactless Reader** – A high-quality, cost-effective FIDO reader for authentication to PCs and workstations.

All devices are fully compatible with Microsoft Entra ID and many other major identity providers, enabling seamless deployment within existing enterprise infrastructure.

Early testers have praised the solution's ease of use and enterprise readiness.

"The new Crescendo Key immediately stood out with its sleek and durable design. Getting started was simple, and the setup process was intuitive and fast. It stands apart from other FIDO keys on the market and is on par with the quality we have come to expect from HID credentials. We will be recommending this authentication device to all of our customers who require a secure credential for authentication to Entra ID and Windows accounts," stated David Backus, Sales Engineer at TX Systems Identity Solutions.

Physical access control support

This one-card solution provides FIDO-based, passwordless access to business applications and physical spaces to increase workforce productivity through simplified deployment and management.

- **Seos® FIDO-Enabled Card** – Combines Seos physical access technology with phishing-resistant FIDO 2.1 authentication in a secure, single credential.
- **MIFARE DESFire EV3 FIDO-Enabled Card** - Integrates advanced DESFire EV3 smart card technology with FIDO 2.1 support for unified access. 🔑



Aneka Gupta
Chief Product Officer at Rubrik,
unveils Agent Rewind in Dubai

RUBRIK INTRODUCES AGENT REWIND TO REVERSE AI AGENT MISTAKES

**NEW SOLUTION POWERED BY PREDIBASE
INFRASTRUCTURE ENABLES SAFE
ROLLBACK OF UNINTENDED AI ACTIONS**

Rubrik, Inc, the Security and AI company, announced the launch of Agent Rewind, following the close of Rubrik's acquisition of Predibase. Agent Rewind, powered by Predibase AI infrastructure, will enable organizations to undo mistakes made by agentic AI by providing visibility into agents' actions and enabling enterprises to rewind those changes to applications and data.

"As companies consider investing in AI, they often don't take into account the mistakes that AI agents can and will make," said Johnny Yu, Research Manager at IDC. "Agentic AI introduces the concept of 'non-human error,' and as

with its human counterpart, organizations should explore solutions that allow them to correct potentially catastrophic mistakes made by agentic AI."

"As AI agents gain autonomy and optimize for outcomes, unintended errors can lead to business downtime," said Aneka Gupta, Chief Product Officer at Rubrik. "Agent Rewind integrates Predibase's advanced AI infrastructure with Rubrik's recovery capabilities to enable enterprises to embrace agentic AI confidently. Today's organizations will now have a clear process to trace, audit, and safely rewind undesired AI actions."

AI agents possess significant potential, yet, like humans, they are prone to

mistakes that result in unintended business disruption. Recent incidents of AI agent errors highlight a spectrum of situations ranging from technical malfunctions and legal issues to even the deletion of entire production databases. A recent study found that AI agents are frequently becoming disoriented, choosing incorrect shortcuts, and struggling to complete even simple multi-step tasks, revealing critical flaws that undermine their reliability and effectiveness.

Agent Rewind makes previously opaque AI actions visible, auditable, and reversible, creating an audit trail and immutable snapshots that facilitate safe rollback. Current observability tools only show what happened, but not why or how to reverse high-risk actions.

"Agent Rewind will close the loop on what happened, why it happened, and how to undo it," said Chad Pallett, Chief Information Security Officer at BioIVT, a global research partner and biospecimen solutions provider for drug and diagnostic development. "When using AI, there is a need for observability and secure rollback. Rubrik and Predibase will provide not just data safety and model speed, but also AI recoverability. In a market craving true observability and remediation, Agent Rewind is the answer I've been waiting for."

When AI goes awry, Agent Rewind offers:

- **Context-Enriched Visibility:** Surfaces agent behavior, tool use, and impact while contextualizing each action, mapping it back to its root cause – from prompts to plans to tools – to enable precise recovery when something goes wrong.
- **Safe Rollback:** Uses Rubrik Security Cloud to rewind what changed, whether that's files, databases, configurations, or repositories.
- **Broad Compatibility:** Will integrate seamlessly with a wide range of platforms, APIs, and agent builders, including Agentforce, Microsoft Copilot Studio, and Amazon Bedrock Agents, and will be compatible with any custom AI agent. 🔑

 tahawultech.com

FUTURE ENTERPRISE AWARDS 2025



13th OCTOBER 2025



Palace Downtown, Dubai



6:00 PM onwards

#FutureEnterpriseAwards2025 | #tahawultech

The **Future Enterprise Awards**, hosted by **CPI Media Group** and **tahawultech.com** is one of the most iconic technology events in the IT industry across the Middle East region.

The fact that the Future Enterprise Awards are so iconic is primarily due to their incredible longevity, this year's edition will mark the 20th edition of the coveted technology awards.

One other indelible factor in the historic success of the Future Enterprise Awards is the fact that the event is always held on **Day 1 of GITEX Global**.

As the digital landscape continues to evolve at incredible speed, recognizing and celebrating innovation is more important than ever.

The Future Enterprise Awards 2025 will pay tribute to the fearless leaders, visionaries and companies that are championing change through cutting-edge technologies that are completely reshaping and transforming the digital future we live in.

OFFICIAL PUBLICATIONS

HOSTED BY

cnme
computer news middle east

Reseller
MIDDLE EAST
THE VOICE OF THE CHANNEL

Security
MIDDLE EAST

 tahawultech.com

For more information about the event and nomination details, please click on the link below :
<https://www.tahawultech.com/futureenterpriseawards/2025/>

FORTINET EXPANDS FORTICLOUD WITH NEW IDENTITY, STORAGE, AND COMMUNICATION SERVICES



Michael Xie
Founder, President, and CTO, Fortinet

FORTIIDENTITY, FORTIDRIVE, AND FORTICONNECT EXTEND THE FORTINET SECURITY FABRIC TO EMPOWER HYBRID ENTERPRISES WITH SECURE ACCESS, STORAGE, AND COLLABORATION

Fortinet, the global cybersecurity leader driving the convergence of networking and security, today announced a major expansion of FortiCloud, its global cloud infrastructure. The latest release introduces FortiIdentity, designed for cloud-delivered identity management for hybrid teams and two new beta services, FortiDrive and FortiConnect, to provide enterprise-grade secure storage and protected communications. Each service is tightly integrated into the Fortinet Security Fabric, giving organisations security-native alternatives to point products often dependent on bolt-on security.

"FortiIdentity, FortiDrive, and FortiConnect, are key milestones in our vision to build a unified global cloud network that brings enterprise-grade security directly into the way teams manage access, store, share, and communicate," said Michael Xie, Founder, President, and Chief Technology Officer at Fortinet. "These new services extend the power of the Fortinet Security Fabric into everyday productivity and access control, reinforcing our strategy to simplify security operations, reduce vendor sprawl, and empower hybrid work at scale."

Integrated Innovation Backed by Global Infrastructure

This announcement builds on Fortinet's continued investment in its global hybrid-cloud infrastructure, including company-owned data centers in Atlanta, Chicago, New York, Plano, Frankfurt, Sydney, and Torija (Spain). These facilities are strategically designed to deliver low-latency services and support regional demand, combining compute, storage and recovery, and security capabilities. Fortinet also addresses growing data sovereignty requirements by enabling organisations to keep data local through its globally distributed infrastructure.

Complementing these investments, Fortinet leverages over 160 points of presence (POPs) through providers like Google Cloud, AWS, and Digital Realty to ensure secure, high-performance delivery of edge services. Fortinet also delivers a broad range of services made available across cloud marketplaces that include AWS, Azure, and Google Cloud, enabling organisations to benefit from greater service resiliency, geographic flexibility, and seamless access to Fortinet's cloud-delivered security offerings wherever they operate.

FortiCloud: Security-Native Services for the Modern Enterprise

With this expansion, Fortinet furthers its strategy of delivering a unified platform that enables organisations to consolidate tools, enhance security posture, and reduce total cost of ownership. The growing FortiCloud service portfolio now includes three new security-native

services designed for today's hybrid workforce:

- **FortiIdentity:** A long-established Fortinet identity and access management (IAM) solution, now delivered from FortiCloud, offers enterprises a full-featured, cloud-native approach to secure identity management. It provides secure single sign-on (SSO), multifactor authentication (MFA), FIDO2 passkeys, and identity federation across Fortinet and third-party applications without the need for additional hardware or software. With support for FortiToken Mobile, FIDO2 passkeys, and SAML/OIDC standards, FortiIdentity simplifies identity administration and scales easily to meet enterprise and MSSP requirements. The addition of FortiPAM-as-a-Service as a module of FortiIdentity provides continuous zero-trust network access (ZTNA) checks needed to protect privileged access to the IT environment.
- **FortiDrive:** A secure file storage and collaboration solution that protects sensitive data at rest and in transit. Featuring advanced encryption and granular access controls, FortiDrive enables teams to store and manage content safely. Real-time collaboration capabilities allow users to co-edit and share files and folders with colleagues or partners. Built-in version history ensures changes are tracked and can be easily rolled back if needed. FortiDrive also includes site management functionality to help organize content by team or project, along with policy-based

compliance enforcement through role-based access control and least-privilege principles.

- **FortiConnect:** A unified communication platform that integrates seamlessly with FortiDrive, enabling secure calling, messaging, meetings, and file sharing from anywhere. It delivers an intuitive collaboration experience underpinned by FortiGuard Labs AI-powered threat intelligence, ensuring communications are protected against evolving cyberthreats.

All three services are natively integrated into the Fortinet Security Fabric, providing centralised visibility, consistent policy enforcement, and real-time threat protection across users, devices, applications, data, and AI agents.

Continued Global Investment

Fortinet's ongoing investment in global cloud infrastructure empowers its platform strategy and commitment to delivering security with the best application experience possible, wherever customers operate. In addition to new POPs, Fortinet's hybrid-cloud model allows customers to access an expanding range of services, including FortiSASE, FortiAppSec, FortiCNAPP, FortiSOC, FortiMail, and FortiAIOps, through the FortiCloud centralised portal.

Delivering Unified, Scalable Security through the FortiCloud Platform

These new services delivered via FortiCloud reflect Fortinet's commitment to simplifying and securing hybrid operations with a unified, cloud-native platform. With a unified platform approach, centralised policy enforcement, and AI-powered threat intelligence, FortiCloud empowers organisations to optimise costs while reducing operational complexity, improve visibility, and protect data and users across distributed environments. Whether securing access, applications, or infrastructure, Fortinet continues to drive security transformation by making cloud security more simple, cost-effective, and natively integrated into the enterprise. **1**

THESE NEW SERVICES EXTEND THE POWER OF THE FORTINET SECURITY FABRIC INTO EVERYDAY PRODUCTIVITY AND ACCESS CONTROL, REINFORCING OUR STRATEGY TO SIMPLIFY SECURITY OPERATIONS, REDUCE VENDOR SPRAWL, AND EMPOWER HYBRID WORK AT SCALE.

MICHAEL XIE, FOUNDER, PRESIDENT, AND CTO, FORTINET

RUBRIK AND SOPHOS PARTNER TO DELIVER MICROSOFT 365 CYBER RESILIENCE

NEW SOLUTION INTEGRATES RUBRIK'S BACKUP AND RECOVERY WITH SOPHOS MDR AND XDR FOR ENHANCED MICROSOFT 365 PROTECTION



Joe Levy, CEO, Sophos.

Rubrik (NYSE: RBRK), the cybersecurity company, and Sophos, a global leader of innovative security solutions for defeating cyberattacks, today announced a strategic partnership to provide Sophos M365 Backup and Recovery Powered by Rubrik. This marks the first Managed Detection and Response (MDR)-optimised Microsoft 365 backup and recovery solution fully integrated into Sophos Central, Sophos' security operations platform. Designed to support IT and cybersecurity teams, the new offering will provide a unified global platform to enhance cyber resilience against ransomware, account compromise, insider threats, and data loss in SharePoint, Exchange, OneDrive, and Teams.

"We are reshaping what it means to stay operational in a world shaped by constant digital disruption," said Joe Levy, CEO, Sophos. "This is the future of cyber resilience: an intelligent, adaptive partnership that ensures organisations remain secure, responsive, and uninterrupted. By combining Sophos' prevention-first approach with Rubrik's unwavering recovery capabilities, we

empower businesses to withstand attacks and maintain continuity, even under pressure.”

Sophos will offer a powerful new add-on solution for its more than 75,000 MDR and XDR customers—enabling fast, secure recovery of critical Microsoft 365 data in the event of accidental deletion or malicious compromise. This solution integrates Rubrik’s industry-leading SaaS-based protection directly into the trusted Sophos Central platform, giving organisations the flexibility to enhance their existing security operations with robust data recovery capabilities. The Sophos Central platform integrates over 350 different telemetry sources across endpoint, cloud, network, identity, email and business applications. The platform leverages deep learning, custom LLMs, and frontier models to detect and respond to threats across the entire attack surface, enhancing defense effectiveness.

“The reality of today’s threat landscape demands a holistic approach to cyber resilience,” said Bipul Sinha, CEO, Chairman, and Co-founder of Rubrik. “With AI-enabled attacks and sophisticated breaches on the rise, organisations need more than just prevention; they need the ability to recover rapidly and reliably. Our partnership with Sophos delivers this critical capability directly within a platform security teams already use and trust, raising the bar for Microsoft 365 resilience.”

The Evolving Threat Landscape

According to The State of Ransomware report by Sophos, nearly half of organisations impacted by ransomware



chose to pay the ransom to recover their data. Despite this, only 54% of affected companies relied on backups for data restoration, highlighting a continued gap in effective cyber resilience practices.

Recent research highlights the urgent need for robust Microsoft 365 data protection: 60% of Microsoft 365 tenants have experienced account takeovers, a frequent launchpad for lateral movement within an organisation, and 81% have encountered email compromise. When global admin credentials are compromised, attackers can manipulate retention settings and permanently delete critical business data. Existing tools were not designed for comprehensive, large-scale recovery, which requires speed, granularity, and reliability for rapid restoration.


Sophos MDR and XDR customers will benefit from:

- **Secure, immutable backups:** Rubrik will isolate Microsoft 365

backups with air-gapped storage, WORM locks, and customer-held encryption keys. Multifactor authentication and data lock prevent tampering—even with compromised credentials.

- **Fast, flexible recovery:** Customers will be able to restore Microsoft 365 emails, OneDrives, SharePoint sites, Teams channels, and more to original or alternate users, including inactive accounts.
- **Automated protection:** Rubrik will automatically discover Microsoft 365 users, sites, and mailboxes, applies Entra ID-based policies, and supports delegated admin – all integrated with Sophos Central to reduce manual effort.
- **Unified experience:** Microsoft 365 protection and security operations will be managed via Sophos Central with no extra tools.

Rubrik and Sophos’ shared commitment to helping organisations operate with confidence in the face of risk, will provide Sophos customers and partners with a powerful solution to recover with speed and precision when threats inevitably break through.

This offering will be available through Sophos’ channel partner network in the coming months. 

THIS IS THE FUTURE OF CYBER RESILIENCE: AN INTELLIGENT, ADAPTIVE PARTNERSHIP THAT ENSURES ORGANISATIONS REMAIN SECURE, RESPONSIVE, AND UNINTERRUPTED.

JOE LEVY, CEO, SOPHOS



Ilya Markelov
Head of Unified Platform product line at Kaspersky.

MOST UAE SECURITY EXPERTS OVERWHELMED BY MULTI-VENDOR TOOLS, SAYS KASPERSKY RESEARCH

86% OF COMPANIES IN THE UAE RELY ON MULTI-VENDOR ECOSYSTEMS DESPITE THE FACT THAT SUCH FRAGMENTED SECURITY SOLUTIONS LEAD TO OPERATIONAL AND FINANCIAL STRAINS. SUCH FINDINGS WERE REVEALED IN THE RECENT KASPERSKY RESEARCH.

A study titled “Improving resilience: cybersecurity through system immunity,” conducted by Kaspersky, examined how organisations manage cybersecurity today, focusing on vendor fragmentation, operational inefficiencies and future consolidation plans. The survey was conducted across the META (the Middle East, Türkiye and Africa) region, as well as Europe, Russia, Latin America, and the Asia-Pacific region.

This report provides a comprehensive analysis of the current state of cybersecurity management across organisations, highlighting significant challenges associated with multi-vendor security environments.

Despite these persistent challenges, a majority of organisations in the UAE continue to operate within multi-vendor environments – 86% currently manage security across multiple providers. Interestingly, nearly half (42%) believe that a single cybersecurity provider could sufficiently meet all their needs, suggesting a recognition of the potential benefits of consolidation. However, only 14% have adopted a single-vendor

WHILE DIVERSIFICATION OF SECURITY SOLUTIONS CAN OFFER CERTAIN BENEFITS, SUCH AS RISK MITIGATION AND COVERAGE BREADTH, AN UNCHECKED INCREASE IN COMPLEXITY OFTEN LEADS TO SIGNIFICANT RESOURCE DRAIN AND OPERATIONAL INEFFICIENCIES.

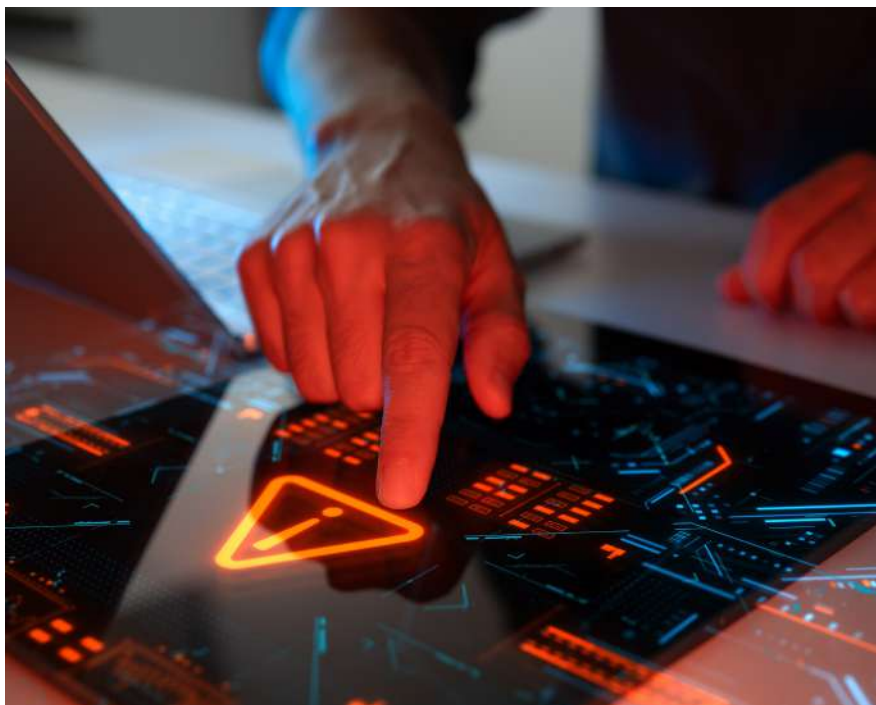
approach in practice, reflecting a cautious approach driven by concerns over over-reliance on one supplier or the perceived risks associated with vendor lock-in.

The landscape is rapidly shifting toward consolidation: an overwhelming 93% of firms are actively moving in this direction, a quarter (21%) have already begun merging their security tools into unified platforms, while an additional 72% plan to do so within the next two years. This trend underscores a strategic shift toward simplifying cybersecurity operations, reducing costs, and achieving more effective threat management through integrated solutions. As organisations increasingly recognise the advantages of streamlined security

architectures, the move toward vendor consolidation is poised to reshape the cybersecurity landscape in the near future.

“The data from our research indicates that many organisations rely on multiple vendors by default, rather than through deliberate strategic planning. While diversification of security solutions can offer certain benefits, such as risk mitigation and coverage breadth, an unchecked increase in complexity often leads to significant resource drain and operational inefficiencies. Moreover, this complexity can create critical blind spots, making it harder to maintain comprehensive threat visibility and respond effectively to emerging risks. The emerging trend toward consolidation reflects a maturation in cybersecurity strategies, emphasising the adoption of integrated platforms that streamline management, reduce manual effort, and enhance overall visibility into security posture,” said Ilya Markelov, Head of Unified Platform product line at Kaspersky.

To enable comprehensive protection of all business assets and processes, Kaspersky experts recommend to use centralised and automated solutions such as Kaspersky Next XDR Expert. By aggregating and correlating data from multiple sources in one place and using machine-learning technologies, this solution provides effective threat detection and fast automated response. Out-of-the-box integrations, automation features and case management help make infrastructure complexity much less of an issue. 📌





Mathivanan Venkatachalam
vice president of ManageEngine.

MANAGEENGINE ENDPOINT CENTRAL DELIVERED 442% ROI ACCORDING TO TOTAL ECONOMIC IMPACT STUDY

STUDY ALSO REVEALS \$4.5 MILLION IN QUANTIFIED BENEFITS OVER THREE YEARS WITH PAYBACK IN UNDER SIX MONTHS FOR ORGANISATIONS.



ManageEngine, a division of Zoho Corporation and a leading provider of enterprise IT management solutions, today announced the findings of a commissioned Total Economic Impact (TEI) study, conducted by Forrester Consulting, of Endpoint Central, its unified endpoint management and security (UEMS) platform. The study revealed that a composite organisation, which is a representative of interviewed customers, realised a 442% return on investment (ROI) over three years and achieved a full payback within six months.

Aimed at capturing real-world outcomes experienced by enterprises using ManageEngine's UEMS platform, the study also found that interviewed customers gained \$4.5 million in total benefits over three years, with a net present value (NPV) of \$3.7 million. The exercise was carried out independently by Forrester through in-depth interviews with four customers and financial modeling of a composite organisation.

"We've always aimed to deliver meaningful outcomes through Endpoint Central, and it's rewarding to see those results consistently reflected in our customers' experiences—and

now quantified in this TEI study," said Mathivanan Venkatachalam, vice president of ManageEngine. "Many of our customers have significantly reduced operational overhead and administrative burden by replacing multiple tools with Endpoint Central. That's exactly the kind of outcome Endpoint Central was built to deliver."

Key Findings From the Study

While ROI is a key outcome, Endpoint Central's broader business impact is evident in the following significant gains realised across productivity, cost, and performance:

- Reduced manual patching effort by up to 95% through automated patch management, resulting in \$913,000 in productivity gains over three years.
- Legacy tool consolidation through Endpoint Central led to over \$1 million in savings over a three-year period.

- Endpoint Central helps streamline IT operations, enhancing endpoint security, reducing costs, and boosting productivity for a decentralised workforce
- Offers improved device compliance and reduced cyber insurance costs by strengthening endpoint security posture

- Secure self-service and remote troubleshooting across IT functions were implemented, reducing help desk effort and improving end-user efficiency.
- Improved real-time visibility and control over hardware and software assets and efficient reclamation of unused licenses.
- Elimination of manual report generation through automated endpoint analytics and reporting workflows.

As per the study, Endpoint Central also enhanced the IT team's ability to support users across geographies and work models through its unified interface and management capabilities. Customers experienced greater endpoint stability and improved end-user experience due to reduced downtime and fewer disruptions.

Beyond operational efficiency, customers also shared real-world gains in compliance, security posture, and insurance savings. "Our compliance rate of devices went from 70% to more than 95% after using Endpoint Central. Devices are much more stable and easier to manage. We were even able to save cyber insurance costs due to this increased security posture," said an IT director in the software services industry in the study. 📌

VISHING AWARENESS MODULE LAUNCHED IN KASPERSKY ASAP PLATFORM

KASPERSKY EXPANDS ITS AUTOMATED SECURITY AWARENESS PLATFORM WITH A DEDICATED VISHING MODULE TO HELP EMPLOYEES RECOGNISE AND RESIST VOICE-BASED SCAMS.

Kaspersky has introduced a new module on vishing (voice phishing) to its ASAP (Automated Security Awareness Platform), continuing its mission to build practical cyber-hygiene skills among employees across industries. The latest update addresses one of the most manipulative and growing types of social engineering, and teaches users how to recognise and respond to voice-based scams.

Vishing has become a major vector for corporate fraud. For example, AIB saw a 79% year-on-year increase in vishing attacks in early 2025, including a case where a business customer nearly lost €41,000 during a scam call. Additionally, in a notable case disclosed by Google and labeled UNC6040, attackers targeted Salesforce users at around 20 organisations via voice phishing, tricking employees into installing a fake app giving full access to corporate data.

Vishing is the fraudulent practice of convincing individuals to reveal personal information and bank details over the phone. The fraudulent scheme might start with an unusual e-mail, and while regular phishing emails ask the victim to follow a link, vishing emails ask that they urgently call the number provided in the email. Kaspersky experts emphasise that this method is used by cybercriminals because when people look at a phishing site, they have the time to think about their actions or notice signs that the page

Tatyana Shumaylova
Senior Product Marketing
Manager, Kaspersky
Security Awareness.



is not legitimate. But when victims talk on the phone, they are usually distracted and find it more difficult to focus. Under these circumstances, attackers do everything they can to further throw people off balance: rushing them, intimidating them and demanding that they urgently provide the needed information that helps them to steal money.

The new module within Kaspersky Automated Security Awareness Platform provides real-world case studies, interactive lessons, and practical scenarios to help users identify red flags and adopt safer communication habits. Alongside this release, Kaspersky ASAP now supports over 30 languages across all user interfaces and training materials, making cybersecurity awareness more

accessible to global teams.

"As social engineering evolves, so must the way we educate people about it. Vishing is no longer just a threat to individuals – it's increasingly being used to target organisations, leading to financial losses, data leaks, and reputational damage. Our new vishing module equips users with the knowledge to defend themselves against voice-based deception – a threat that is becoming increasingly sophisticated and personal. We help companies prepare their employees to recognise and resist this type of attack. Since vishing is often a gateway to more serious breaches, it's vital to build awareness across a wide range of related topics," said Tatyana Shumaylova, Senior Product Marketing Manager at Kaspersky Security Awareness. 🔒



tahawultech.com

CISO50 & FUTURE SECURITY AWARDS 2025



 23rd September 2025  Sofitel Dubai Downtown, Dubai  06:00 PM onwards

The most anticipated cybersecurity leadership event in the region returns.

The **CISO 50 Forum & Future Security Awards 2025** brings together the Middle East's most influential cybersecurity decision-makers, experts, and technology leaders to celebrate vision, resilience, and innovation.

This exclusive gathering will spotlight C-level executives and organisations who are driving the evolution of cybersecurity in an era of digital transformation and risk.

Whether you're a corporate leader securing enterprise environments or a solutions provider shaping the security landscape — this is your platform to be recognised and remembered.

OFFICIAL PUBLICATIONS

cnme
computer news middle east

Reseller MIDDLE EAST
THE VOICE OF THE CHANNEL

Security MIDDLE EAST

HOSTED BY

 **tahawultech.com**

#CISO50FSA2025 | #tahawultech



ASUS ExpertBook B5 B5405

**Smart. Secure. AI-Ready
for Business.**



AI-empowered
productivity



Light weight and portable



Long Battery Life



Accelerate business success

FOR FREE DEMO, CONTACT US AT
marketingme.uae@asus.com