ISSUE 98 | SEPTEMBER 2025

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

LINKSHADOW FUTURE OF CYBER DEFENSE

GITEX 2025 TO SHOWCASE LINKSHADOW'S CYBERMESHX PLATFORM, BRINGING UNIFIED INTELLIGENCE AND EXPLAINABLE AI TO MEET THE CHALLENGES OF AN EVOLVING THREAT LANDSCAPE.

tahawultech.com

cnme
computer news middle east
SUPPLEMENT

CONTENTS

Security ADVISOR MIDDLE EAST

EDITOR'S NOTE

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

Sandhya DMello
Editor

RESILIENCE IN THE AGE OF INTELLIGENT THREATS

The cybersecurity landscape is accelerating into uncharted territory, shaped by artificial intelligence, cloud proliferation, and the growing sophistication of attackers. September's issue of Security Advisor Middle East captures this inflection point—where innovation and disruption meet trust and resilience.

Our cover story spotlights LinkShadow's CyberMeshX platform, a bold step towards unifying the fragmented security universe. As the industry converges on Dubai for GITEX 2025, the company's ambition reflects a wider truth: enterprises no longer want silos, they want intelligent ecosystems that deliver visibility, speed, and confidence.

ADAPTIVE ECOSYSTEMS DRIVE RESILIENCE

This month's news and research echo that theme of convergence. SentinelOne's acquisition of Observo AI underscores that security is, fundamentally, a data problem demanding new architectures. Cloudflare and Microsoft's takedown of RaccoonO365 shows how collective disruption can outpace criminal innovation. Meanwhile, leaders such as Tenable, Dell, Kaspersky, and HP remind us that resilience is not static but must constantly evolve across cloud, identity, and endpoint.

Thought leadership from SANS, Veeam, Omnix, and Cloudflare highlights the paradoxes of AI—its promise to empower defenders and its potential to embolden adversaries. The ISACA Infosec & Cybersecurity Congress 2025, which we proudly supported, further reinforced that trust and resilience are not just technical imperatives but cultural and strategic ones.

The pages ahead offer a sweeping view of this shifting terrain—market leadership, new frameworks, disruptive launches, and bold innovations. For CISOs and security leaders, the message is clear: building cyber resilience in 2025 demands not just sharper tools but stronger ecosystems, trusted partnerships, and an adaptive mindset.

EVENTS

tahawultech.com
FUTURE SECURITY
AWARDS

tahawultech.com
CISO50
AWARDS & FORUM

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

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.

DELL RAISES CYBER RESILIENCE STANDARDS WITH ALL-FLASH POWERPROTECT DATA DOMAIN

Dell Technologies unveils the all-flash PowerProtect Data Domain appliance, offering up to 4x faster restores and significant energy savings.

Organisations across industries are contending with increasingly sophisticated cyberattacks that threaten critical data, disrupt operations and erode customer trust. With 88% of enterprises anticipating that generative AI will cause an explosion in data volumes—while 65% admit they back up less than half their data—the pressure on IT leaders to strengthen resilience has never been greater.

Dell Technologies has positioned itself as a long-standing partner in enabling organisations to build resilience. Its strategy rests on three pillars: reducing attack surfaces, detecting threats, and ensuring rapid recovery. The PowerProtect portfolio has become a benchmark in this space, trusted by more than 15,000 customers worldwide for robust data protection on-premises and across multicloud environments.

Redefining cyber resilience

The launch of the PowerProtect Data Domain All-Flash appliance represents a significant evolution of Dell's cyber resilience offering. Built on the proven Data Domain architecture, this high-performance appliance introduces speed, security and efficiency at scale.

Key capabilities include:

- Performance at scale: Up to four times faster data restores and double the replication speed, minimising downtime. Enhanced analytics deliver nearly three times faster integrity validation within a Cyber Recovery vault.
- Efficiency gains: Requires 40% less rack space and provides up to 80% power savings, with a data reduction ratio of up to 65:1.
- Advanced protection: Built-in data immutability, encryption, and hardware root of trust to safeguard against tampering.
- Seamless integration: Native compatibility with Dell PowerStore and PowerMax, plus a wide-ranging backup software ecosystem.
- Extended ecosystem support: Broad DD Boost integration for flexibility, efficiency and collaborative growth.

Portfolio-wide enhancements

The PowerProtect strategy is reinforced with software updates designed to address emerging cyber resilience challenges:

- PowerProtect Data Manager adds support for Red Hat Enterprise Linux deployment, SUSE options for Dell PowerMax, and extended archive-to-object integrations with Wasabi and Dell ObjectScale.
- PowerProtect Cyber Recovery introduces compatibility with the new all-flash appliance and CyberSense Analytics support for Commvault

client-direct backups of Oracle databases.
- PowerProtect Backup Services now extends to Microsoft Azure Storage as a backup target, alongside AWS. It also expands protection for Microsoft environments, offering granular recovery for Dynamics 365, Microsoft 365, Azure VMs and Entra ID.

Strategic impact for enterprises

For organisations in the Middle East and beyond, these advancements are more than incremental updates—they represent a shift in how resilience is built into the digital core. With regional enterprises accelerating digital transformation and confronting increasingly complex cyber risks, Dell's combination of enhanced speed, scalability and security positions it as a reliable partner for ensuring business continuity.

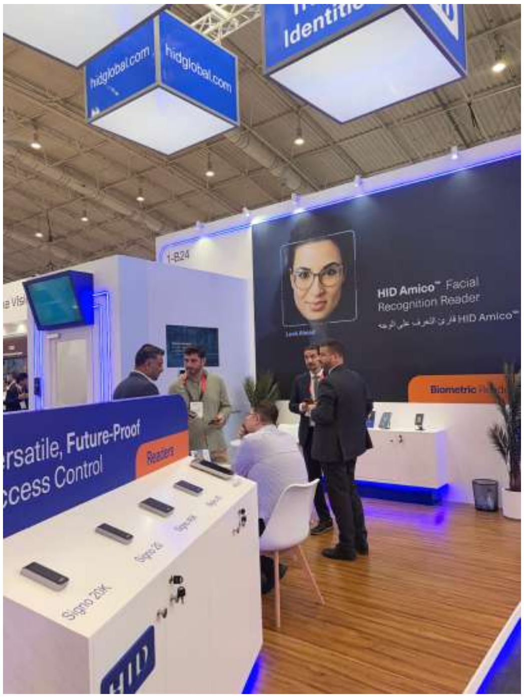
For CISOs and IT leaders, the all-flash PowerProtect Data Domain provides a clear opportunity to modernise resilience strategies while optimising operational efficiency. Crucially, it equips organisations to handle the data-intensive future driven by AI adoption, safeguarding both innovation and trust.

Cyber resilience is emerging as more than just a safeguard—it is a core enabler of digital progress. By ensuring the protection of mission-critical data and maintaining operational continuity, organisations can refocus resources on innovation and long-term value creation. Dell's continued investment in its PowerProtect portfolio underscores its commitment to supporting enterprises in navigating increasingly complex threat landscapes.

HID SHOWCASES NEXT-GENERATION ACCESS CONTROL AT INTERSEC SAUDI ARABIA 2025, SUPPORTING VISION 2030

HID, a global leader in trusted identity solutions, showcased its latest innovations in physical access control and mobile credentialing at the 7th edition of Intersec Saudi Arabia 2025. From biometric recognition to intelligent controllers and mobile-first access solutions, HID demonstrated technologies that align with the Kingdom's Vision 2030 and its accelerating digital transformation agenda.

Saudi Arabia's security market is witnessing rapid growth, fuelled by large-scale infrastructure developments and national digitalisation initiatives. Research forecasts that the sector will expand from USD 2.0 billion in 2024 to USD 3.4 billion by 2030, representing a compound annual growth rate of 9.1%. This underscores the need for secure, interoperable and future-ready access control systems.


hidglobal.com
hidglobal.com
Identity
1-B24
HID Amico™ Facial Recognition Reader
...rsatile, Future-Proof ...ccess Control
Readers
Biometric Re...
Signo 20K
HID

"At a time when Saudi Arabia is undergoing a profound digital and infrastructure transformation, the need for secure, interoperable and future-ready access control systems has never been greater," said Gustavo Gassmann, Vice President of Emerging Markets for Physical Access Control at HID. "Our solutions support the Kingdom's Vision 2030 ambitions by delivering technologies that enhance security, streamline operations and provide a seamless user experience."

Next-generation access innovations

At booth 1-B24, HID presented live demonstrations of its newest technologies, including:

- HID Amico Biometric Readers: Contactless facial recognition readers with 3.5" or 7" TFT colour displays, suitable for mid-sized organisations and high-traffic environments. The 7" model includes a built-in SIP intercom.
- Mercury Intelligent Controllers: Next-generation MP1501 and MP1502 controllers feature enhanced processing, secure boot, TLS 1.3 support and flexible PoE+ installation for modern security infrastructures.
- HID® Aero Controllers (X100 and X1100): Provide robust IO support for up to two access points, ensuring reliable monitoring and secure foundations for access deployments.
- HID Signo Readers: Modern, flexible readers supporting multiple credential technologies and offering advanced security features.
- HID Mobile Access: Enables smartphones and smartwatches to serve as secure access credentials, integrated with Apple Wallet and Google Wallet, replacing traditional physical cards.

Supporting digital transformation in the Middle East

HID's portfolio reflects a strategic focus on combining advanced hardware with mobile and digital credentialing.

By integrating biometric recognition, intelligent controllers and mobile-first solutions, the company aims to help organisations future-proof their security strategies while delivering efficiency and user convenience.

"Our strategy goes beyond launching new products," said Sam Cherif, Senior Director and Head of Middle East Africa at HID. "We are committed to building future-ready security ecosystems that support enterprises and government entities across the Middle East in achieving greater security and operational efficiency."

HID's participation at Intersec Saudi Arabia 2025 comes at a pivotal moment for the Kingdom's security sector, as demand for advanced identity solutions rises in line with national infrastructure and digitalisation initiatives.

CLOUDFLARE JOINS MICROSOFT IN GLOBAL OPERATION TO DISMANTLE RACCOON0365

Cloudflare, in partnership with Microsoft, has successfully disrupted the phishing-as-a-service (PhaaS) criminal enterprise known as Raccoon0365. The operation was conducted by Cloudflare's Cloudforce One and Trust & Safety teams, in coordination with Microsoft's legal actions, to dismantle the infrastructure supporting widespread credential theft campaigns.

Raccoon0365 abused Cloudflare services and other providers to conceal its phishing kits, which were designed to steal Microsoft 365 credentials. Victims were lured to fake login pages via phishing emails containing malicious links or QR codes. Once solved through a simple CAPTCHA, users were redirected to fraudulent Microsoft O365 pages where their credentials, cookies, and account data could be harvested.

Cloudflare and Microsoft coordinated a global operation to disrupt the Raccoon0365 phishing network targeting Microsoft 365 users.

The stolen information was sold to subscribers, enabling financial fraud, extortion, and potential ransomware deployment.

Large-scale takedown

In early September 2025, Cloudflare executed a coordinated takedown of hundreds of domains and Worker accounts associated with Raccoon0365. This proactive approach marked a departure from reactive, case-by-case mitigation.

The takedown, aligned with Microsoft's civil lawsuit filed in late August, effectively dismantled the actor's infrastructure across Cloudflare's network. According to the company, the operation was intended to increase the group's costs, disrupt their activities, and send a message that "the free tier is too expensive for criminal enterprises."

The Raccoon0365 model

Raccoon0365 functioned as a subscription-based phishing service, lowering the barrier for cybercriminals to conduct sophisticated credential harvesting campaigns.

Since July 2024, Microsoft has observed its kits used to steal at least 5,000 Microsoft credentials from victims in 94 countries. The group offered tiered subscription plans through a private Telegram channel, priced from $355 for 30 days to $999 for 90 days, with payments accepted exclusively in cryptocurrency.

The service marketed itself as secure, anonymous, and capable of bypassing multi-factor authentication. Microsoft has identified the group's leader as Nigeria-based Joshua Ogundipe, with evidence of collaboration with Russian-speaking actors.

Coordinated disruption

Cloudflare's approach evolved through three phases:

- **Reactive stage:** addressing individual abuse complaints as domains were reported.
- **Collaboration:** Microsoft initiated the legal seizure of hundreds of domains, while Cloudflare simultaneously suspended Raccoon0365 operations on its platform.
- **Proactive takedown:** using signup patterns, Cloudflare mapped the group's infrastructure, banned associated domains, suspended Worker scripts, and placed warning interstitials on blocked sites.

The operation, conducted between 2–4 September 2025, was coordinated with Microsoft and US law enforcement to ensure long-term disruption of the group's activities.

HP RESEARCH UNCOVERS INCREASINGLY SOPHISTICATED PHISHING CAMPAIGNS HIDING MALWARE IN EVERYDAY FILE TYPES.

HP research uncovers increasingly sophisticated phishing campaigns hiding malware in everyday file types.

HP Inc. has warned that attackers are evolving their social engineering playbook, deploying highly convincing phishing lures and chaining "living-off-the-land" (LOTL) techniques to bypass security controls.

The company's latest Threat Insights Report, covering April to June 2025, shows how cybercriminals are combining old techniques with fresh twists, making it harder than ever for defenders to spot malicious activity disguised as legitimate system behaviour.

One campaign involved an exceptionally realistic fake Adobe Reader invoice. The lure featured a fabricated loading bar to persuade users it was a genuine document in progress. Beneath the surface, however, attackers had embedded a reverse shell within an SVG image file, handing them remote control of infected devices. To evade analysis, downloads were restricted to German-speaking regions, reducing exposure to automated threat-detection systems.

Another attack used Microsoft Compiled HTML Help files to conceal malware inside image pixel data. The files, disguised as project documentation, carried an XWorm payload. PowerShell was then deployed to launch a multi-stage infection and erase digital traces, making investigations significantly harder.

Old threats, sharpened tactics

Despite a law enforcement crackdown earlier this year, Lumma Stealer – one of the most active malware families of 2025 – made a strong comeback in Q2. The report found the malware distributed through IMG archive attachments that used LOTL techniques to bypass email security filters.

"Attackers aren't reinventing the wheel, but they are refining their techniques," said Alex Holland, Principal Threat Researcher, HP Security Lab. "We're seeing more chaining of living-off-the-land tools and the use of less obvious file types, such as images, to evade detection. A lightweight script can often achieve the same effect as a more complex remote access trojan, but with far less chance of triggering alarms."

Growing challenge for defenders

The report highlights how detection-based tools are struggling to keep pace. Thirteen percent of email threats analysed by HP bypassed at least one secure email gateway. Archive files remain the top delivery method at 40 percent, followed by executables and scripts at 35 percent. Attackers continue to rely heavily on trusted software like WinRAR, with .rar files used in more than a quarter of campaigns.

Dr Ian Pratt, Global Head of Security for Personal Systems at HP Inc., warned: "Living-off-the-land techniques are notoriously difficult for security teams because it's hard to tell legitimate activity from an attack. You're stuck between a rock and a hard place – lock down activity and create friction for users, or leave it open and risk compromise. Even the best detection will miss some threats, so defence-in-depth with containment and isolation is essential."

HP Wolf Security's hardware-enforced isolation allows malware to execute safely within secure containers, giving researchers visibility into attack methods without endangering users. To date, customers have opened more than 55 billion email attachments, web pages and downloaded files without a single reported breach.

By spotlighting these campaigns, HP aims to give organisations the insights they need to strengthen cyber resilience in the face of increasingly creative and adaptive adversaries.

KASPERSKY STRENGTHENS CLOUD PROTECTION WITH NEW CLOUD WORKLOAD SECURITY UPDATE

Kaspersky has expanded its Cloud Workload Security suite to address rising cloud security challenges, adding new runtime defences and platform integrations.

Kaspersky has released an upgraded version of its Cloud Workload Security (CWS) offering, aimed at strengthening protection across hybrid and multicloud environments. The update addresses the growing complexity of enterprise cloud infrastructures by improving visibility, enhancing container runtime defence, and providing organisations with a more cost-efficient and flexible approach to securing workloads.

Research conducted by Kaspersky and ISG highlights the urgency of stronger protection measures. In their joint paper, Alleviating cloud migration difficulties with robust hybrid-cloud and container security, 60 per cent of surveyed organisations identified monitoring and proactively preventing runtime misconfigurations of cloud assets as one of their top five cloud security challenges. The latest CWS update directly responds to these concerns, equipping enterprises to remain one step ahead of evolving cyberthreats.

Kaspersky Cloud Workload Security consists of two core products: Kaspersky Container Security (KCS) and Kaspersky Hybrid Cloud Security (KHCS). The new release of KCS introduces node OS vulnerability scanning and file threat protection to extend runtime defence across both nodes and orchestrators. Customers are now able to enrich network reputation data with feeds from their own sources, alongside NIST and Kaspersky databases, ensuring intelligence tailored to their unique threat landscape. Operational transparency is also improved with detailed logging of changes in Role-Based Access Control (RBAC) cluster objects, while incident response becomes more agile through WebHooks support, which allows data to be shared with any compatible software without requiring direct integration. Furthermore, the product now supports Microsoft Azure Registry and Google Cloud Platform Kubernetes & Registry, expanding the protection of workloads across a wider set of environments.

The update also extends security policies across Assurance, Runtime and Response to achieve higher detection rates and greater flexibility, enabling protection to be aligned with both business priorities and regulatory requirements. In parallel, the Light Agent in Kaspersky Hybrid Cloud Security has been enhanced to leverage Kaspersky Endpoint Security for Windows (12.10) and Kaspersky Endpoint Security for Linux (12.3), improving integration and boosting security capabilities for hybrid infrastructures.

The enhanced CWS suite has been designed to tackle persistent customer challenges such as cloud security blind spots, rising infrastructure costs, regulatory compliance pressures, and the limitations of traditional endpoint and open-source tools in protecting multicloud workloads. By combining advanced automation with rich contextual intelligence, the solution allows enterprises to strengthen resilience, reduce operational risk and maintain compliance without hindering business objectives.

Anton Rusakov-Rudenko, Senior Product Marketing Manager for Cloud & Network Security Product Line at Kaspersky, said: "With the latest updates to Kaspersky Cloud Workload Security, we're continuing to push the boundaries of cloud security, providing our customers with the most comprehensive and robust protection available. Our goal is to empower businesses to take full advantage of the cloud's potential, without compromising on security. With these updates, we're helping our customers to stay one step ahead of emerging threats and maintain the highest levels of security and compliance in their cloud infrastructure."

SANS SECURE AI BLUEPRINT OFFERS STRUCTURED GUIDANCE FOR ENTERPRISE ADOPTION

The SANS Institute has launched its Secure AI Blueprint, a comprehensive model to help organisations adopt artificial intelligence securely and responsibly across their operations.

The framework, titled Own AI Securely, responds to growing demand from enterprises grappling with questions around AI safety, compliance, and operational control. Security teams in both the public and private sectors are increasingly required to defend systems evolving faster than current playbooks can support. The blueprint provides outcome-focused guidance that reflects the realities of enterprise-scale AI adoption and the skilled workforce it requires.

Rob T. Lee, Chief of Research and Chief AI Officer at SANS Institute, says the Secure AI Blueprint provides structure where AI adoption has lacked clarity.

The UAE has positioned AI as a cornerstone of its governance and economic diversification agenda. The National Strategy for AI 2031 outlines plans to integrate AI as a driver of efficiency, growth, and sustainability. PwC forecasts that global AI spending will exceed USD 300 billion by 2026, with AI contributing up to 13.6% of the UAE's GDP by 2030.

"As roles related to AI rapidly shift and new risks constantly emerge, organisations need to keep up with this pace of change and respond decisively," said Rob T. Lee, Chief of Research and Chief AI Officer at SANS Institute. "This blueprint gives structure to an environment that has, until now, lacked clear direction. It's built on field-tested insights and designed to help security leaders act with clarity and purpose."

The Secure AI Blueprint introduces a three-track model, supported by 14 training courses and GIAC certifications that map directly to organisational functions. It enables enterprises to build a capable, skilled AI cybersecurity workforce through three domains:

- **Protect AI** – Security and engineering teams defend AI systems against poisoning, prompt injection, and data leakage, with strong controls for access, deployment, and monitoring.
- **Utilise AI** – Cyber defenders use AI to enhance detection, triage, and response within SOCs, digital forensics, and red team operations, ensuring they can counter adversaries operating at machine speed.
- **Govern AI** – Executives and boards establish oversight, compliance frameworks, and AI fluency, ensuring alignment with regulations while fostering trust and accountability.

"The blueprint is based on what's already changing inside real organisations," Lee added. "Leaders are not looking for more generic headlines about how the threat landscape is evolving fast, they're looking for a way to act. The SANS model provides structure where there has been confusion, and alignment where there has been fragmentation."

SENTINELONE TO ACQUIRE OBSERVO AI TO TRANSFORM SIEM AND SECURITY OPERATIONS

SentinelOne has announced its intent to acquire Observo AI, the AI-native data streaming platform designed for telemetry pipeline management. The acquisition is expected to accelerate SentinelOne's AI SIEM and data offerings, which already rank among the company's fastest-growing solutions.

The integration of Observo AI will allow SentinelOne to strengthen its capabilities in delivering open, intelligent, and autonomous security operations, helping security operations centre (SOC) teams collect, enrich, and act on data more efficiently across the entire security ecosystem.

Addressing the challenges of modern SOCs

The announcement comes at a time when SOC teams are grappling with rising costs, operational complexity, and delays caused by unprecedented data volumes. Traditional data platforms—designed before the advent of AI-enabled SOCs and today's increasingly sophisticated threats—struggle to keep pace.

Observo AI offers an AI-native telemetry pipeline that ingests, enriches, summarises, and routes data before it reaches a SIEM or data lake. By processing information at the source, customers benefit from reduced costs, faster detection, and sharper incident response.

AI-native capabilities at scale

SentinelOne highlights several advantages Observo AI will deliver:

- Open integration: Support for open formats such as OCSF, JSON, OTLP, and Parquet ensures flexibility without vendor lock-in.
- AI-driven enrichment: Real-time classification, correlation, and summarisation improve data quality and reduce noise before storage.
- Operational efficiency: Intelligent filtering can reduce data volumes by up to 80 per cent while enabling full-fidelity log recovery when required.
- Enterprise scale: Features such as centralised fleet management, automated discovery, and PII masking reinforce governance, compliance, and security posture.
- Empowering humans and AI: Natural language querying, anomaly detection, and enriched telemetry help both human analysts and AI agents act with greater speed and precision.

Tomer Weingarten
CEO and Co-founder of SentinelOne.

Building towards autonomous security

This acquisition builds on SentinelOne's existing investment in hyperscale data infrastructure within its Singularity Platform. By integrating Observo AI, the company will offer a policy-driven data pipeline optimised for real-time enrichment, filtering, and routing.

According to SentinelOne, the combined architecture will enable agentic AI workflows—where autonomous agents leverage enriched, real-time data to detect, decide, and respond at machine speed with human-level reasoning.

Industry perspectives

"Security is, at its heart, a data problem, and legacy, rules-based data pipeline platforms simply weren't built for today's ever-growing attack surface," said Tomer Weingarten, CEO and Co-founder of SentinelOne. "Observo AI is miles ahead of its rivals and will uniquely benefit customers with an AI-native data architecture, one that is open by design, intelligent by default, and built for the scale and speed needed for autonomous security operations."

Gurjeet Arora, Co-founder and CEO of Observo AI, added: "Observo AI was born in the AI and cloud era to help security and DevOps teams tackle previously unimaginable data problems. Joining forces with SentinelOne gives us a rare opportunity to define the future of autonomous security."

Transaction details

SentinelOne will acquire Observo AI in a cash and stock transaction, subject to regulatory approval and customary closing conditions. The deal is expected to close in SentinelOne's third quarter of fiscal year 2026.

TENABLE RANKED FIRST IN GLOBAL DEVICE VULNERABILITY AND EXPOSURE MANAGEMENT

Tenable, the exposure management company, has been ranked first for 2024 worldwide market share in the IDC Worldwide Device Vulnerability and Exposure Management Market Shares.

Exposure management is increasingly recognised as the future of proactive and preventive cybersecurity. Unlike traditional vulnerability management, it provides organisations with a holistic view of risk, helping to measure and reduce exposures before they are exploited. Tenable attributes its leadership to its early adoption of exposure management principles, coupled with a robust partner ecosystem and channel-first approach.

AI-powered risk visibility

The Tenable One platform unifies data from more than 300 third-party security tools alongside Tenable's own sensors. By correlating and normalising this information, then applying attack path analytics, the platform offers security teams a single AI-powered view of exposures across their digital infrastructure. This enables defenders to prioritise and remediate the vulnerabilities most likely to be weaponised.

Mark Thurmond, Co-Chief Executive Officer at Tenable, commented:

"We remain focused on pushing the envelope of exposure management solutions that help our customers evolve their security strategies and not just stop breaches, but prevent them before they even happen."

The IDC report highlights Tenable's position as the most open and interconnected exposure management platform on the market, noting its extensive integrations and data aggregation capabilities.

Advancing with AI-driven exposure management

The analysis also points to Tenable's recent acquisition of Apex Security, reinforcing its commitment to integrating artificial intelligence into exposure management. In August 2025, Tenable launched AI Exposure, a capability within Tenable One that provides visibility into how AI is deployed across organisations. This innovation enables enterprises to detect risks and apply controls to securely adopt generative AI tools.

According to Michelle Abraham, Senior Research Director for Security and Trust at IDC:

Mark Thurmond, Co-CEO, Tenable

"Proactive exposure management is the future as traditional vulnerability detection transforms into holistic risk management and remediation. As attack surfaces expand, organisations must leverage advanced tools to illuminate hidden risks and close critical gaps before exploitation occurs."

Market leadership recognition

This ranking builds on Tenable's recognition in the IDC MarketScape: Worldwide Exposure Management 2025 Vendor Assessment (doc #US52994525, August 2025), where the company was named a Leader.

With approximately 44,000 customers worldwide, Tenable continues to position exposure management as a foundation of enterprise resilience, delivering visibility and actionable intelligence to defend against evolving threats.

CROWDSTRIKE DELIVERS UNIFIED DATA AND IDENTITY PROTECTION FOR THE AI ERA

CrowdStrike used its flagship security conference to deliver a clear message to enterprises: security in the AI era must be unified, intelligent and resilient. The company introduced two major enhancements to its Falcon platform—Falcon Data Protection and Falcon Next-Gen Identity Security—both designed to address critical blind spots that legacy solutions fail to cover. Together, these innovations mark a decisive move towards a consolidated, platform-based approach that aligns with the realities of hybrid, AI-driven business environments.

Redefining data protection for GenAI

The rise of generative AI has transformed how organisations use and share information, but it has also exposed them to unprecedented risks. Traditional data loss prevention and posture management tools were created for static infrastructures and cannot cope with the dynamism of modern workflows. Falcon Data Protection seeks to change that by safeguarding sensitive data across endpoints, cloud environments, SaaS applications and generative AI tools.

Elia Zaitsev
Chief Technology Officer, CrowdStrike

"AI has reshaped how data is created and shared, but legacy data loss prevention and posture management tools weren't built to secure data in the modern era," said Elia Zaitsev, Chief Technology Officer at CrowdStrike. "Falcon Data Protection follows sensitive data everywhere it moves, across devices, cloud services, SaaS applications, and GenAI workflows. By delivering the real-time visibility and enforcement customers need, we're making it easier to consolidate cybersecurity at scale and securely innovate with AI."

With Falcon Data Protection, security no longer stops at the browser or the network boundary. The solution extends into local applications and runtime cloud environments, giving security teams visibility into how shadow AI tools are deployed on endpoints and offering AI-driven classification that distinguishes critical data such as credentials and secrets from less sensitive information. It also introduces a more complete view of insider risk by correlating data movements with identity and HR signals, enabling faster detection and response.

Closing identity gaps with unified protection

While securing data is vital, identity continues to be the most common entry point for attackers. In today's hybrid enterprises, access spans human users, machines and increasingly, AI agents.

LINKSHADOW CYBERMESHX: UNIFY YOUR ENTIRE SECURITY UNIVERSE – ONE PLATFORM, COMPLETE VISIBILITY

LINKSHADOW SETS THE STAGE FOR THE FUTURE OF CYBERSECURITY AT GITEX 2025 WITH ITS CYBERMESHX PLATFORM, PROMISING UNIFIED INTELLIGENCE FOR A RAPIDLY EVOLVING THREAT LANDSCAPE.

LinkShadow, a global leader in cutting-edge cybersecurity solutions, is redefining cybersecurity through its flagship platform CyberMeshX, a unified security ecosystem that integrates data, identity, and network protection. Headquartered in Athens, Georgia, founded in 2015, the company has grown into a recognised innovator in AI-powered cybersecurity, with a global footprint and strong presence in the Middle East.

Speaking to Sandhya D'Mello, Technology Editor, CPI Media Group, for the September issue of Security Advisor Middle East, Fadi Sharaf El-Dean, Chief Revenue Officer, LinkShadow, charted the brand's plans to offer disruptive solutions to organisations to be proactive in detecting threats and build on its cyber resilience strategies.

Gitex — Global stage

The global brand is gearing up for the UAE's popular five-day technology exhibition — Gitex Global which will set the global stage in October 2025. The tech fair has emerged as the definitive showcase of technology shaping the digital economy. For cybersecurity professionals across the Middle East, it is more than an exhibition — it is a barometer of future resilience. In 2025, the spotlight shines on LinkShadow, whose CyberMeshX platform is being positioned as a transformative force in the industry.

Enterprises struggle with increasingly sophisticated threats and fragmented defense systems. CyberMeshX offers a bold promise: a single, unified platform that empowers security teams with comprehensive visibility, contextual intelligence, and actionable insights.

Beyond SIEM and XDR: The new security mesh

The cybersecurity industry has long relied on solutions such as Security Information and Event Management (SIEM) and Extended Detection and Response (XDR), each of which is valuable yet often operates in silos. The tools excel at monitoring specific layers — logs, endpoints, or network activity — but they leave gaps that adversaries are quick to exploit.

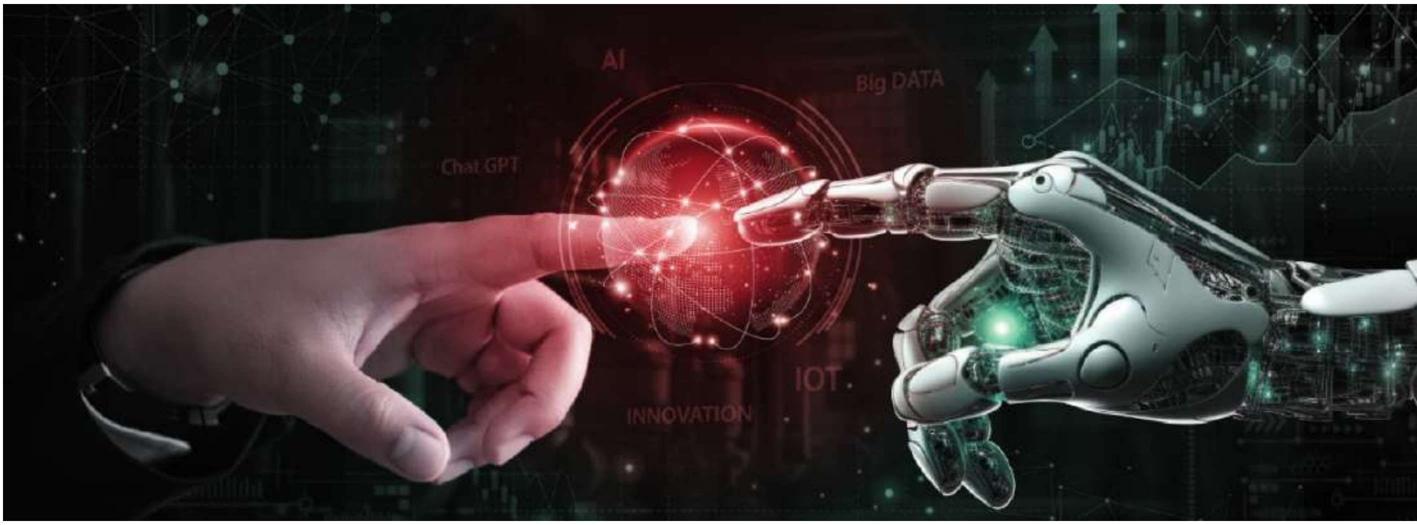
Fadi Sharaf said, "CyberMeshX isn't just another SIEM or XDR bolted together. Traditional platforms focus on isolated layers — logs, endpoints, or network events. CyberMeshX fuses identity, data, and network visibility into one mesh, giving security teams a single investigation plane, where instead of piecing together random alerts, they see the entire attack storyline, end-to-end across cloud, endpoints, and identities."

By reimagining detection and response through a Cybersecurity Mesh Architecture (CSMA), LinkShadow ensures that organisations are no longer piecing together incomplete pictures, but instead view entire attack narratives with clarity.

Trust in AI: Explainability at the core

Artificial intelligence has become indispensable in security operations, but it also introduces concerns around bias, opacity, and reliability in mission-critical environments. For LinkShadow, trust is non-negotiable.

"We all know AI is becoming central, but in mission-critical environments, trust is everything. Every detection comes



with the why: linked evidence, MITRE mapping, and context. We continuously retrain to minimise bias, and most importantly, we reduce false positives through multi-signal correlation — so analysts don't waste time chasing ghosts," said Fadi Sharaf.

This emphasis on explainable AI reflects a practical philosophy: technology must empower analysts, not overwhelm them. With confidence restored, security teams can focus on strategy rather than firefighting.

Identity: Today's top breach vector

In today's landscape, identity has emerged as the new perimeter. From service accounts to hybrid cloud users, digital identities have become prime targets for attackers. LinkShadow's answer is Identity Threat Detection and Response (ITDR), a critical pillar within CyberMeshX.

"Identity is today's top breach vector. With LinkShadow ITDR, we baseline every identity — users, service accounts, and privileges — across hybrid and multi-cloud. We can flag suspicious behavior, such as impossible travel, privilege escalation, or token misuse, in real-time. It strengthens the enterprise identity posture by ensuring that trust is continuously validated, not just assumed," said Fadi.

This proactive approach to identity security marks a decisive shift from static validation to continuous verification, ensuring enterprises stay ahead of emerging threats.

Data sovereignty and compliance: The GCC imperative

In the GCC, regulatory compliance and data sovereignty are top boardroom priorities. With a patchwork of evolving regulations — from the UAE's Personal Data Protection Law (PDPL) to Saudi Arabia's National Cybersecurity Authority (NCA) frameworks — organisations need tools that guarantee compliance across cloud, SaaS, and on-premise environments.

"In our region, data sovereignty is crucial. LinkShadow DSPM automatically discovers and classifies sensitive data across SaaS, cloud, and on-prem. It enforces retention rules, highlights misplaced PII/PCI/PHI data, and builds a living data inventory. That gives CISOs confidence they are compliant with frameworks like PDPL, SAMA, NCA, and ADHICS v2 — not once a year, but continuously," said El-Dean.

This approach transforms compliance from a periodic exercise into a continuous state of readiness, offering CISOs reassurance in the face of tightening regional laws.

Deep Visibility with Intelligent NDR

The foundation of CyberMeshX includes LinkShadow's Intelligent Network Detection and Response (NDR), a capability built to uncover threats in real time across complex network environments. What sets it apart is its adaptive intelligence — the ability to learn, profile, and respond as threats evolve.

NDR provides security teams with:

- Complete visibility through custom dashboards, centralized threat visualization, and real-time measurement of security tool effectiveness.
- AI-driven threat hunting, where anomaly detection, automated incident response, and deep forensic analysis empower SOC analysts to neutralize risks before they escalate.
- Behavioral analytics that continuously profile assets, quantify risks, and flag anomalies for prioritised response.

By combining traffic and protocol analysis with automated response, LinkShadow's NDR transforms raw network data into actionable insights.

It reduces Mean Time to Detect and Respond (MTTDR), strengthens compliance reporting, and simplifies network mapping — ensuring no blind spot is left uncovered.

For enterprises, this translates into faster decisions, proactive containment, and greater resilience, enabling SOC teams to move from reactive firefighting to strategic defense.

Turning alert fatigue into intelligence

Ask any analyst about their greatest frustration, and the answer is consistent: alert fatigue. Hundreds of daily alerts, most of them noise, stretch resources thin and create opportunities for real threats to slip through. CyberMeshX directly tackles this problem.

"One of the biggest frustrations in SOCs is drowning in alerts. CyberMeshX changes that. Instead of 50 disconnected alerts, analysts get a coherent narrative:

'credential theft → lateral movement → data exfiltration' in a single storyboard. It cuts the noise and transforms detection into clear, actionable intelligence," explained El-Dean.

The platform reframes cybersecurity from managing alerts to interpreting stories — narratives that are richer, sharper, and more actionable.

Resilience with ROI: Doing more with less

CISOs today are tasked with achieving resilience while balancing shrinking budgets. CyberMeshX addresses this dual mandate by consolidating toolsets, lowering SIEM ingestion costs, and accelerating investigations.

"CISOs are under pressure to deliver more resilience with tighter budgets. CyberMeshX delivers measurable ROI by cutting SIEM ingestion costs, consolidating overlapping tools, and reducing investigation time from hours to minutes. Analysts are freed from noise to focus on real threats — that's both cost savings and resilience in one move," points out Fadi Sharaf.

Here, the conversation extends beyond defense to financial stewardship — ensuring cybersecurity is seen as both protector and enabler of business value.

LinkShadow recognises that most enterprises already operate with complex, layered security stacks. Rip-and-replace strategies are impractical. CyberMeshX is designed API-first, integrating seamlessly with existing tools such as firewalls, CASBs, SIEM, and SOAR.

The migration philosophy is pragmatic: start with visibility — for example ITDR or DSPM — while keeping legacy tools operational. Gradually, CyberMeshX becomes the brain of the security operations, while existing systems remain the muscles. This reduces disruption while maximising outcomes.

Preparing for the future: AI adversaries and tightening laws

Looking ahead, the regional threat landscape is expected to intensify, with AI-driven phishing, deepfake campaigns, and multi-stage attacks targeting critical sectors such as finance, healthcare, and energy. At the same time, stricter data residency laws will demand even greater vigilance.

LinkShadow is aligning CyberMeshX precisely with these realities — uniting identity, data, and network signals to build full attack stories that help organisations anticipate, not just react.

Ultimately, the CyberMeshX vision is about reshaping the future of cyber defense. Instead of reacting to endless alerts, organisations are equipped with decision-intelligence layers that automate containment, strengthen posture, and deliver proactive resilience.

"We're entering a new era. Defense is shifting from reactive alerts to proactive resilience. Adversaries are using AI to automate attacks — defenders must do the same to stay ahead. Platforms like CyberMeshX will be the decision-intelligence layer of the SOC: explainable AI, unified visibility, and automated containment. That's the foundation of the next generation of cyber defense," said El-Dean.

As GITEX 2025 unfolds, LinkShadow's CyberMeshX is set to capture the imagination of cybersecurity leaders seeking answers to some of the industry's toughest challenges. By unifying visibility, contextualising threats, and embedding intelligence at every layer, the platform promises to do more than just defend — it enables organisations to thrive in the age of AI-driven threats.

For CISOs, analysts, and security professionals in the Middle East, CyberMeshX is not just another product launch at GITEX. It is a blueprint for the future of cybersecurity — resilient, intelligent, and unified.

ISACA & TAHAWULTECH INFOSEC CYBERSECURITY CONGRESS 2025 HIGHLIGHT DIGITAL TRUST, RESILIENCE, AND AI SECURITY

The ISACA Abu Dhabi Infosec & Cybersecurity Congress 2025, hosted in partnership with Tahawultech.com, convened industry leaders, experts, and security professionals to address the urgent challenges shaping the future of cybersecurity. With an agenda centred on trust, resilience, and the evolving impact of AI, the event — hosted in Abu Dhabi on September 16 — offered practical insights and strategic direction to navigate today's digital threat landscape.

Call for trust and resilience

The day commenced with a welcome address by Sandhya D'Mello, Editor, CPI Media Group, who underscored the pivotal role of trust and innovation in securing digital futures. She also extended gratitude to Gold Sponsor Delinea and Silver Sponsor Teksalah for supporting the congress. This was followed by opening remarks from Dr. Alok Tuteja, Ex-President of ISACA UAE Chapter, who set the tone for the day's discussions, highlighting the rapid technological shifts redefining governance and risk in cybersecurity.

Navigating trust in the intelligent age

The first panel, "Navigating the Trust Deficit in the Intelligent Age", explored how organisations can balance innovation and governance as AI and automation reshape industries. Moderated by Sandhya D'Mello, the session featured: Kapil Matta, Regional Head, DigitalXForce; Bader Al Zyouud, Head of Section – Information and Security, Governance and Risk Management, Abu Dhabi Media (ADM); and Bharat Raigangar, Global Head – AI Cyber Security and Risk Management, Maseera Holding.

The discussion emphasised that digital security extends beyond technology—encompassing confidence, resilience, and adaptability in a fast-evolving landscape.

Following the panel, a special sponsor message from Delinea showcased how privileged access management is transforming security practices worldwide. A fireside chat with Vijay Balakrishnan, Sales Engineer at Delinea, provided deeper insights into practical strategies for enhancing security and digital trust.

AI's double edge: security paradoxes

The second panel discussion, "AI's Double Edge in the Perfect Storm", examined how artificial intelligence accelerates innovation while simultaneously introducing new vulnerabilities. Speakers included: Dr. Alok Tuteja, Head of Governance,

tahawultech.com
INFOSEC & CYBERSECURITY CONGRESS 2025
ABU DHABI
DR.ALOK TUTEJA
CGEIT, CRISC
Ex-President
ISACA UAE Chapter
AMAR PRAKASH
Audit Manager
AL TAYER GROUP
ZAHEER MUBARAK SHAIKH
Chief Information Security Officer
MBANK

CONGRESS 2025
ABU DHABI
HANI ABDEL KARIM BANI AMER
Head – Information Security
Al Etihad Payments
VISHNU PADMAKUMAR
Head of Digital Security Section
General Pension and Social Security Authority (GPSSAAE)
ALI ISMAIL AWAD
Associate Professor of Cybersecurity
United Arab Emirates University (UAEU)
Cybersecurity Country Head – HBME
HSBC Bank Middle East Limited
#infosec&cybersecuritycongress

KAPIL MATTA
Regional Head
DigitalXForce
BADER AL ZYOUUD
Head of Section – Information Security Governance & Risks Management
Abu Dhabi Media (ADM)
BHARAT RAIGANGAR
Global Head – AI Cyber Security and Risk Management
Maseera Holding

Esyasoft Holdings; Amar Prakash, Audit Manager, Al Tayer Group; and Zaheer Mubarak Shaikh, Chief Information Security Officer, MBANK. The session highlighted the paradoxes of AI—trust vs. risk, and opportunity vs. threat—emphasising the need for balance and foresight in deployment strategies.

Building resilience amid uncertainty

The third panel, "Building Resilience – Strategy, Culture and Digital Trust in the Age of Uncertainty", moderated by Kapil Matta, featured: Vishnu Padmakumar, Head of Digital Security Section, GPSSAAE; Ali Ismail Awad, Associate Professor of Cybersecurity, UAE University; and Ali Othman, Cybersecurity Country Head – HSBC Bank Middle East Limited. The conversation reinforced resilience as a core organisational capability, rooted not only in robust technology but also in adaptive strategy and culture.

Delinea
for the
IT Administrator
Identity Lifecycle & Governance

VIJAY BALAKRISHNAN
Sales Engineer
Delinea
tahawultech.com
INFOSEC & CYBERSECURITY CONGRESS 2025
ABU DHABI
#securitycongress2025 #tahawultech #isacauaechapter

Recognising cybersecurity leadership
The congress also celebrated excellence through the CISO Infosec and Cyber Risk Leadership Awards 2025, recognising individuals and organisations driving impactful change in the cybersecurity ecosystem. Among the awardees were:

- **Manish Agarwal,** M. H. Enterprises LLC
- **Ali Chehade,** CFI Global
- **Bharat Jethanand Raigangar,** Maseera Holding
- **Mohamed Riyasudeen,** Al Ain Ahlia Insurance Company (PSC)
- **Talal Albalas,** Ministry of Culture, Government of United Arab Emirates
- **Bipin Mehta,** HSBC Bank Middle East Limited
- **Vishnu Padmakumar,** General Pension and Social Security Authority (GPSSAAE)
- **Hani Abdel Karim Bani Amer,** Al Etihad Payments
- **Amar Prakash,** Al Tayer Group
- **Ali Ismail Awad,** United Arab Emirates University (UAEU)

Presenters included representatives from Delinea, Teksalah, CPI Media Group, and ISACA-Abu Dhabi Chapter.

Collaboration and community
The event concluded with networking, offering attendees the opportunity to continue conversations and explore collaborations.

Sandhya D'Mello, closing the sessions, remarked: "Today's congress has shown us that building digital trust requires not just strong technology, but collective resilience, cultural readiness, and shared responsibility. We look forward to continuing this dialogue in future editions."

TP-LINK MEA POWERS INTO 2025 WITH WI-FI 7, AI, AND SCALABLE SECURITY

IN AN EXCLUSIVE INTERVIEW WITH TAHAWULTECH.COM, LUCAS JIANG, GENERAL MANAGER OF TP-LINK MEA, SHARES TP-LINK'S VISION FOR TRANSFORMING CONNECTIVITY, EMPOWERING CHANNEL PARTNERS, AND DRIVING DIGITAL TRANSFORMATION ACROSS THE MIDDLE EAST AND AFRICA.

TP-Link is setting bold benchmarks for innovation in 2025, reshaping the future of connectivity and security. The company's strategic roadmap include rollout of a comprehensive Wi-Fi 7 portfolio and AI-optimised network management to game-changing surveillance advancements with solar-powered VIGI devices and Omada's centralised systems. With an emphasis on empowering channel partners, driving sustainability, and expanding across the Middle East and Africa, Jiang explains how TP-Link is making cutting-edge technology more accessible while solidifying its position as a leader in secure, scalable networking solutions.

How does TP-Link's Wi-Fi 7 technology enhance connectivity, and what challenges do you foresee in its adoption across the MEA region?
TP-Link's Wi-Fi 7 technology brings groundbreaking advancements in wireless networking, set to transform connectivity experiences. We take great pride in being the first vendor to launch a complete range of Wi-Fi 7 solutions for both home and enterprise environments.

The Wi-Fi 7 technology brings significant improvements in speed, latency, and network capacity. It delivers ultra-fast data rates of up to 46 Gbps—nearly 4.8 times faster than Wi-Fi 6—thanks to 320 MHz bandwidth and 4096-QAM modulation, ideal for HD streaming, gaming, and smart homes. Latency is reduced by up to four times, enabling real-time performance for VR and interactive applications. Additionally, Multi-Link Operation (MLO) boosts network capacity and efficiency by handling multiple data streams across frequency bands, making it ideal for device-dense environments like offices and public spaces.

The adoption of Wi-Fi 7 technology across the Middle East and Africa (MEA) region faces several challenges. One of the primary hurdles is infrastructure limitations, as many areas still lack the robust telecommunications framework needed to support high-speed connectivity. This shortfall makes the deployment of advanced technologies like Wi-Fi 7 difficult. Economic disparities also play a significant role, with the high costs of implementation and operation potentially restricting access in regions where disposable incomes are lower. Additionally, regulatory considerations impact the rollout, as the availability of the 6 GHz frequency band—crucial for Wi-Fi 7's performance—differs from country to country, depending on local spectrum policies and approvals. Finally, market awareness remains a key issue; without sufficient education on the benefits of Wi-Fi 7, both consumers and businesses may be hesitant to upgrade, leading to a slower rate of adoption across the region.

How does Omada's flexible management architecture cater to enterprise networking needs, and what sets it apart from competitors?
Omada's flexible management architecture is tailored to meet the varied networking needs of modern enterprises by offering a robust and intelligent approach to network administration. At the core of its solution is centralised cloud management, powered by a Software-Defined Networking (SDN) platform that seamlessly integrates access points, switches, and routers to ensure unified control over both wireless and wired connections. Omada also features zero-touch provisioning, enabling remote deployment and configuration without the need for on-site technical support—significantly simplifying setup and reducing operational costs. Additionally, the platform leverages AI-driven technology to analyse network performance, offer optimisation recommendations, and proactively resolve potential issues, thereby boosting network efficiency and ensuring consistent reliability.

TP-Link's Omada distinguishes itself in the competitive networking solutions market through a range of standout features tailored for flexibility, efficiency, and security. One of its key advantages is flexible management options—users can manage their networks without the need for a dedicated controller, choosing between hardware controllers, software controllers, or cloud-based management. This approach allows businesses to customise their setup according to their needs while avoiding unnecessary subscription costs. Omada's unified network architecture further simplifies operations by enabling centralised management of WAN, LAN, and wireless components through a single platform, enhancing overall efficiency.

Its comprehensive cloud-based management capabilities allow administrators to remotely monitor and configure networks using the Omada Cloud-Based Controller. Tools like batch configuration, multi-site management, and remote firmware updates streamline day-to-day network maintenance. Security and reliability are also at the forefront of Omada's offering—the system ensures that user traffic does not pass through the cloud, maintaining data privacy, while delivering 99.9% SLA availability, 24/7 automated fault detection, and backup servers in geographically isolated locations for added reliability. Finally, AI-driven network optimisation equips IT teams with proactive insights, such as automatic channel selection and power adjustment, helping reduce interference and significantly boosting wireless network performance.

With cybersecurity being a major concern, how does Omada ensure secure and scalable network management for businesses?
TP-Link's Omada platform is designed to provide businesses with secure and scalable network management, integrating advanced security measures, independent verification, and a forward-looking approach to continuous improvement. At the heart of this solution lies a comprehensive security framework, which is central to TP-Link's product strategy. Omada is built to anticipate, identify, and respond to risks effectively through internal penetration testing, real-world threat modelling, and adherence to industry standards like the OWASP IoT Top 10, ensuring resilience against ever-evolving cyber threats.

Security assurance is further reinforced through rigorous internal and external assessments. TP-Link collaborates with accredited third-party security labs to examine Omada products, ensuring any vulnerabilities are addressed proactively. Public security data shows that TP-Link maintains vulnerability rates that are equal to or lower than other industry leaders, underscoring its strong commitment to robust cybersecurity practices.

As a strong proponent of the secure-by-design philosophy, TP-Link actively supports global security initiatives, including the U.S. Cyber Trust Mark and the EU's Cyber Resilience Act. These frameworks guide Omada's development process, ensuring transparency through Software Bills of Materials (SBOMs) and alignment with top-tier industry standards.

Omada also prioritises proactive threat mitigation and transparency. Businesses receive timely firmware updates and critical security advisories, along with clear end-of-life policies to ensure continued support. The platform's cloud-based centralised management system further enhances protection by isolating management data from user traffic.

Engagement with the global cybersecurity community is another pillar of TP-Link's strategy. Through its vulnerability disclosure program and participation in initiatives like PWN2OWN, TP-Link ensures fast responses—typically within five working days—to any reported issues, continuously testing and improving Omada's defenses.

Omada's strength also lies in TP-Link's CI/CD development approach, which integrates security at every stage of the lifecycle. This enables early detection and resolution of potential vulnerabilities while ensuring scalability, high availability, and rapid response to threats. By embedding security into its core and staying closely aligned with industry best practices, TP-Link has positioned Omada as a reliable, future-ready solution for secure business network management.

What makes VIGI a standout surveillance solution, and how does it integrate with modern security ecosystems?

VIGI emerges as a powerful, AI-enhanced, and cost-effective surveillance solution designed to meet the evolving security needs of modern businesses. Its ease of deployment, scalability, and compatibility with current security ecosystems make it a future-ready choice for seamless and intelligent security management. With advanced features like AI-powered analytics, ONVIF support, Omada SDN integration, and industry-leading warranty services, VIGI offers a comprehensive and reliable approach to surveillance.

At the core of its capabilities are AI-powered analytics. VIGI cameras utilise advanced AI chips and deep-learning algorithms to monitor live footage in real time, detect unusual events, and send immediate alerts. This intelligent approach significantly reduces false alarms and enhances response times, improving overall security effectiveness. In addition, VIGI's ColorPro Night Vision technology ensures sharp, full-color images even in extremely low-light conditions, enabling round-the-clock surveillance with exceptional clarity.

VIGI also offers flexible management options through both standalone setups and centralised Video Management Systems (VMS). The VMS enables unified control over multiple devices, streamlining operations and providing user-friendly access across different sites. For broader compatibility, VIGI supports the ONVIF protocol, allowing integration with a wide range of third-party NVRs and VMS platforms, ensuring seamless interoperability in diverse security environments.

Moreover, VIGI is designed to integrate effortlessly with TP-Link's Omada Software-Defined Networking (SDN) ecosystem. This compatibility allows centralised monitoring of both surveillance and enterprise network infrastructure, with Power over Ethernet (PoE) support simplifying installation and connectivity. Businesses also benefit from the VIGI Cloud VMS, a cloud-hosted platform that offers centralised control via web portals, mobile apps, and PC clients—ideal for managing security across multiple locations.

By combining AI intelligence, superior night vision, versatile management tools, and strong integration capabilities, VIGI positions itself as a smart, scalable, and future-proof surveillance solution tailored for modern businesses.

What are TP-Link MEA FZE's key innovations and strategic plans for networking and surveillance solutions in 2025?

In 2025, TP-Link is set to transform connectivity and security with the full launch of its Wi-Fi 7 and MGIG solutions, catering to both home users and businesses, especially SMEs and large enterprises. These offerings promise ultra-fast speeds, reliable connectivity, and unified network performance across all user segments.

TP-Link is also integrating AI-driven technology across its product line to enhance network performance. These AI-enhanced systems will automatically optimise traffic, troubleshoot issues, and strengthen security, creating efficient, self-managing networks for homes and businesses alike.

On the surveillance front, TP-Link's VIGI portfolio introduces innovations like solar-powered, 5G-connected security devices, enabling flexible, sustainable installations without traditional wiring. A highlight is the InSight S345-4G device with three LAN ports for efficient multi-device connectivity.

Additionally, Omada Central offers centralised management of both networking and surveillance systems, simplifying operations for SMEs by enabling unified control across multiple sites. Together, VIGI and Omada Central deliver a powerful combination of intelligent security and seamless connectivity, making TP-Link a leader in next-generation networking and surveillance solutions.

What are TP-Link's strategic plans for expanding its presence in the Middle East and Africa (MEA) in 2025?
In 2025, TP-Link is focusing on expanding its footprint across the MEA region by strengthening partnerships with local distributors and increasing its presence in smaller cities and rural areas. This strategic effort aims to make high-performance, affordable networking solutions accessible to a broader audience, especially small and medium-sized businesses (SMBs), and support digital transformation in underserved regions.

How does TP-Link support its channel partners in keeping up with evolving technology?
TP-Link places a strong emphasis on partner empowerment through structured training and hands-on technical learning. Recognising the rapid pace of digital innovation, TP-Link ensures that distributors and channel partners are well-equipped with the latest knowledge and skills. By offering immersive training programs, TP-Link enables partners to confidently implement and support advanced solutions such as Wi-Fi 7 and VIGI surveillance systems, building trust and fostering long-term collaboration.

What role does sustainability play in TP-Link's 2025 strategy?
Sustainability is a key component of TP-Link's 2025 vision. The company is integrating energy-saving technologies into its product designs to reduce carbon footprints and improve energy efficiency. With increasing global awareness around environmental issues, TP-Link aims to lead the way in offering eco-friendly networking solutions suitable for both personal and professional use.

What steps is TP-Link taking to ensure the security of its networking and IoT products?
Security is a top strategic priority for TP-Link. The company employs rigorous internal and external testing—including penetration tests and threat modeling—to secure its devices. TP-Link demonstrates fewer vulnerabilities and faster resolution times compared to industry peers. It also supports global security initiatives like the EU Cyber Resilience Act, U.S. Cyber Trust Mark, and the "Secure by Design" pledge. Transparency is maintained through Software Bills of Materials (SBOMs) and regular firmware updates, and the CI/CD development model ensures rapid threat response and customer trust.

How does TP-Link engage with the broader security community?
TP-Link actively collaborates with the cybersecurity community through its vulnerability disclosure program and participation in security events such as PWN2OWN. These engagements help the company stay ahead of emerging threats, reinforce its security posture, and uphold its reputation as a trusted leader in networking and IoT security.

GENAI AT FOREFRONT OF CYBERSECURITY

WITH DIGITAL THREATS BECOMING MORE SOPHISTICATED, GENAI IS REVOLUTIONISING HOW ORGANISATIONS ARE BUILDING THEIR DIGITAL DEFENSES. IT IS NOW RESHAPING THE WAY ORGANISATIONS USE IT AS A POWERFUL TOOL TO DETECT, RESPOND AND PREDICT CYBERATTACKS, WRITES BASSEL KHACHFEH, DIGITAL SOLUTIONS MANAGER AT OMNIX INTERNATIONAL.

Bassel Khachfeh
Digital Solutions Manager at Omnix International

Cybersecurity is increasingly shifting from a reactive stance to a proactive focus on cyber intelligence, with AI playing a crucial role in driving this transformation. GenAI in particular, is paving the way for automated threat detection, enabling real-time anomaly monitoring and phishing email analysis. AI-powered SOC automation enhances efficiency by summarising security logs and facilitating rapid responses. It also helps in predicting and countering threats before they escalate, reducing detection and response time, minimising chances of human error.

GenAI is advancing rapidly in cybersecurity, and certain industries face heightened security demands because of the sheer volume of data they handle. The adoption and application of these new tools work specifically well for the financial services sector to detect fraudulent transactions in real time. In healthcare it tightens the security around sensitive patient data, while in energy and utilities it helps to monitor critical infrastructure for cyber-attacks and in telecommunications it helps to detect network breaches across distributed systems.

In the Middle East, sectors like oil and

gas, banking, and government services are actively investing in GenAI to strengthen national cybersecurity infrastructure. The UAE has AI-driven security initiatives, while Saudi Arabia integrates AI into its Vision 2030 cybersecurity goals.

Globally, firms like Microsoft and Google use GenAI to detect threats in seconds, and the EU AI Act promotes responsible adoption. However, with increased use of GenAI, comes a greater risk of and responsibility to tackle its higher usage by cyber criminals to develop more sophisticated attacks.

The attacks include automated malware bypassing security filters, AI-generated phishing mimicking trusted contacts, and possible data poisoning corrupting AI models. These risks highlight the need for continual testing, model monitoring and stricter AI governance policies.

While AI has been at the forefront of cybersecurity, with it comes the challenge of addressing ethics and privacy concerns, especially in sensitive areas such as healthcare, finance, oil & gas, etc. On the other hand, lack of transparency makes it difficult to understand decisions generated by AI. However, these can be tackled by implementing strict governance policies, greater transparency that have explainable AI models as well as having diverse and inclusive datasets.

What also helps is being increasingly aware of and following global data privacy laws such as GDPR in Europe or the DIFC Data Protection Law in the Middle East. It helps build trust and compliance.

Simultaneously it is also important for organisations to have Human-In-The-Loop (HITL) systems to ensure that AI decisions are accurate and it remains a key focus within AI implementations, particularly in mission critical environments.

It is evident that large enterprises are the highest users of GenAI, but small businesses can also benefit from it by having cloud-based security platforms, open-source threat intelligence tools and using managed AI-driven security service. This helps in strengthening their security posture cost effectively.

To successfully integrate GenAI into cybersecurity workflows, organisations should adopt best practices that include:

- Having an AI security framework that follows industry standards
- Implement model explainability and accountability
- Use strong testing to identify model vulnerabilities
- Stress on human validation for critical threat decisions
- Continuously train models with current threat data

Looking into the future, GenAI will move toward more autonomous context-aware security solutions. Collaborative AI learning will allow AI models to learn across distributed environments without compromising data privacy. AI-powered digital forensics will speed up incident analysis. AI-driven SOCs will redefine the speed and scale of threat response. However, the future will also see the growing use of defensive AI that will help in threat detection and prevention, incident response, vulnerability management, and other aspects such as fraud detection, user behaviour analytics and adaptive authentication.

It is important for organisations to remain agile and continuously adapt, but also to invest in both technology and skilled personnel to remain resilient.

GenAI today is actively shaping cybersecurity. From threat prediction to attack prevention, it offers unparalleled advantages. To realise its full potential calls for ethical deployment, collaboration across industries, investment in skilled personnel, and strong governance. A thoughtful balance between innovation and oversight, GenAI will be capable to secure as well as redefine the digital future.

DORA'S DEMANDS ON FINANCIAL SERVICES - AND HOW TO RISE TO THEM

Few industries are under the same level of regulatory scrutiny as financial services. New frameworks are introduced all the time, and for good reason: the sector underpins national infrastructure and is a prime target for cyberattacks and fraud. In other words, regulation has to be watertight.

The EU's Digital Operational Resilience Act (DORA) is the latest in a long list of measures designed to raise the bar on how financial institutions and their third-party providers prepare for, withstand, and recover from disruption. Introduced in January, it focuses on incident reporting, third-party oversight and resilience testing. But six months on, nearly all financial services organisations surveyed (96%) acknowledge they still need to strengthen their resilience to meet the regulation's requirements.

So what's slowing things down? And what will actually help firms move forward?

Easing the strain on teams
One of the biggest side effects of DORA so far has been the extra load it puts on IT and security teams - 41% of organisations surveyed cited it as a significant challenge when meeting DORA requirements. Given that the cybersecurity sector is already a high-pressure industry, it's no surprise that burnout is an ongoing problem. However, meeting DORA requirements does not should not contribute to this problem so much.

The answer isn't to add DORA as just another project to complete on an already crowded list. Instead, firms need to treat resilience more holistically. Using data resilience maturity models

(DRMMs) allows DORA compliance to be part of a bigger resilience plan, rather than an isolated exercise. This approach not only takes pressure off teams but also improves businesses' data resilience as a whole.

"Testing, testing…"

Another sticking point in meeting compliance requirements is the challenges around testing. Nearly a quarter of EMEA firms still don't have recovery and continuity testing in place, and almost as many haven't started resilience testing at all. That's risky.

Without regular testing, there's no way to know whether new controls will actually work when they're needed. Running that first test can feel daunting - believe me, I know. No one wants to uncover problems that might be a pain to fix. But in reality, testing is one of the best ways to make progress. It's a clear DORA requirement, but more importantly, it builds confidence that systems will hold up in the face of a real cyber incident.

Andre Troskie
EMEA Field CISO, Veeam.

Rethinking third-party relationships

Finally, the last major hurdle to DORA compliance is third-party oversight - over a third of organisations call it the "most challenging to implement", and a fifth haven't addressed it at all.

The main issue? Most firms underestimated just how many external providers they rely on. The average enterprise has 88 third-party partners, which is far more than most resilience strategies account for, and a massive number of connections to keep up with. In the past, financial firms often assumed these providers had resilience built in, but DORA demands more: clear responsibility models and transparent SLAs that spell out exactly who is accountable for what.

That means renegotiating contracts and bringing together security, risk, legal and management teams to get it done. It's not a small task, but it's a necessary one if organisations want genuine confidence in their resilience.

Looking ahead

The compliance issues around DORA won't be resolved overnight. After all, building resilience takes time, and there will inevitably be bumps in the road. But firms that approach DORA as part of a broader resilience journey, rather than a standalone compliance project, will ultimately come out stronger because of it.

The best place to start is with some honest questions: Where are my company's weak spots? Do we really know how resilient our suppliers are? And are we testing enough to trust our defences? The answers may be uncomfortable in the short term, but they're the foundation of long-term confidence in data resilience - for DORA and well beyond.

> GIVEN THAT THE CYBERSECURITY SECTOR IS ALREADY A HIGH-PRESSURE INDUSTRY, IT'S NO SURPRISE THAT BURNOUT IS AN ONGOING PROBLEM. HOWEVER, MEETING DORA REQUIREMENTS DOES NOT SHOULD NOT CONTRIBUTE TO THIS PROBLEM SO MUCH.

THE RISING CHALLENGE OF ZERO-DAY VULNERABILITIES IN CYBERSECURITY

Ezzeldin Hussein
Regional Senior Director, Solution Engineering, META, SentinelOne

In the current digitally advancing world, the war between cyber-criminals and defenders gets stronger and fiercer. Today's enterprises commonly use cloud, on-premise apps, hybrid tools for collaboration purposes, and interconnected networks and technologies. Though this interconnectedness helps with making operations more flexible, it can also lead to the exploitation of zero-day vulnerabilities. A recent serious zero-day vulnerability affecting SharePoint on-premise systems, known in industry circles as "ToolShell" (CVE-2025-53770), reminds us of the uncertain and ever-evolving nature of the threat landscape. The vulnerability allowed the execution of a remote code that was unauthenticated, prior to a formal patch being issued. This is a typical model of the extent of innovation attackers are capable of and why organisations need to reassess how well they are equipped to face cyber risk, especially with regard to unidentified and unpatched risks.

Sero-Day Vulnerabilities as the New Normal

Zero-days remain invisible, unless they are discovered. They refer to vulnerabilities in software or systems that cyber attackers might have already seen and employed for attacking, but the security experts are unaware of. This opens a very risky window for threat actors. In ToolShell's case, attackers remotely ran arbitrary code. This would have given them access to the systems that are compromised. Though a major case, this is not rare. These zero-day vulnerabilities have become increasingly common, and attacks have come in different forms. They now target frameworks, email servers, collaborative platforms and security products.

The question now is how can enterprises stay alert and be well-prepared for these invisible threats?

Building Cyber Resilience: From Reactive to Proactive

Effective cybersecurity in the face of zero-day threats requires a multi-layered and forward-looking strategy. Here are five key focus areas every organisation should adopt:

1. Assume Breach & Minimise Blast Radius

The first shift in mindset must be this: assume a breach is inevitable. This isn't pessimism, it's realism. By adopting an "assume breach" posture, companies can invest in segmentation, access controls, and identity protections that limit how far an attacker can move once inside. Privileged access should be limited, lateral movement should be monitored, and sensitive data must be isolated.

2. Adopt Extended Detection & Response (XDR)

Detection is no longer enough; organisations need tools that correlate behavior across endpoints, identities, cloud workloads, and networks. XDR platforms provide that visibility, enabling faster detection of anomalies and coordinated response across environments. When a zero-day is exploited, the ability to see the full kill chain and isolate affected systems becomes mission-critical.

3. Invest in Threat Intelligence & Real-Time Updates

Staying ahead means being informed. Enterprises should subscribe to threat intelligence feeds and work with cybersecurity partners who offer real-time updates, including Indicators of Compromise (IOCs) and hunting queries, even before public advisories are issued. Early detection and context-rich threat intel can dramatically reduce dwell time and response lag.

4. Integrate Vulnerability Management with Active Monitoring

Traditional vulnerability management often runs on a monthly cadence, too slow for today's environment. Modern organisations need continuous vulnerability exposure assessments that integrate with their detection tools. If a system is found to be vulnerable, real-time flags should trigger proactive isolation or prioritisation in patch pipelines.

5. Foster Cross-Team Collaboration and Executive Visibility

Cyber risk is a business risk. IT, security, and executive leadership must collaborate closely to ensure that the organisation's risk tolerance, response protocols, and communication plans are well understood and exercised. Business continuity planning should include simulations for zero-day incidents — not just ransomware or known malware.

From Defense to Anticipation

While patching known vulnerabilities remains essential, organisations can no longer rely solely on post-exploit remediation. The key lies in anticipating threats through behavioral analysis, automated response, and architectural resilience. Emerging technologies, including AI-powered security platforms, are helping analysts detect suspicious patterns even without a known signature. This level of proactive defense is increasingly becoming the gold standard. It's also critical to eliminate blind spots. Tools should be able to detect unexpected process executions, unusual SharePoint or IIS behaviors, and anomalous command-line arguments, signs that something like ToolShell may be at play.

Conclusion: Staying One Step Ahead

Zero-days will continue to surface. Some may grab headlines; many will fly under the radar. But the organisations that thrive in this reality are those that don't wait for the news to act. They invest in proactive visibility, rapid containment, and flexible response strategies.

The ToolShell vulnerability may fade from news cycles in weeks, but the lesson it carries must remain: in cybersecurity, speed and preparedness make all the difference. The winners are those who treat sero-day defense not as a one-time effort, but as a core capability woven into the fabric of their technology, their processes, and their culture.

About the Author: Ezzeldin Hussein is Senior Director, Solutions Engineer at SentinelOne, a global leader in AI-powered cybersecurity.

Bashar Bashaireh
AVP Middle East, Türkiye & North Africa at Cloudflare

THE FUTURE UNFOLDING: AI, CYBERSECURITY, AND NEW DIGITAL INFRASTRUCTURE

The digital landscape is undergoing a rapid transformation, driven by several converging factors: the swift advancements in artificial intelligence (AI), growing infrastructure needs, the escalating challenges of cybersecurity, the shifting regulatory landscape, and fundamental changes in how we connect and collaborate. Together, these elements are shaping the future of the internet, creating a complex, interconnected ecosystem where each trend influences and amplifies the others. As a result, we must rethink our approaches to infrastructure, security, and the role of technology in our lives.

The AI Revolution: The Future Is Now (But Unevenly Distributed)

AI, once merely a buzzword, is now at the core of many technological advancements. A recent McKinsey survey on AI reveals that 65% of organizations use generative AI regularly, and 72% have integrated AI into at least one business function. AI's impact is becoming as transformative as the advent of electricity in the early 20th century, which reshaped entire industries and economies. Similarly, AI is now embedded in various workflows, enhancing productivity and fostering new forms of creativity.

AI-powered coding assistants are streamlining software development, generative AI tools are enhancing content creation, and advanced AI models are assisting healthcare providers with early disease detection. These real-time breakthroughs are revolutionizing industries, making AI an invisible but indispensable part of our daily lives.

However, with such advancements come significant responsibilities. Concerns around algorithmic bias, data privacy, and intellectual property have moved from hypothetical to urgent. As AI systems become increasingly integrated into everyday life, society faces the challenge of balancing innovation with accountability. This balance is crucial for both engineers and policymakers and is vital for all who rely on digital services.

Infrastructure Evolution: The Edge Gets Sharper

While AI might dominate the headlines, profound changes are also taking place in the foundational layers of our digital world. Edge computing, once a nascent concept, is now rapidly evolving into a more sophisticated model that fundamentally alters how we conceive of infrastructure.

To understand this, imagine the internet as a sprawling city. In the past, most computing tasks were handled in large, centralized data centres. Now, edge computing is like setting up satellite offices across the city's suburbs, bringing processing power closer to the areas that need it. This localized model reduces latency, enabling real-time analytics, autonomous vehicles capable of split-second decision-making, and gaming without lag. Beyond speed, when AI is integrated into this distributed framework, it opens up entirely new classes of applications.

However, these advantages come with their own challenges. The demand for GPU capacity to support AI workloads has skyrocketed, often outstripping supply. As a result, infrastructure providers must rethink chip designs, explore new architectures, and invest in sustainable energy solutions. The future data centre will likely be a global network of micro-facilities, carefully coordinated to balance performance, sustainability, and security.

The growth of edge computing highlights the need for neutrality, flexibility, and a distributed approach to computing and storage. By directing workloads to regions abundant in resources and clean energy, we can create an economically viable and environmentally responsible digital ecosystem. The edge is not just becoming more powerful but smarter, more efficient, and more adaptive to the demands of an increasingly connected world.

Cybersecurity: New Challenges Amid a Changing Landscape

Cybersecurity remains a paramount concern for businesses and IT leaders. According to Cloudflare's Shielding the Future: Middle East & Türkiye Cyber Threat Landscape Report 2024, 42% of regional business and IT leaders expect cybersecurity to make up at least 20% of their organizations' IT spend over the year ahead. Of those expecting a budgetary increase, 91% anticipate a rise of more than 10%.

While this is good, cybersecurity now faces a range of transformative forces, including the democratization of AI, the adoption of zero-trust security models, and the rise of quantum computing.

AI is a double-edged sword in cybersecurity. On the one hand, AI enhances threat detection and automates defense systems. IBM's 2024 Cost of a Data Breach Report highlights that AI-driven tools can reduce breach costs by nearly half. On the other hand, cyber attackers are leveraging AI to create more adaptive and sophisticated threats. This has led to the shift away from static defenses towards more agile, continuously updated security models.

AI's role in cyberattacks is also a growing concern. Hackers are using AI to launch automated, adaptive malware attacks that exploit vulnerabilities on an unprecedented scale. There is an urgent need to leverage AI for defense and bolster cybersecurity measures.

The rise of quantum computing adds an additional layer of urgency. Quantum computing's emerging capabilities could eventually compromise current encryption methods, necessitating a move towards quantum-safe cryptography. Recent breakthroughs in quantum chip technology, like Google's advances, make it clear that quantum-scale challenges are imminent. Preparing for this shift by adopting crypto-resilience is no longer a matter of choice but a pressing priority.

Connectivity: The Next Frontier Is Above Us

For all the innovations in AI, edge computing, and cybersecurity, one fundamental element underpins them all: connectivity. As the digital world evolves, ensuring robust, universal connectivity is crucial. Over the next few years, new approaches like satellite-based networks will significantly expand global internet access. Projects such as SpaceX's Starlink aim to connect even the most remote regions, while the rollout of 5G and the future development of 6G will dramatically enhance network performance and alter the way we architect communication systems.

However, connectivity isn't just about increasing speed. As the Internet of Things (IoT) and machine-to-machine interactions become more prevalent, networks must be capable of handling massive volumes of data, from autonomous drones delivering medical supplies to sensors monitoring agricultural fields. The challenge will be ensuring that these networks are secure, reliable, and scalable, meeting the demands of a connected world.

The Human Element: A Workforce in Transition

At the heart of these technological transformations lies the human element. As the digital landscape evolves, so too does the demand for new skills. The digital skills gap is rapidly widening, and as AI, cybersecurity, and other technologies become more integrated into daily life, coding literacy, cybersecurity awareness, and AI fluency are becoming essential competencies for the 21st century workforce. The World Economic Forum forecasts that 23% of global jobs will change due to technological advancements like AI and automation.

The rise of remote collaboration platforms is another significant shift. Initially a response to the pandemic, remote work is now a permanent fixture. Today's platforms go beyond basic tools like email and video calls, integrating AI-driven features such as real-time language translation and meeting transcription. These innovations create opportunities for more inclusive workplaces and communities, but they also present challenges in terms of ensuring technology meets diverse human needs.

Conclusion: Navigating the Digital Horizon

The technological shifts we are witnessing are interdependent, with AI, edge computing, cybersecurity, connectivity, and human resources all influencing one another. Companies will need to take a holistic approach to navigate this complex landscape, choosing partners who can scale operations, maintain security, and adapt to evolving regulations.

As we stand at this critical juncture, the choices made in the coming years will determine whether we harness these technologies to solve global challenges or become overwhelmed by their complexity. The digital horizon is rich with opportunities. By fostering responsible stewardship, thoughtful regulation, and collaboration between enterprises, governments, and citizens, we can ensure that the digital ecosystem remains resilient and trustworthy. The true measure of success will not be the number of new technologies we adopt but how effectively we integrate them into the fabric of society to meet the needs of a rapidly changing world.

planview®

PLANVIEW MIDDLE EAST LAUNCH

ACCELERATING INNOVATION
SHAPING THE FUTURE OF BUSINESS

Strategy to Execution
Driving Transformation Success

TUESDAY 07th October 2025	Raffles The Palm, Dubai	5:30 PM to 9:30 PM

Planview, a global leader in Strategic Portfolio Management (SPM) and Digital Product Development (DPD), is making a bold entry into the Middle East with the launch of its dedicated regional entity. Backed by significant investments in cloud infrastructure, this landmark event highlights Planview's commitment to empowering enterprises with the tools and insights needed to drive strategy, innovation, and business transformation.

Taking place on **7th October 2025** at **Raffles The Palm, Dubai**, the launch will bring together senior leaders, technology experts, and innovators from across industries. With keynote addresses, panel discussions, and customer success stories, the event will explore how organisations can bridge strategy to execution and unlock measurable impact in a rapidly evolving digital economy.

OFFICIAL PUBLICATIONS

cnme computer news middle east

Reseller MIDDLE EAST THE VOICE OF THE CHANNEL

Security ADVISOR MIDDLE EAST

HOSTED BY

tahawultech.com

For more information on the event, please visit the event website:
https://tahawultech.com/planview-middle-east-gala

#Planview | #tahawultech

SMARTPHONE CYBERATTACKS SURGE BY NEARLY A THIRD IN EARLY 2025, KASPERSKY REPORTS

LATEST RESEARCH HIGHLIGHTS SHARP RISE IN ANDROID MALWARE, BANKING TROJANS AND PRE-INSTALLED THREATS, WITH ATTACKERS EXPLOITING FAKE APPS AND SIDELOADING PRACTICES.

Kaspersky has reported a significant escalation in smartphone-targeted cyberattacks during the first half of 2025, with Android users experiencing a 29 per cent increase in malicious activity compared with the same period in 2024. The number of attacks was also 48 per cent higher than the second half of last year, highlighting an accelerating trend in mobile-focused cybercrime.

The security company identified several prominent mobile threats this year, including SparkCat, SparkKitty and Triada. However, the attack landscape has expanded further, with adversaries distributing malicious applications disguised as adult content or VPN services to compromise users' devices and credentials.

> **ATTACKERS WILL LIKELY FIND WAYS TO BYPASS VERIFICATION, UNDERSCORING THE NEED FOR USERS TO COMBINE ROBUST SECURITY SOLUTIONS, CAUTIOUS APP SOURCING AND REGULAR OS UPDATES.**
> **ANTON KIVVA, KASPERSKY**

New attack vectors emerge

In the second quarter of 2025, Kaspersky uncovered applications designed for adult content that were weaponised with functionality enabling dynamically configured distributed denial-of-service (DDoS) attacks. Once installed, the trojanised apps transmitted specific data from the victim's device to attacker-controlled servers at predefined intervals, making them part of coordinated botnet campaigns.

Similarly, a counterfeit VPN client was identified intercepting one-time passwords (OTPs) from various messaging platforms and social media accounts. By monitoring device notifications, the malware exfiltrated authentication codes and forwarded them to threat actors via a Telegram bot, effectively granting attackers access to compromised accounts.

Prevalence of malicious applications

Among the most widespread threats were Fakemoney scam applications, banking trojans and pre-installed malware. Fakemoney apps entice victims with false promises of earning rewards through games, investments or tasks, but ultimately steal personal data, financial information or deliver no payouts.

Pre-installed trojans such as Triada and Dwphon were also prevalent. Embedded into the firmware during the manufacturing process, these threats enable persistent data theft and unauthorised actions, remaining active even after devices are reset to factory settings.

Banking trojans multiply

Banking trojans represented one of the fastest-growing mobile threats in 2025. Kaspersky recorded nearly four times as many detections in the first half of 2025 compared with the same period in 2024, and more than double compared with the latter half of last year. These malicious applications target financial information, enabling attackers to steal funds directly from victims' accounts.

Industry perspective

Anton Kivva, Malware Analyst Team Lead at Kaspersky, said, "The first half of 2025 saw a surge in Android malware attacks compared to 2024. There are different attack vectors, and sideloading apps from outside app stores is one of them. Google's recent initiative to verify developers even for sideloaded apps is an attempt to counter malware spread via APK files outside official app stores. However, this step is not a silver bullet. Malware continues to infiltrate even the Google Play Store, where developer verification has long been in effect. Malware infiltrates Apple's App Store as well."

Kivva added that attackers are likely to continue circumventing verification mechanisms, reinforcing the importance of layered defences and user vigilance.

Recommendations for mobile users

To reduce exposure to mobile threats, Kaspersky advises:

- Downloading apps only from official stores such as the Apple App Store and Google Play, while remaining aware that these platforms are not immune to compromise.
- Reviewing app permissions carefully, particularly high-risk ones such as Accessibility Services.
- Checking app reviews and only using links from verified developer websites.
- Installing reliable security software, such as Kaspersky Premium, to detect and block malicious activity.
- Regularly updating operating systems and key applications to patch known vulnerabilities.

With mobile devices increasingly central to both professional and personal digital lives, the sharp rise in smartphone-targeted malware underlines the urgency for enterprises and individuals to enhance their mobile security posture.

Would you like me to also condense this into LinkedIn and X social media posts optimised for engagement with cybersecurity professionals?

TENABLE RESEARCH FINDS CLOUD AND AI GROWTH OUTPACING SECURITY STRATEGIES

HYBRID, MULTI-CLOUD AND AI ADOPTION DRIVE COMPLEXITY, BLIND SPOTS, AND HEIGHTENED RISK ACROSS ENTERPRISE ENVIRONMENTS.

Tenable, the exposure management company, has published its State of Cloud and AI Security 2025 report, which reveals that the rapid expansion of hybrid, multi-cloud and AI-driven systems is outpacing enterprise security strategies, creating blind spots and new layers of risk.

The research shows that 82 per cent of organisations now operate hybrid infrastructures spanning on-premises and cloud, while 63 per cent rely on multiple cloud providers, managing an average of 2.7 environments. Each platform introduces its own policies, tools and shared responsibility models, creating a fragmented security landscape. This sprawl results in disjointed visibility, inconsistent identity governance, and gaps in monitoring – weaknesses that attackers are quick to exploit.

Identity has emerged as one of the biggest challenges, with excessive permissions and weak governance regularly cited as root causes of cloud breaches. As AI workloads increase, they add another layer of complexity, amplifying these risks. In response, some organisations are even moving workloads back on-premises to regain greater control.

While many enterprises are investing in technologies such as unified security monitoring (58 per cent), Cloud Security Posture Management (57 per cent), and Extended Detection and Response (54 per cent), the report highlights that few have achieved unified risk oversight across hybrid and multi-cloud environments. Many of these tools still operate in silos, limiting their effectiveness and leaving significant exposure gaps.

Tenable's State of Cloud and AI Security 2025 highlights how fragmented IT environments and inconsistent identity governance are undermining cyber resilience.

The State of Cloud and AI Security 2025 survey, conducted by the Cloud Security Alliance on behalf of Tenable, polled over 1,000 IT and security professionals worldwide. The findings underline a critical need for more adaptive, integrated defences capable of keeping pace with the rapid evolution of cloud and AI infrastructure.

"The report confirms what we're seeing every day in the field," said Liat Hayun, VP of Product and Research at Tenable. "AI workloads are reshaping cloud environments, introducing new risks that traditional tools weren't built to handle."

Jim Reavis, Co-founder and CEO of the Cloud Security Alliance, echoed this concern: "We're in the middle of the fastest evolution in cloud computing history. Unfortunately, as our research made clear, many security strategies are already behind the curve. The risks of standing still are growing by the day. Organisations need to rethink their approach and build adaptive, future-ready defences that can evolve as quickly as the technologies they safeguard."

To address these challenges, Tenable Cloud Security provides unified visibility and risk management across IT, hybrid and multi-cloud ecosystems. It focuses on identity, misconfigurations and access governance, while enabling teams to integrate AI-specific exposures into their strategies. This allows security teams to transition from reactive incident response to proactive exposure management.

FUTURE PLANET STAGE
10 X MAIN STAGE
10X STAGE

EDUCATION SECTOR STRENGTHENS AGAINST RANSOMWARE BUT IT TEAMS FACE HEAVY TOLL

SOPHOS' LATEST STATE OF RANSOMWARE IN EDUCATION REPORT HIGHLIGHTS IMPROVED RECOVERY RATES AND REDUCED RANSOM PAYMENTS, BUT REVEALS MOUNTING STRESS AND BURNOUT AMONG CYBERSECURITY STAFF.

Sophos' 2025 State of Ransomware in Education report finds schools and universities are recovering faster from ransomware but warns of the human cost for IT teams.

Sophos has released its fifth annual State of Ransomware in Education report, showing that schools and universities are making measurable progress against ransomware. The study of 441 IT and cybersecurity leaders worldwide highlights falling ransom payments, reduced recovery costs, and faster data restoration. Yet, these gains come at a significant human cost, with IT staff reporting widespread stress, burnout, and career disruption. Almost 40 per cent of respondents admitted to suffering anxiety after attacks.

Over the past five years, ransomware has evolved into one of the most pressing threats to education. Primary and secondary schools in particular have been viewed as vulnerable targets, often underfunded and lacking skilled cybersecurity resources, yet responsible for safeguarding sensitive data. The consequences of attacks extend beyond financial losses, disrupting learning, eroding trust, and exposing students and staff to privacy risks.

Stronger resilience and reduced costs

Sophos' research points to notable progress. Primary and secondary institutions successfully blocked 67 per cent of ransomware attempts before encryption, the highest success rate recorded in four years. Universities prevented 38 per cent. At the same time, ransom demands fell sharply, down 73 per cent over the past year. In lower education, average payments dropped from US$6 million to US$800,000, while in higher education they declined from US$4 million to US$463,000. Recovery costs outside of ransom payments also dropped significantly – by 77 per cent in higher education and 39 per cent in lower education. Of those organisations whose data was encrypted, 97 per cent managed to restore access.

> **WHILE IT'S ENCOURAGING TO SEE SCHOOLS STRENGTHENING THEIR ABILITY TO RESPOND, THE REAL PRIORITY MUST BE PREVENTING THESE ATTACKS IN THE FIRST PLACE.**
> **ALEXANDRA ROSE, SOPHO**

Ongoing vulnerabilities and rising human impact

Despite these improvements, the report underscores serious gaps. Two-thirds of respondents cited ineffective or missing security tools, a shortage of skilled staff, and unaddressed vulnerabilities. AI-enabled threats are compounding these risks, with nearly a quarter of ransomware incidents in lower education originating from phishing campaigns. As adversaries experiment with deepfakes and synthetic voice scams, schools are increasingly exposed to emerging attack methods.

Higher education institutions, often home to valuable AI research and large language model datasets, remain a high-value target. Sophos found that exploited vulnerabilities (35 per cent) and previously unknown security gaps (45 per cent) were among the most common entry points for attackers. Beyond the technical impact, every institution that experienced encrypted data reported consequences for IT teams. More than one in four staff members took leave following an incident, 40 per cent reported stress and anxiety, and over one-third felt personal guilt for failing to prevent breaches.

Building long-term resilience

"Ransomware attacks in education don't just disrupt classrooms, they disrupt communities of students, families, and educators," said Alexandra Rose, Director, CTU Threat Research at Sophos. "While it's encouraging to see schools strengthening their ability to respond, the real priority must be preventing these attacks in the first place. That requires strong planning and close collaboration with trusted partners, especially as adversaries adopt new tactics, including AI-driven threats."

Sophos recommends several measures to help schools maintain progress and adapt to evolving threats. Prevention should remain the top priority, ensuring attacks are blocked before they can cause damage. Institutions should also seek funding opportunities such as the US FCC's E-Rate subsidies and the UK NCSC's free cyber defence service for schools. A unified security approach across complex IT environments will help eliminate blind spots, while partnerships with managed detection and response providers can reduce pressure on stretched IT teams. Robust incident response plans and regular simulation exercises remain essential for ensuring rapid recovery when attacks succeed.

The State of Ransomware in Education 2025 report draws on survey responses from 243 lower education and 198 higher education institutions across 17 countries, all of which experienced ransomware in the past year. Conducted between January and March 2025, the research covers organisations ranging from 100 to 5,000 employees and provides one of the most detailed views yet of the shifting ransomware landscape in global education.

NEW STUDY REVEALS INSIDER THREATS AND AI COMPLEXITIES ARE DRIVING FILE SECURITY RISKS TO RECORD HIGHS, COSTING COMPANIES MILLIONS

WITH 61% OF ENTERPRISES HIT BY INSIDER BREACHES, RESEARCH SPONSORED BY OPSWAT HIGHLIGHTS UNIFIED, MULTI-LAYERED PLATFORMS AS THE FUTURE OF RESILIENT DEFENSE

A new study sponsored by OPSWAT, a global leader in critical infrastructure protection, reveals that organisations face escalating risks from insider activity, legacy tools, and the growing complexity of artificial intelligence (AI). Independently conducted by Ponemon Institute, the report found that in the past two years, 61% of organisations have suffered file-related breaches caused by negligent or malicious insiders, at an average cost of $2.7 million per incident.

The research underscores that insiders represent the single biggest risk to file security. Forty-five percent of respondents cited negligent or malicious insiders leaking data as the most serious threat, far surpassing external actors. Alarmingly, only 40 percent of organisations say they can detect and respond to file-based threats within a day (25 percent) or within a week (15 percent).

The report also shed light on the

role of AI in file protection, highlighting that adversaries are now exploiting generative AI models, e.g. embedding prompts in macros or exposing hidden data through AI parsers. To combat these threats, many enterprises are themselves turning to AI for faster detection and cost savings. Currently, 33 percent of organisations have integrated AI into their file security strategies, and an additional 29 percent plan to do so by 2026. To safeguard sensitive corporate files in AI-driven workflows, organisations primarily deploy prompt security tools (41 percent) and masking techniques to protect confidential data (38 percent). Despite these efforts, governance remains inconsistent, with only 25 percent of organisations having a formal Generative AI (GenAI) policy in place, while 29 percent have banned GenAI altogether.

Such gaps leave organisations with poor confidence in their ability to protect files at critical points such as uploads, transfers, and third-party sharing. The findings indicate that files are most vulnerable at critical exchange points. Only 39 percent of respondents express confidence that files remain secure when transferring them to and from third parties, while just 42 percent feel confident during file uploads. The environments posing the greatest risk include file storage systems such as on-premises, NAS, and SharePoint (42 percent), followed closely by web file uploads via public portals and web forms (40 percent).

"As threats continue to accelerate and increase in cost, cyber resilience has shifted from being a technical priority to being a strategic, fiscal imperative," said Dr. Larry Ponemon, Founder of the Ponemon Institute. "Executives must take ownership by investing in technology that reduces risk and cost while enabling organisations to keep pace with an ever-evolving AI landscape."

The findings further reveal a sharp shift away from legacy point solutions toward unified, multi-layered platforms that incorporate technologies such as multiscanning, Content Disarm & Reconstruction (CDR), and adaptive sandboxing. By 2026, two-thirds of enterprises expect to be using these advanced technologies.

"A multi-layered defense that combines sero-trust file handling with advanced prevention tools is no longer optional but is the standard for organisations looking to build resilient, scalable security in the AI era," added George Prichici, VP of Products at OPSWAT. "Leveraging a unified platform approach allows file security architectures to adapt to new threats and defend modern workflows and complex file ecosystems inside and outside the perimeter."

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. The company's mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

IDENTITY SECURITY BECOMES STRATEGIC IMPERATIVE AS AI-DRIVEN THREATS INTENSIFY

CISCO'S 2025 STATE OF IDENTITY SECURITY REPORT REVEALS THAT 85% OF ORGANISATIONS ARE ADOPTING SECURITY-FIRST IDENTITY PRACTICES TO COUNTER RISING THREATS AND GROWING COMPLEXITY.

Fady Younes, Cisco's Managing Director for Cybersecurity in MEA, Türkiye, Romania and CIS, emphasises identity as the new frontline of cybersecurity.

Cisco has released its 2025 State of Identity Security report, which examines the challenges and strategies IT and security leaders are adopting to navigate an increasingly complex threat landscape. Drawing insights from 650 executives worldwide, the study reveals that 85% of organisations are now taking a security-first approach to identity in response to AI-driven threats.

In the UAE, this focus aligns with the country's ambitions to lead in digital transformation. Initiatives such as the National Cybersecurity Strategy reinforce the principle that technological progress must be underpinned by strong cybersecurity foundations, safeguarding identities, systems, and data as the nation advances towards a digital-first economy.

Fady Younes, Managing Director for Cybersecurity at Cisco Middle East, Africa, Türkiye, Romania and CIS, commented:

"Identity has become the new frontline of cybersecurity. As AI-powered threats accelerate, organisations can no longer rely on fragmented tools and outdated practices. A security-first identity strategy is now essential to protect data, build trust, and enable innovation in an increasingly digital world. At Cisco, we are addressing this challenge head-on through innovations in zero trust, passwordless authentication, and identity threat detection to help organisations strengthen their defences with speed and confidence."

Facing complexity and a confidence crisis

Despite the recognition of its importance, identity security remains fraught with challenges. Only one-third (33%) of leaders are confident that their current identity provider can prevent attacks, reflecting the risks posed by complex infrastructures and poor visibility into vulnerabilities.

The study found that 94% of leaders believe identity infrastructure complexity undermines security, while 75% lack a clear understanding of identity-related risks. More than half (51%) of organisations have experienced financial losses due to breaches, prompting 82% of financial decision-makers to increase their investment in identity security in 2025.

AI as both threat and catalyst

Artificial intelligence represents both risk and opportunity. AI-powered phishing, cited by 44% of leaders, stands out as a top threat for 2025, alongside insider attacks and supply chain compromises. At the same time, organisations are leveraging AI for defensive purposes, harnessing its data-processing capabilities to identify and mitigate vulnerabilities at scale.

Persistent phishing threats and MFA gaps

Phishing continues to be a major concern. While 87% of leaders consider phishing-resistant multi-factor authentication (MFA) a critical element of security strategy, only 30% express high confidence in their phishing defences. Weak or absent MFA (36%), coverage gaps (34%), and failures of one-time passcodes (29%) remain key drivers of breaches.

A call for security-first IAM

The study also highlights that identity is frequently overlooked during initial infrastructure planning, with 74% of IT leaders admitting to a reactive approach that increases costs and reduces visibility. To counter this, 79% of organisations are exploring vendor consolidation as a means to simplify identity and access management (IAM) and enhance oversight.

Nevertheless, only 52% of organisations have fully integrated identity and device telemetry, limiting real-time visibility. Contractor and third-party access controls remain weak points, with 86% reporting gaps. While 87% of leaders recognise the importance of identity threat detection and response, only 32% have implemented Identity Security Posture Management (ISPM) solutions.

The 2025 State of Identity Security report makes clear that organisations must prioritise robust, security-first identity practices to manage the growing complexity of threats. Addressing the current gaps in confidence, execution and infrastructure will be critical for enterprises seeking not only to protect against AI-driven attacks, but also to build digital trust and support innovation.

> **IDENTITY HAS BECOME THE NEW FRONTLINE OF CYBERSECURITY. A SECURITY-FIRST IDENTITY STRATEGY IS NOW ESSENTIAL TO PROTECT DATA, BUILD TRUST, AND ENABLE INNOVATION.**
> ***FADY YOUNES, CISCO***

SANS 2025 SOC SURVEY EXPOSES CRITICAL GAPS AND WHAT TOP TEAMS ARE DOING RIGHT

85% OF ANALYSTS SAY ENDPOINT ALERTS DRIVE RESPONSE, YET 42% OF SOCS LACK A STRATEGY FOR MANAGING INCOMING DATA.

The 2025 Global SOC Survey from SANS Institute reveals a stark disconnect between alert response and data strategy in Security Operations Centers (SOCs). While 85% of SOC analysts cite endpoint security alerts as their primary response trigger, 42% of SOCs admit to dumping all incoming data into a SIEM without a plan for retrieval or analysis. Recently released, the report highlights this and other critical insights drawn from thousands of practitioners worldwide and offers the industry's most comprehensive, vendor-neutral benchmark of SOC maturity, tooling, and staffing.

"SOCs are the backbone of modern cyber defense, but many remain overwhelmed and under-resourced," said Christopher Crowley, Certified Instructor at SANS Institute and lead author of the survey. "This year's data offers a clear look at how SOCs are adapting to the demands of 24/7 operations, AI integration, and remote work - while also surfacing common missteps and areas for growth."

Key findings from the 2025 report include:

- 82% of SOCs report operating 24/7.
- 85% of SOC analysts cite endpoint alerts as their primary response trigger.
- 73% allow some degree of remote work for SOC personnel.
- 42% send all incoming data to a SIEM without a defined strategy for management or retrieval.
- 42% use AI/ML tools in an out-of-the-box capacity without customization.

"If company leadership isn't prepared to fully commit the resources to make a tool effective, it would be better not to deploy it at all," said Crowley. "A shiny new technology that seems like a great solution requires budget, training, time and integration into workflow."

"We define a SOC by its capabilities, architecture, staffing, and whether those functions are internal or outsourced," added Crowley. "This report helps security leaders understand how others are building and evolving their SOCs, and where they stand in comparison."

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

cnme computer news middle east

Reseller MIDDLE EAST THE VOICE OF THE CHANNEL

Security ADVISOR MIDDLE EAST

HOSTED BY

tahawultech.com

For more information about the event and nomination details, please visit the event website below :-
https://www.tahawultech.com/futureenterpriseawards/2025/

BEYONDTRUST UNVEILS FIRST IDENTITY SECURITY CONTROLS FOR AI AGENTS

NEW CAPABILITIES IN IDENTITY SECURITY INSIGHTS PROVIDE VISIBILITY, ORCHESTRATION, AND GOVERNANCE FOR AGENTIC AI ACROSS ENTERPRISE ENVIRONMENTS.

BeyondTrust, a global leader in identity security, has launched the first production-ready security controls for AI agents. Delivered through its Identity Security Insights® and Pathfinder Platform, the new capabilities provide visibility into agent activity, secure orchestration of their actions, and an integrated intelligence layer to support faster and more informed security decisions.

Marc Maiffret, Chief Technology Officer at BeyondTrust, warned that the rapid adoption of agentic AI represents a critical new identity challenge.

"The rise of AI agents is creating a new and urgent identity security challenge. Often built on low-code and no-code platforms, they can be deployed in minutes with privileges that rival human admins," he said. "BeyondTrust uniquely connects visibility with proactive control across all identities so customers can rein in this new frontier of risk and turn AI into a safe force multiplier that also meets compliance requirements."

Marc Maiffret, Chief Technology Officer at BeyondTrust, says securing AI agents requires a holistic approach across the identity ecosystem.

Expanding identity security to AI agents

The release builds on BeyondTrust's August 2025 launch of Secrets Insights, which addressed risks tied to secrets and non-human identities. The latest update extends Identity Security Insights with three core capabilities:

- AI Agent Insights — Extends identity governance to AI agents, enabling discovery, classification, and risk scoring across SaaS and cloud platforms such as Salesforce Agentforce and ServiceNow. The capability uncovers shadow AI and enforces Zero Standing Privilege (ZSP) and Just-In-Time (JIT) policies.
- Model Context Protocol (MCP) orchestration — Provides a secure bridge for brokering agent actions across BeyondTrust products. This supports workflows such as JIT API requests in Entitle, credential rotations in Password Safe, and future integration with large language models.
- Omnipresent AI decision-support layer — Embedded in the Pathfinder Platform, this assistant delivers real-time insights and remediation steps based on customers' identity data. It is powered by BeyondTrust Phantom Labs™ research.

Why it matters for enterprises

The new capabilities are designed to help organisations adopt AI safely, while maintaining security and compliance:

- Accelerate AI adoption securely — Gain visibility into AI, human, and service identities, with privilege escalation paths mapped.
- Boost productivity — Automated remediation and real-time intelligence reduce risk while increasing operational speed.
- Simplify governance — Consolidated visibility, enforcement, and governance across all identity types.

With these innovations, BeyondTrust is extending its established Paths to Privilege and True Privilege™ capabilities across human, machine, secrets, and AI identities.

Addressing shadow AI

BeyondTrust also warns that most organisations remain unaware of the extent of shadow agentic AI operating within their businesses. To address this, the company has expanded its Identity Security Risk Assessment service to include AI-specific risks, enabling customers to identify exposures before attackers or auditors do.

MANAGEENGINE ENHANCES UNIFIED SECURITY PLATFORM WITH REENGINEERED THREAT DETECTION

NEW LOG360 CAPABILITIES ADDRESS SOC ALERT FATIGUE BY REDUCING FALSE POSITIVES, SCALING WITH ENTERPRISE DEMAND, AND ENSURING CURRENT THREAT COVERAGE.

Manikandan Thangaraj,
Vice President at ManageEngine.

> **THE BIGGEST CHALLENGE FOR SECURITY TEAMS TODAY ISN'T COLLECTING DATA—IT'S SEPARATING GENUINE SIGNALS FROM OVERWHELMING NOISE. MANIKANDAN THANGARAJ, VICE PRESIDENT, MANAGEENGINE**

ManageEngine, the enterprise IT management division of Zoho Corporation, has announced a significant enhancement to its security information and event management (SIEM) solution, Log360. The platform now incorporates a reengineered threat detection framework designed to reduce alert fatigue and improve operational efficiency for security operations centre (SOC) teams.

Log360 is a unified SIEM solution with integrated data loss prevention (DLP) and cloud access security broker (CASB) capabilities. Its Vigil IQ TDIR module combines threat intelligence, ML-based anomaly detection, correlation-driven attack detection, and incident management for advanced threat defence. With its latest reengineered detection capabilities, Log360 delivers improved signal fidelity, reduced false positives, and holistic visibility across on-premises, cloud, and hybrid environments.

Industry research highlights the scale of the challenge: more than 60% of SOC teams are overwhelmed with irrelevant threat data, while over half of cloud security alerts are considered noise, according to the 2025 Threat Intelligence Benchmark study commissioned by Google. ManageEngine's latest release directly addresses this problem by filtering out redundant alerts, enabling faster triage and reducing analyst burnout.

Manikandan Thangaraj, Vice President at ManageEngine, said:
"We've reengineered our detection system to not just build more complex rules, but to deliver true efficiency and empower SOC with flexible, granular rule-tuning capabilities that go beyond simple thresholds. With this advancement, SOC analysts can filter out benign noise without sacrificing the ability to catch a true compromise."

Enhancements for modern SOC teams

The upgraded Log360 platform introduces a unified detection console, object-level rule filters, and more than 1,500 prebuilt detection rules aligned with the MITRE ATT&CK framework and SIGMA standards. These rules are cloud-delivered and continuously updated to ensure that SOC teams remain equipped against emerging threats.

Architectural improvements have also been made to support enterprise scalability. A multi-tier structure, role-specialised log processing, and centralised multi-site collection deliver resilience and performance as data sources and log volumes expand across hybrid and distributed environments.

Key capabilities at a glance

- Reengineered detection: Consolidated detection console integrating correlation rules, MITRE ATT&CK mappings, UEBA insights, and threat intelligence feeds.
- Cloud-delivered content: 1,500+ prebuilt rules covering scenarios from privilege escalation to SaaS attacks, continuously updated for accuracy and coverage.
- Enterprise-grade scalability: Multi-tier architecture, log processor clusters, and centralised collection for large, distributed enterprises.

Customer validation

The effectiveness of the new detection capabilities has been validated by Emergency Communications of Southern Oregon (ECSO) 911, a United States-based ManageEngine customer. As a combined emergency dispatch facility and Public Safety Answering Point (PSAP), ECSO handles all 911 lines for Jackson County and Crater Lake National Park.

Corey Nelson, IT Manager at ECSO 911, said: "For a 911 emergency communications centre, security is the foundation of public trust—and any failure has immediate, real-world consequences. With Log360's optimised detection rules and filtering techniques, we have reduced false or low-priority alerts by 90%, allowing our analysts to focus on the threats that matter most."

ANOMALI APPOINTS CHRIS VINCENT AS CHIEF SALES OFFICER

INDUSTRY VETERAN TO DRIVE GLOBAL MARKET LEADERSHIP AND ACCELERATE REVENUE GROWTH

Anomali, the leading Security and IT Operations Platform, has announced the appointment of Chris Vincent as Chief Sales Officer. Vincent will lead the company's go-to-market and accelerate revenue growth.

Vincent brings over 20 years of sales leadership in cybersecurity and enterprise technology. His expertise spans building and leading high-performing sales teams, executing strategic transformations, embedding channel sales, and rapidly scaling revenue. These achievements establish him as the ideal leader to drive Anomali's mission to help customers modernise their security and IT operations with a disruptive data lake, next generation intelligence and safe agentic AI to deliver business outcomes while scaling productivity across operations.

"Vincent's deep expertise and proven track record make him the ideal leader to accelerate our global sales strategy with emphasis on the channels," said Ahmed Rubaie, CEO of Anomali. "His passion to help and delight customers and channel partners aligns well with our strategic direction and values. I am particularly excited about Chris leading our global expansion with MDRs, MSSPs and GSIs."

In his previous roles, Vincent served as Chief Revenue Officer at AKAIdentity and Halcyon, where he was instrumental in driving go-to-market strategy and the adoption of advanced cyber resilience solutions. He also spent over a decade at Optiv and its predecessor, Accuvant, guiding enterprise sales teams through significant growth periods. Additionally, he founded and successfully exited Clarity, a workflow automation company.

"I am excited to join Anomali during this transformative phase," said Chris Vincent. "Our AI-powered Security and IT Operations Platform, built on a high-speed data lake, is uniquely positioned to simplify security and IT operations and replace and consolidate outdated, fragmented solutions. We will deliver lightning-fast clarity, AI-assisted action, and measurable business outcomes for our clients worldwide while significantly reducing budget dollars."

As Anomali continues to redefine the future of security and IT operations, Chris Vincent's appointment marks a pivotal step in the company's journey to deliver unparalleled clarity, speed, and business outcomes for enterprises worldwide.

Fortify Your Cybersecurity
Fortinet
Global Cybersecurity Leader

Omada by tp-link

Omada Central

Unified Networking & Surveillance Solutions

Manage

Manage

Business Networking

Business Surveillance

Manage Trusted Networking and Surveillance Products

Omada Gateways

Omada Switches

Omada Access Points

Omada Cameras

Omada NVRs

- Unified Cloud Management
- Zero-Touch Provisioning (ZTP)
- AI Optimization & Built-In Troubleshooting
- Network Security & SD-WAN Reliability
- Cloud Based Controller
- Custom Guest Wi-Fi & Captive Portal
- Integrated Surveillance Management
- Role-Based Access Control (RBAC) & Multi-Tenant Support