ISSUE 106 | MAY 2026

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

INDUSTRIALISATION OF RANSOMWARE

ANTI-RANSOMWARE DAY 2026 SPECIAL

AGENTIC AI, SHADOW AGENTS, AND A 389 PER CENT SURGE IN VICTIMS. THE MIDDLE EAST'S DEFENDERS ARE NO LONGER FIGHTING A CYBERCRIME BUT ARE CONFRONTING AN ECONOMY.

tahawultech.com

cnme computer news middle east SUPPLEMENT

tahawultech.com

Women in TECHNOLOGY FORUM AND AWARDS

Give to gain. Powering women in tech

Gala Dinner Event

June 2026 | Dubai | 6:00 PM onwards

#WomenInTech2026 | #IWD2026 | #tahawultech

In alignment with International Women's Day 2026, TahawulTech.com, organised by CPI, invites you to the Women in Technology Forum & Awards 2026 — a flagship platform dedicated to advancing leadership, inclusion, and impact across the technology ecosystem.

The forum brings together CEOs, technology decision-makers, innovators, policymakers, and trailblazers to explore how organisations that actively invest in women — through mentorship, leadership pathways, skills development, and visibility — gain stronger innovation, resilience, and long-term growth.

Whether you are a technology leader, changemaker, or organisation committed to shaping a more inclusive digital future, this forum offers a powerful space to contribute, connect, and lead.

We look forward to welcoming you to Dubai this April as we come together to Give to Gain.

OFFICIAL PUBLICATIONS

cnme computer news middle east

Reseller MIDDLE EAST THE VOICE OF THE CHANNEL

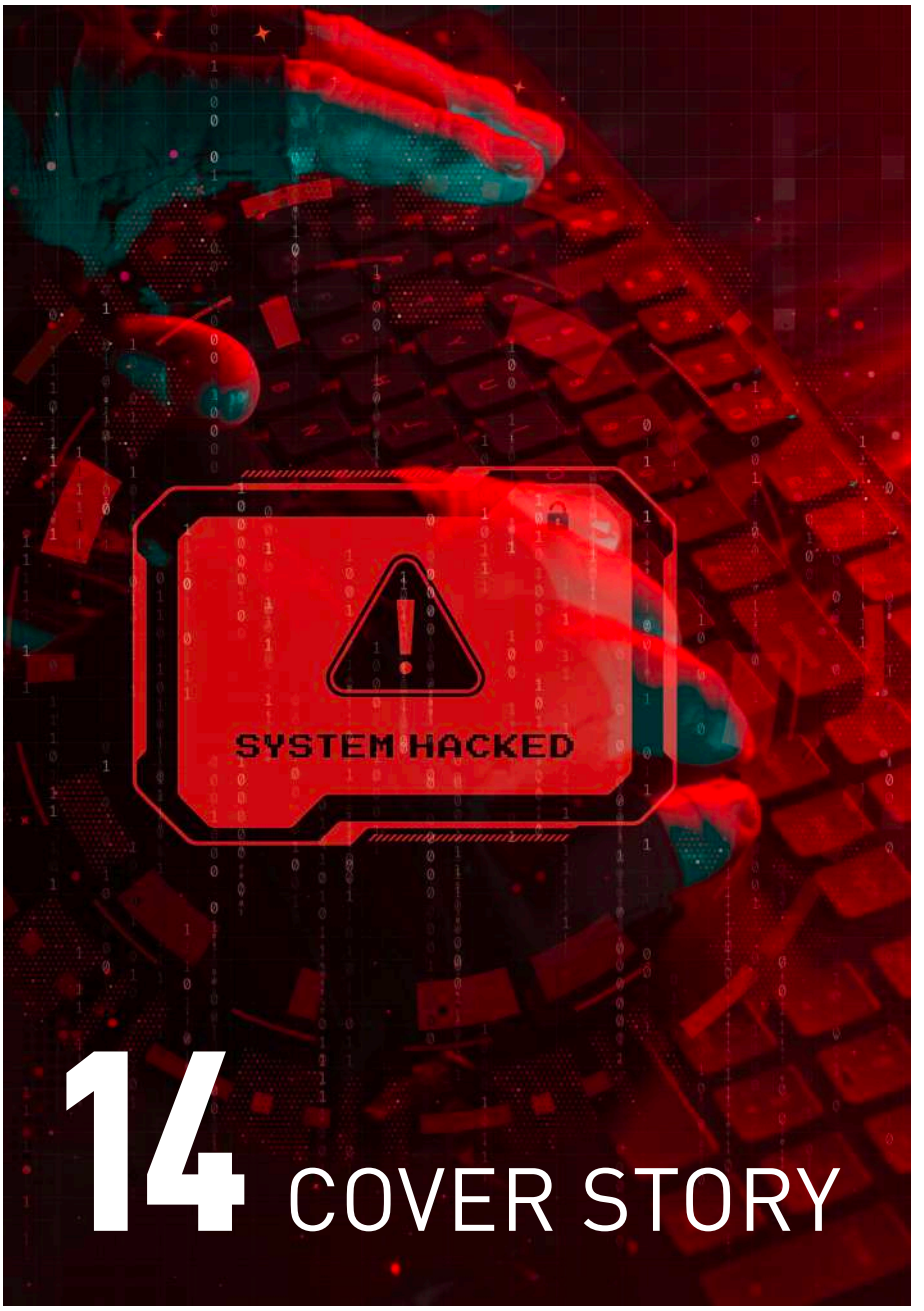
Security ADVISOR MIDDLE EAST

HOSTED BY

tahawultech.com

For more information about the event and nomination details, please visit the event website below :-
https://www.tahawultech.com/women-in-tech/2026/

CONTENTS



tahawultech.com

KSA FUTURE ENTERPRISE AWARDS 2026

30th August 2026

Radisson Blu Hotel & Convention Center
Riyadh Minhal

06:30 PM onwards

#KSAFEA2026 | #tahawultech

In August, CPI will be hosting the inaugural Future Enterprise Awards in Riyadh. The awards are designed to recognize IT and business leaders that are driving rapid digital transformation across the Kingdom.

The KSA Awards want to acknowledge those who are championing change, whether it be from a private or public sector organization, we want to pay tribute to the fearless trailblazers forging a new path and a new identity for the KSA.

GOLD SPONSOR

logitech

OFFICIAL PUBLICATIONS

cnme computer news middle east

Reseller MIDDLE EAST

Security MIDDLE EAST

HOSTED BY

tahawultech.com

For more information about the event and nomination details, please visit the event website below :-
https://tahawultech.com/ksa-futureenterpriseawards/2026/

EDITOR'S NOTE

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

Sandhya DMello
Editor

DEFENDING AT MACHINE SPEED

May 2026 marks a turning point for cybersecurity in the Middle East. The conversations dominating this edition are no longer about isolated breaches or patch cycles. They are about the industrialisation of cybercrime and the rise of an entirely new trust infrastructure built for the agentic AI era.

This month's cover story unpacks the staggering 389 per cent surge in ransomware victims flagged by Fortinet, alongside the rise of "encryption-less" extortion and shadow agents that compress the attack lifecycle to machine speed. Ransomware in 2026 is no longer a crime. It is an economy, and the region sits squarely in its crosshairs.

RESILIENCE, IDENTITY, SOVEREIGNTY, TRUST

The response from industry has been decisive. Veeam's launch of the DataAI Command Platform signals the creation of a new infrastructure category designed to bring resilience, security, governance and privacy into one connected trust layer. Cisco, SentinelOne, Group-IB, ManageEngine and Tech Mahindra are similarly racing to embed identity, automation and AI-driven response into the security fabric. Closer to home, the UAE Cyber Security Council and CPX have unveiled the 'UAE Cyber Factory', a bold step toward homegrown, AI-powered cyber sovereignty in a country defending against more than 800,000 daily attacks.

Our World Password Day feature explores how identity-first security is replacing legacy credential models, while Sophos research reveals that 71 per cent of organisations suffered an identity-related breach in the past year. It is a sobering reminder that humans and non-human identities alike are now the frontline.

From Cloudforce One's findings on AI reasoning as the new attack surface, to Genetec's call for stronger credential governance, this edition captures an industry pivoting from reactive defence to predictive, identity-led resilience.

The perimeter has moved. The data, and the trust around it, is now the battleground.

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

VEEAM LAUNCHES DATAAI COMMAND PLATFORM, THE INDUSTRY'S FIRST UNIFIED DATA AND AI TRUST INFRASTRUCTURE FOR THE AGENTIC ERA

Combining the world's number one data resilience with number one data security, Veeam delivers the missing layer in the AI stack, bringing together data, access, identities and AI in one connected trust platform.

Veeam Software, the Data and AI Trust Company, announced the Veeam DataAI Command Platform at VeeamON 2026 in New York City. The platform marks a defining moment for enterprise technology: the creation of an entirely new infrastructure category purpose-built for a world where autonomous AI agents operate inside the enterprise at machine speed, all powered by data.

The DataAI Command Platform is the result of Veeam's acquisition of Securiti AI — the top-ranked platform in data and AI security — fused with Veeam's twenty years of resilience leadership and its protection of more than 550,000 customers across 150+ countries, including 77% of the Global 2000.

Anand Eswaran, CEO, Veeam.

"The infrastructure to deploy AI exists. The infrastructure to trust it doesn't. With the DataAI Command Platform, Veeam is building the missing layer combining resilience, security, governance, compliance and privacy, in one platform," said Anand Eswaran, CEO at Veeam. "Today, agents need to get to data, which means we need to open the security perimeter. That means the security control point is now the data itself and that demands a new approach to trust that can accelerate the safe use of AI."

The Defining Challenge of the Agentic Era

Enterprises have entered the Agentic Era. Autonomous AI agents now outnumber human employees 82:1, and 97% of those agents carry excessive privileges. The volume and speed at which agents operate is collapsing the window available to detect and respond to threats. Agentic AI is now the number one cyber threat.

Introducing the Veeam DataAI Command Platform

The Veeam DataAI Command Platform is where data, access, identities and AI converge in a single connected trust layer for AI. It spans production data and backup data, covering every agent, identity and model across an organisation's entire IT estate. The platform is built on six integrated capabilities:

DataAI Command Graph — The intelligence foundation powering the entire platform. With 300+ connectors across every cloud, Software-as-a-Service (SaaS) application and on-premises environment, the graph provides a granular understanding of the data, not which database exists, but which specific file carries sensitive data, who has access, and which exact change created a risk condition. Uniquely, the graph now spans both live and backup systems simultaneously — context that no point solution in the market has today.

DataAI Security — Powered by the top-ranked DSPM platform, providing best-in-class data and AI security posture management combined with identity intelligence and resilience confidence in a single unified view.

DataAI Governance — Control enforced at the data source, not at the agent. Known and unknown agents — whether sanctioned or rogue — cannot access sensitive data if that data is governed at the source. This closes the structural gap in runtime-only agent governance approaches.

DataAI Compliance — Mapped against 100+ regulatory frameworks, including the EU AI Act, DORA, GDPR, HIPAA, NIST and AI RMF. It generates auditable evidence regulators and boards need.

DataAI Privacy — Automated privacy policies enforced in real time, at the source by user and jurisdiction. Powered by the most advanced identity intelligence graph in the industry (a People Data Graph) that unifies structured and unstructured personal data across hybrid multicloud environments, enabling faster and more accurate privacy operations than traditional siloed data mapping tools.

DataAI Precision Resilience — Twenty

years of recovery leadership, now evolved for machine-speed threats. Because the DataAI Command Graph understands the data estate at granular depth, recovery is surgical: undo exactly what went wrong without rewinding the entire system. Alongside the DataAI Command Platform, Veeam today announces a preview of the first two resilience offerings on the platform. Veeam Intelligence ResOps for M365 brings the full intelligence of the DataAI Command Graph to the world's most widely deployed SaaS platform. And the new DataAI Resilience Module in the DataAI Command Platform gives existing Veeam Data Platform customers access to the platform's cross-domain intelligence and agentic capabilities — no re-migration required.

VeeamON 2026

Veeam is also announcing the Veeam Data Platform 13.1 preview, Veeam Intelligence ResOps and the Veeam Data and AI Trust Maturity Model. The new model has been informed by data and insights from more than 300 CIOs and CISOs. The model provides a prescriptive four-pillar, 12-dimension, 49 sub-dimension framework across five maturity levels, enabling enterprises to benchmark their current posture and define a clear path to becoming fully AI-ready.

QUALYS AND CONVERGE LAUNCH JOINT OFFERING TO LOWER CYBER INSURANCE PREMIUMS

Collaboration streamlines the insurance application process, reduces the risk of inaccurate self-reporting, and incentivises strong cyber posture.

Qualys, Inc., a leading provider of cloud-based IT, security and compliance solutions, together with Converge, pioneers in advanced cyber risk management and underwriting, announced a joint offering that rewards organisations for demonstrated cybersecurity compliance. The collaboration allows Qualys customers who actively manage and prove strong security hygiene with Enterprise TruRisk Management (ETM) to potentially qualify for reduced cyber insurance premiums from Converge.

Sumedh Thakar, President and CEO of Qualys.

Traditional cyber insurers struggle to price and assess risk accurately against the backdrop of increasing ransomware attacks, data breaches and supply chain incidents. Current cyber insurance applications rely on manual questionnaires, a process that is time-consuming, inconsistent and easy to get wrong. The Qualys Converge Connect Insurance Report (CCIR) generated by ETM allows a company's data to speak for itself, verifying vulnerability management, patch management and endpoint detection controls in a standardised format that Converge underwriters can evaluate quickly and accurately. By providing underwriters with accurate insights into an organisation's security posture in real time, the Qualys CCIR results in a more objective and precise premium that reflects real risk levels rather than industry averages.

Automated data from Qualys ETM feeds into the CCIR, saving time, reducing administrative burden and eliminating the risk of inaccurate self-reporting. The report will include metrics that showcase measurable risk reduction, faster remediation velocity, higher compliance rates and expanded asset coverage. It reduces friction and streamlines the cyber insurance application process, while giving organisations an ongoing incentive for improving their cyber hygiene.

"Cyber risk has historically been priced on snapshots and self-reported answers, leaving real exposure invisible between renewals," said Tom Kang, CEO of Converge. "With verified data, we will be able to underwrite to a company's live security posture and provide policyholders who do the hard work of reducing risk to see the benefits."

"Cyber insurance is key to the overall risk management strategy, but there has to be an easier way to correlate the strength of an organisation's cyber posture with what they should pay in insurance," said Sumedh Thakar, President and CEO of Qualys. "That's why we created ETM to provide stakeholders with an accurate picture of their true risk, enabling better business outcomes like cyber insurance savings, and a greater incentive to reduce their cyber risk."

The Qualys CCIR will cover a range of solutions across the Qualys portfolio, including ETM, Vulnerability Management, Detection and Response (VMDR), TruRisk Eliminate, and Endpoint Detection and Response (EDR). The report, independently generated live, will be valid for 30 days.

GENETEC URGES STRONGER IDENTITY, CREDENTIAL GOVERNANCE FOR PHYSICAL SECURITY SYSTEMS

Genetec is calling on organisations to move beyond basic cyber hygiene and adopt a governance-first approach to identity and access across connected physical security systems.

Genetec Inc., the global leader in enterprise physical security software, is urging organisations to strengthen credential governance across connected physical security systems, as AI accelerates the scale and sophistication of cyber threats.

AI-driven tools are accelerating credential-based attacks by increasing their speed, scale and precision. For organisations managing connected cameras, access control systems, servers and cloud services, weak or poorly governed credentials can expose sensitive operations and create new pathways into organisations. This includes the passwords used to connect directly to devices themselves, which are often overlooked but can provide a direct entry point if not properly managed. In this environment, relying on periodic password changes or basic cyber hygiene is no longer sufficient.

Firas Jadalla, Regional Director, Middle East, Turkey and Africa, Genetec Inc.

"AI is changing the speed and scale of cyber risk," said Firas Jadalla, Regional Director, Middle East, Turkey and Africa, Genetec Inc. "Attackers can now move faster and are using AI to impersonate people, tailor social engineering attacks, uncover vulnerabilities at scale, and evade detection. To respond, organisations need to actively govern access and identity across their systems, not just set controls once and hope they hold."

The recent Genetec Enterprise Physical Security in the Cloud Era research, which was based on insights from more than 7,300 physical security professionals worldwide, found that 58.7% of organisations have experienced an increase in phishing and smishing attacks, while 41% reported a rise in overall physical or cyber incidents. Social engineering was identified by 43.5% as a leading attack vector.

Across the Middle East, where organisations are accelerating digital transformation and investing heavily in smart, connected infrastructure, the need to secure identity and access across physical security systems is becoming increasingly important. As cyber risks become more sophisticated, stronger credential governance can help organisations protect critical environments while supporting wider cyber resilience priorities.

Genetec is encouraging organisations to move beyond isolated credential controls and adopt a governance-first approach to identity management in physical security environments, including:

Strengthen identity and credential controls

Organisations should eliminate default and shared credentials, enforce strong authentication such as passkeys, and adopt multi-factor authentication (MFA) to reduce common attack entry points. This must extend to devices as well, replacing static passwords with certificate-based authentication when possible, and ensuring centralised management and regular credential rotation.

Closer alignment between IT and physical security teams

Bringing IT and physical security teams together helps apply consistent security standards, improve visibility into access risks, and coordinate incident response. As physical security systems become more connected to enterprise networks, cross-functional alignment can help organisations identify weak points and respond more effectively to credential-based attacks.

Governance-first management of physical security systems

Organisations should manage physical security infrastructure with the same rigour as other mission-critical systems. This includes regular access reviews, controlled updates, and partnerships with trusted technology partners that support long-term security, transparency and operational resilience.

GROUP-IB LAUNCHES PREVYN AI TO BRIDGE GAP BETWEEN DETECTION AND PREDICTIVE CYBER DEFENCE

New cognitive core orchestrates agentic research and assistive response to outpace machine-speed threats.

Group-IB, a leading creator of predictive cybersecurity technologies to investigate, prevent and fight digital crime, announced the launch of Group-IB Prevyn AI. As the cognitive core of the Group-IB Unified Risk Platform, Prevyn AI transforms Group-IB's data lake into rapid insights in Threat Intelligence and decisive actions in Managed XDR.

Built to address the "execution gap" facing modern security teams, Prevyn AI moves beyond simple chatbots to provide a foundational reasoning capability designed for adversary-centric analysis. The system is powered by Group-IB's intelligence Data Lake, accumulated from decades of active cybercrime investigations, local insights from its Digital Crime Resistance Centres around the globe, and collaboration with international law enforcement. By grounding its reasoning in proprietary adversary intelligence rather than common open-source data, Prevyn AI delivers analysis that is both materially deeper and immediately operationally relevant.

From Agentic Research to Assistive Response

Within Group-IB Threat Intelligence, Prevyn A**I** functions in an agentic mode, coordinating 11 specialised agents to carry out complex, adversary-focused intelligence and research. These agents — including experts in malware, threat actors and dark web monitoring — are modelled on real High-Tech Crime investigative logic. This adversary-centric approach allows the platform to identify attacker intent and infrastructure staging before attacks launch, moving security from a reactive to a predictive posture. Internal evaluations show that this system improves research quality by more than 20% across accuracy and analytical depth.

In Managed XDR, the system operates in assistive mode to reduce the operational burden of SOC work. Prevyn AI analyses alerts, generates incident reports and prepares structured remediation workflows. This allows analysts to execute complex responses with a single click, ensuring that defenders can respond at the pace required to fight weaponised, machine-speed attacks.

Human-in-the-Loop Governance

Designed for high-stakes and regulated environments, Prevyn AI features a structural analyst-in-the-loop architecture. Every AI recommendation requires human approval before execution, ensuring that business-critical decisions remain under human control and align with emerging global AI governance expectations such as DORA and the EU AI Act.

"Threat actors are already operating at machine speed, and defenders cannot respond at the pace required when investigations remain manual. The name Prevyn comes from 'pre-vision'. Our goal is to move security from reactive to predictive, helping teams identify threat actor intent and infrastructure before an attack even launches," said Dmitry Volkov, CEO of Group-IB.

Group-IB Prevyn AI is now available to all existing Group-IB Threat Intelligence and Managed XDR customers at no additional cost.

MANAGEENGINE ANNOUNCES NATIVE SOAR TO CLOSE THE DETECTION-TO-RESPONSE GAP WITH CROSS-DOMAIN AUTOMATION

Built-in orchestration and low-code playbooks in Log360 let security teams handle the full incident life cycle within one platform, bringing detection, AI investigation and automated response into a single data model.

ManageEngine, a division of Zoho Corporation and a leading provider of enterprise IT management solutions, announced a core architecture upgrade in Log360, its unified security platform, introducing native SOAR capabilities, seven new integrations with some of the industry's leading security vendors, and cross-domain orchestration capabilities that place detection, AI investigation and automated response in a single data model.

Manikandan Thangaraj, Vice President, ManageEngine.

The upgrade introduces native SOAR built into the unified security platform's core data model, adds seven critical integrations across leading EDR, identity and threat intelligence platforms to expand cross-domain orchestration, and combines a low-code playbook builder with ready-to-use templates designed for faster time to value.

Security operations are entering the agentic automation era, albeit with infrastructure that was not built for it. Across most SOCs, tools multiply without converging, each coming with its own alert queue, data model and demand on analyst time. The visibility problem is rarely a shortage of tooling; it's a failure of integration. AI agents and autonomous response only work when the layers beneath them share context, and most security stacks do not.

Log360's native SOAR is engineered for that shared context. A single playbook can isolate an endpoint through EDR, revoke a compromised session through IAM, enrich the incident with external threat intelligence, open a service ticket and notify the SOC, all driven by the same alerts, detections and behavioural signals the platform already produces.

"The next evolution in security operations is about rethinking the architecture so that AI, detection and response share the same foundation," said Manikandan Thangaraj, Vice President of ManageEngine. "When an AI investigation agent and an orchestration engine operate over the same data model, the friction that has kept security teams reactive for years is eliminated. No API handoffs, no reconstructing context, no gap between insight and action. The best automation isn't prescriptive, it's programmable. That's what we've built into Log360."

Key New Capabilities in Log360

Expert playbooks, ready on day one: A CDN-delivered library of prebuilt response templates means automation is live on day one. When teams are ready to go deeper, analysts extend workflows through low-code platform Zoho Qntrl, while engineers take full control with Python or Deluge. The approach allows teams to build once and continuously adapt workflows to evolving environments and compliance requirements.

Automated response across the entire stack: One automated workflow can isolate endpoints, revoke compromised credentials, open service tickets and enforce response actions across EDR platforms, network infrastructure and business applications, eliminating manual handoffs between teams and tools.

Context-aware incident response: Playbooks enrich alerts with threat intelligence and asset context, apply conditional logic to route incidents by severity or compliance scope, and execute multi-step response sequences automatically without human intervention.

Endpoint coverage that closes the cross-domain gap: Endpoint telemetry, along with identity and cloud context, is brought into Log360's correlation and response layer to track and contain threats from a single platform.

TECH MAHINDRA, CISCO PARTNER TO LAUNCH CYBER RESILIENCE FABRIC

Joint solution combines Cisco's Splunk Enterprise Security with Tech Mahindra's proprietary Risk Scoring Platform to give enterprises unified visibility, intelligence-led decision-making and faster response across complex threat environments.

Tech Mahindra, a leading global provider of technology consulting and digital solutions to enterprises across industries, announced a partnership with Cisco, the worldwide leader in networking and security, to launch a joint security solution, Cyber Resilience Fabric. The solution is designed to help enterprises strengthen digital resilience by enabling unified visibility, intelligence-led decision-making and faster response across increasingly complex threat environments.

Saket Singh, SVP & Business Head – Digital Core Services (Cloud, Infrastructure, Network and Cyber Security Services), Tech Mahindra

Cyber Resilience Fabric integrates Cisco's Splunk Enterprise Security with Tech Mahindra's proprietary Risk Scoring Platform to bring together real-time security data, AI-assisted analytics and contextual risk intelligence. The solution is purpose-built for enterprise leaders including CISOs, CIOs and CTOs who require deeper visibility into cyber risk posture while ensuring governance alignment, regulatory compliance and uninterrupted operations. By applying contextual risk prioritisation across security events, the platform enhances triage accuracy, reduces operational noise and delivers a consolidated view across security, operational and risk signals.

Saket Singh, SVP & Business Head – Digital Core Services (Cloud, Infrastructure, Network and Cyber Security Services), Tech Mahindra, said, "In today's hyper-connected enterprise landscape, the growing scale and sophistication of cyber threats are overwhelming traditional security operations, often leading to delayed detection and fragmented response. Through our partnership with Cisco, we are addressing this challenge by combining contextual risk intelligence with AI-driven analytics to help enterprises move from reactive alert management to proactive, risk-led decisioning. Cyber Resilience Fabric will enable faster detection, prioritised response and stronger operational resilience."

The solution enables organisations to transition from traditional alert triage to risk-based, business-aligned decisioning, improving the ability to detect threats earlier, respond with precision and ensure resilient recovery of business-critical services. Cyber Resilience Fabric tackles a critical industry gap where enterprises are grappling with expanding attack surfaces and rising operational complexity. By embedding intelligence-driven prioritisation into security workflows, the solution enables faster and more effective incident management.

Shannon Leininger, SVP, Global Partner Sales & Splunk Channel Chief, Cisco, said, "The convergence of data, AI and security is non-negotiable for modern enterprises. By integrating Splunk's and Tech Mahindra's unique capabilities, we are accelerating our customers' ability to prioritise effectively and automate their defence, delivering real, measurable digital resilience."

The announcement further reflects a shared commitment between Tech Mahindra and Cisco to deliver enterprise-ready, outcome-driven security solutions that empower organisations to operate securely, adapt continuously and recover rapidly as cyber threats evolve.

CISCO INTRODUCES SECURITY INNOVATIONS TO SUPPORT ENTERPRISE AI AGENT ADOPTION

With end-to-end security across AI actions, Cisco is helping organisations confidently deploy AI agents at scale.

Cisco announced significant security innovations designed for the agentic AI ecosystem, where software no longer just answers questions — it acts. At RSA Conference 2026, Cisco introduced solutions to address AI security issues and remove a top barrier to agent adoption. By establishing trusted identities, enforcing strict Zero Trust Access controls, hardening agents before deployment, enforcing guardrails at runtime, and giving security operations centre (SOC) teams the tools to stop threats at machine speed, Cisco is building security into the foundation of the emerging AI economy.

Jeetu Patel, President and Chief Product Officer at Cisco

"AI agents aren't just making existing work faster; they're a new workforce of co-workers that dramatically expand what organisations can accomplish," said Jeetu Patel, President and Chief Product Officer at Cisco. "Projects shelved for lack of resources are now within reach. The only limit is imagination, and security teams are the key to unlocking this opportunity by making the agentic workforce safe enough to trust."

In a recent Cisco survey of major enterprise customers, 85% reported experimenting with AI agents, but just 5% had moved agentic technology into production.

To unleash the vast potential of AI agents, Cisco is addressing three key pillars to securing the agentic workforce. First: protecting the world from agents, ensuring they can only act as intended. Second: protecting agents from the world, ensuring they can't be manipulated or corrupted. Third: detecting and responding to AI incidents at machine speed and scale.

Protect the world from agents: establish trust before agents go to work

Like new employees, AI agents need onboarding to establish their identity, understand their function, and map them to an accountable human manager. Yet today, most enterprises are unaware of which agents are running, let alone who is responsible if something goes wrong. Existing SSE tools weren't built to enforce time-bound access for agentic workload identities, nor can they understand context behind agent requests.

According to the 2025 Cisco Talos Year in Review released, attackers overwhelmingly targeted a subset of components that directly authenticate users, enforce access decisions, or broker trust between systems. Adversaries' focus on identity will only accelerate with the rise of agentic workloads.

To address these challenges, Cisco is extending Zero Trust Access to AI agents, holding them accountable to a human employee and securing agentic actions. New Duo IAM capabilities integrate with novel MCP policy enforcement and intent-aware monitoring in Cisco Secure Access to enforce strict access control, uniquely helping organisations gain full visibility and governance over their agentic workforce. These capabilities include:

Agent Identity Management: Customers can register agents in Duo IAM and map them to accountable human owners, ensuring every agent has a verified identity and enabling traceability of actions.

Agent and Tool Visibility: Cisco Identity Intelligence discovers agentic and non-human identities to help organisations understand existing AI usage.

Strict Access Control: Agents are assigned fine-grained permissions only for the specific tasks they perform or resources they need for a short duration, with all tool traffic routed through an MCP gateway to eliminate blind spots.

Protect agents from the world: AI Defense safeguards the agentic workforce

As businesses race to deploy AI agents across increasingly complex and distributed environments, Cisco is expanding AI Defense with powerful new tools that help organisations test, trust and secure their AI agents and the interactions between them.

To empower more organisations to meet this challenge head-on, Cisco

is democratising the industry-leading capabilities of AI Defense by launching Cisco AI Defense: Explorer Edition. This new self-service solution is built on the same core AI Defense Validation engine trusted by Global 2000 customers. After signing up, users can begin red teaming the AI models and applications that will be deployed into agentic workflows to uncover susceptibility to attacks and measure risk posture before deployment. This toolkit enables AI developers, AppSec teams and security researchers to build and secure AI agents.

Together, these capabilities let organisations move from pilot to production with confidence: knowing their agents have been tested, benchmarked and hardened before they ever touch a production system.

Building on the release of its first open source foundation AI model, Cisco is introducing DefenseClaw — a secure agent framework designed to eliminate friction between development and security. By integrating a suite of essential open source tools — including Skills Scanner, MCP Scanner, AI BoM and CodeGuard — DefenseClaw helps ensure that every skill is scanned and sandboxed, every MCP server is verified, and every AI asset is automatically inventoried, enabling developers to deploy secure agents with greater speed and confidence.

Detect and respond at machine speed: empowering the agentic SOC

The same AI agents posing new security challenges can also be the most powerful tool in a defender's arsenal. Today's SOC analysts are overwhelmed by alert fatigue and fragmented data, spending more time on research than response.

Splunk, part of Cisco's security portfolio, has already moved to embed AI capabilities into key SOC workflows. It is further evolving the SOC from reactive to proactive.

UAE CYBER SECURITY COUNCIL AND CPX LAUNCH 'UAE CYBER FACTORY'

The UAE Cyber Security Council (CSC), in collaboration with its national strategic cybersecurity partner CPX Holding, a leading provider of cutting-edge cyber and physical security solutions and services, today announced the launch of the 'UAE Cyber Factory'.

The landmark initiative, unveiled at the fifth edition of the 'Make it in the Emirates' exhibition, is a decisive step toward strengthening the nation's digital leadership and reinforcing its cyber sovereignty. As cyber threats continue to evolve in scale and complexity, the initiative is set to enhance the country's ability to anticipate, detect and respond to increasingly sophisticated attacks targeting both institutions and individuals. With more than 800,000 daily cyberattacks recorded in recent months, as per the UAE Cyber Security Council, the urgency to build robust and adaptive defenses has become critical to safeguarding national infrastructure and public trust.

His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security for the UAE Government, said, "The launch of the UAE Cyber Factory signals a new phase of leadership, positioning the UAE as a global hub for advanced cybersecurity and a digital power shaping the future of the industry. In the face of rising global challenges, the UAE stands as a leading model that not only protects but also innovates and leads by developing advanced technologies capable of detecting, preventing and deterring cyber threats effectively."

The UAE Cyber Factory will design, build and scale the next generation of cybersecurity capabilities through the design of advanced programs, technologies and systems powered by AI, enabling the UAE to address rapidly evolving cyber threats with greater speed and precision. The factory will also serve as a fully sovereign integrated ecosystem that empowers the nation with end-to-end ownership of its cybersecurity capabilities, enhances digital independence and strengthens its readiness to proactively counter cyber threats.

Through this initiative, CSC and CPX aim to create a fundamental shift in the UAE's cybersecurity landscape, aligning with the country's ambition to design, develop and produce globally competitive cybersecurity solutions locally.

Hadi Anwar, CEO of CPX, said, "We are truly honored to serve as the trusted partner of the UAE Cyber Security Council and contribute to this milestone project. The UAE Cyber Factory marks a major step toward a sovereign, future-ready cybersecurity ecosystem. It brings together local talent, advanced engineering and innovation built in the UAE. By enabling end-to-end capabilities and strengthening national ownership of digital defenses, it will help create a secure and resilient environment for government, businesses and citizens."

INDUSTRIALISATION OF RANSOMWARE: 2026 IS YEAR OF RECKONING

RANSOMWARE IN 2026 IS NO LONGER A CRIME; IT IS AN ECONOMY, AND THE MIDDLE EAST SITS SQUARELY IN ITS CROSSHAIRS.

Ransomware began its life as a blunt instrument. A malicious payload landed on an endpoint, files were encrypted, and a ransom note demanded payment in exchange for a decryption key. The economics were simple, the operators were artisanal, and the defence playbook — patch, back up, restore — was tractable for any organisation willing to invest in the basics.

That world is gone.

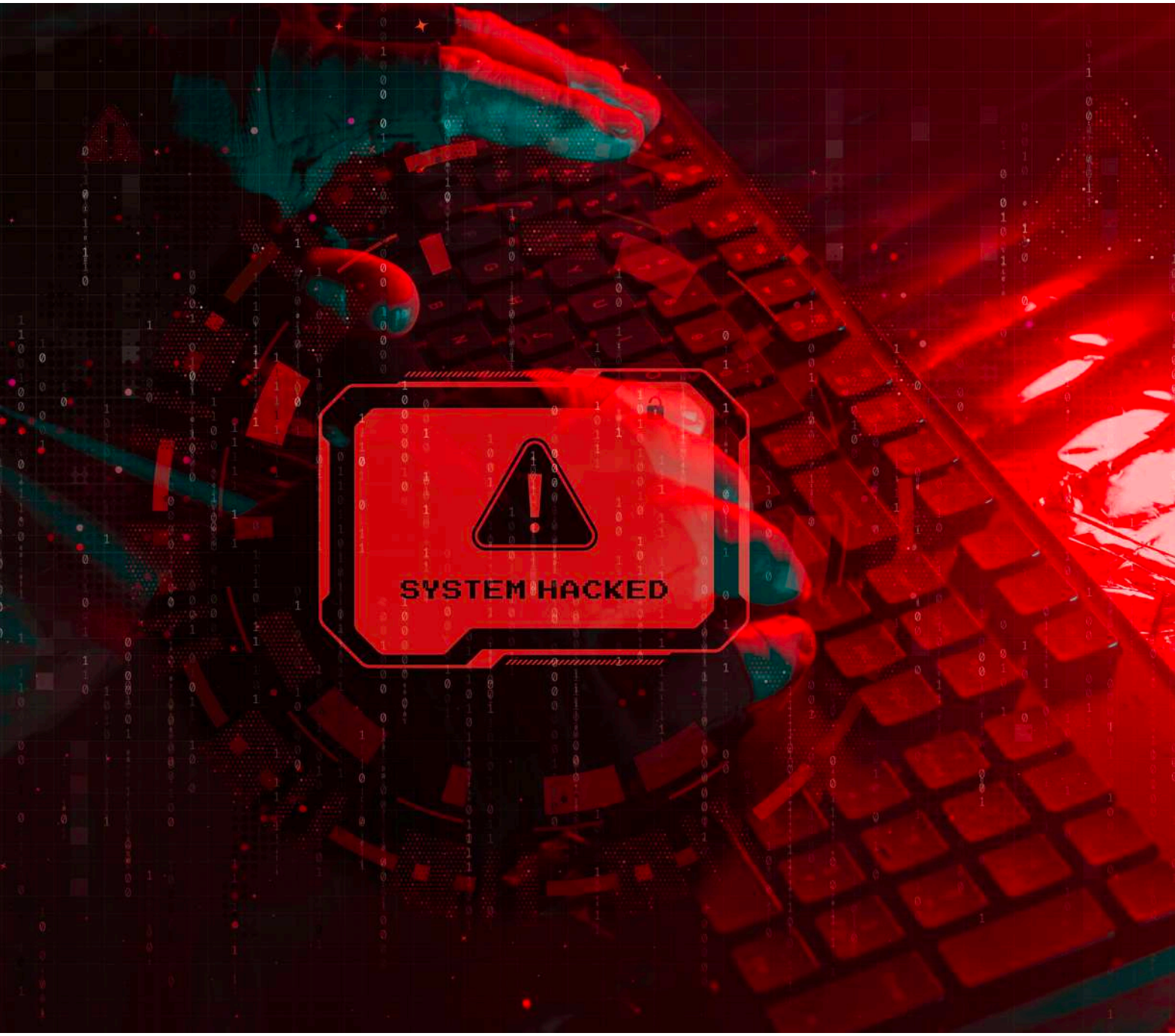
Modern ransomware is a multi-stage, multi-actor, AI-accelerated operation. The encryption payload, once the centrepiece, has become almost an afterthought. Today's attackers infiltrate identity infrastructure first, harvest credentials through commodity stealer malware, sell or trade that access through Initial Access Brokers, exfiltrate sensitive data over weeks of quiet reconnaissance, and only then — if at all — deploy encryption. Kaspersky's 2026 research captures the trajectory precisely: the industry is witnessing the rise of "encryption-less" extortion, where threat actors monetise stolen data through reputational and regulatory pressure rather than file lockdown. The Gentlemen, identified by Kaspersky as one of the most consequential new ransomware actors of 2026, exemplifies this shift toward scalable, business-like extortion focused primarily on data theft.

The numbers from Fortinet's 2026 Global Threat Landscape Report from FortiGuard Labs tell the story in stark relief. Confirmed ransomware victims have surged to 7,831 globally, up from roughly 1,600 the previous year — a 389 per cent year-on-year increase. Manufacturing tops the target list with 1,284 victims, followed by business services at 824 and retail at 682. The compression of the attack life cycle is equally dramatic: time-to-exploit, once measured at 4.76 days, has collapsed to 24 to 48 hours for critical outbreaks. With the recent React2Shell vulnerability, active exploitation attempts surfaced within hours of public disclosure.

The accelerant is agentic AI. FortiGuard Labs has documented a thriving dark web economy for AI-enabled offensive tooling — enhanced versions of WormGPT and FraudGPT alongside newer services such as HexStrike AI for automated reconnaissance and BruteForceAI for intelligent, multi-threaded credential attacks. These tools function as commercial products, with versioning, tiered pricing, and customer support. Fortinet calls the emerging operator class shadow agents: AI-powered components that reduce skill requirements while compressing the attack life cycle. Brute force attempts dropped 22 per cent year-on-year, even as global exploitation attempts rose 25.49 per cent. Criminals are working smarter, not harder.

Identity is the new perimeter. FortiCNAPP intelligence confirms that most confirmed cloud incidents in 2025 originated from stolen, exposed, or misused credentials. Within dark web "database" activity, stealer logs now dominate at 67.12 per cent of advertised datasets. Credential-stealer malware — RedLine at 911,968 infections, Lumma at 499,784, Vidar at 236,778 — has become the upstream engine feeding the entire ecosystem. Kaspersky's parallel research adds another dimension: endpoint detection and response "killers" — tools designed to disable security solutions before deploying ransomware — have become standard kit in modern intrusions, alongside the growing role of Initial Access Brokers running Access-as-a-Service operations through compromised RDWeb portals.

Kaspersky Security Network data places the Middle East fourth globally in ransomware exposure, with 7.27 per cent of regional organisations attacked in 2025 — ahead of Europe at 3.82 per cent, and



trailing only Latin America, Asia-Pacific, and Africa. Global ransomware damages were projected to reach approximately $57 billion in 2025 — nearly $156 million every single day. Among active groups, Kaspersky identifies Qilin as the dominant ransomware-as-a-service operator following RansomHub's seizure, with Clop and Akira rounding out the top three. Even more concerning: ransomware families have begun adopting post-quantum cryptography standards, signalling a generational shift in how encrypted data may resist future decryption.

The defence mandate has shifted with the threat. Prevention alone is no longer credible. Resilience — measured by how quickly an organisation can detect, contain, and recover — has become the metric that matters. Identity security, immutable backups, tested recovery procedures, continuous exposure management, and unified visibility across hybrid environments are no longer optional. They are the architecture of survival.

Industry Voices:
To mark Anti-Ransomware Day, leading cybersecurity voices shared their perspectives on what it takes to stay operational in 2026.

Derek Manky, Chief Security Strategist and Global VP of Threat Intelligence, Fortinet FortiGuard Labs

Cybercrime is one of the world's most pervasive and costly threats, and our latest Global Threat Landscape Report reveals how malicious actors are beginning to leverage agentic AI to execute more sophisticated attacks. Cybercriminals are increasingly using AI to bolster their tactics, and cyber defenders must evolve cybersecurity operations into an industrialised defence — adopting AI-enabled tools that respond at the same velocity as modern threats.

Fabio Assolini, Lead Security Researcher, Kaspersky GReAT

Ransomware has evolved into a highly organised ecosystem focused on monetising stolen data, disabling defences, and scaling attacks with business-like efficiency. Threat actors are quickly adapting, weaponising legitimate tools, exploiting remote access infrastructure, and even adopting post-quantum cryptography years earlier than many expected. The purpose of Anti-Ransomware Day is to raise global awareness about the threats posed by ransomware and to promote best practices for prevention and response. We urge all users to stay secure, set up layered defences, invest in backups, and boost cyberliteracy levels to counter attacks.

Walid Natour, Director – Security Engineering, Tenable

The era of human-speed defence is over. Frontier AI models have broken the economics of vulnerability discovery — what once took researchers weeks can now be done by AI-powered attackers in hours, collapsing the window between flaw discovery and ransomware exploit from months to minutes. In 2026, enterprises must abandon reactive firefighting and 30-day patch cycles. Standard tools flag around 60 per cent of vulnerabilities as critical — operationally unworkable. Leaders must focus on the small fraction, often under 2 per cent, that create a reachable attack path to critical assets.

Meriam ElOuazzani, Vice President for Middle East, Turkey, and Africa, Censys

Ransomware has always been a numbers game. What AI is doing is changing the maths in the attacker's favour. Reconnaissance that used to take a skilled operator a week now takes an automated agent an afternoon. For organisations in the Middle East, the most exposed surface is the one they cannot see. Digital transformation has been fast, the attack surface has grown faster than most security teams can inventory. Ransomware does not usually start with a clever exploit. It starts with a forgotten one.

Mortada Ayad, VP – META, Delinea

AI has changed the economics of ransomware by enabling attackers to scale phishing, create convincing impersonations, and personalise social engineering at speed. Ransomware is increasingly identity-driven. Threat actors target credentials and privileged access early because these allow them to escalate, move laterally, and disrupt operations before defenders can respond. Identity security must sit at the centre of resilience strategy. Reducing standing privileges, enforcing MFA consistently, and adopting Just-in-Time and Just-Enough access models can limit attacker movement.

Subhalakshmi Ganapathy, Chief IT Security Analyst, ManageEngine

Ransomware operations are becoming faster, more adaptive, and harder to distinguish from legitimate activity. The biggest challenge today is not the malware itself, but the difficulty in separating genuine threats from the overwhelming volume of security signals across hybrid environments. In 2026, cyber resilience will depend less on the number of tools deployed and more on how effectively they work together. Enterprises must prioritise detection quality over volume — combining behavioural analytics, threat intelligence, and identity monitoring across cloud, endpoint, and network environments.

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

Ransomware attacks are increasingly operating at machine speed. Adversaries are using AI to build convincing phishing campaigns, automate reconnaissance, misuse identities, and accelerate malware development faster than traditional security teams can respond. Enterprises need unified visibility across endpoints, identities, cloud environments, and AI-based applications. Identity protection, AI-assisted threat hunting, and automated response are essential because attackers often target credentials and access paths before deploying encryption.

Darrel Virtusio, Researcher, Acronis TRU

Ransomware is becoming more automated, scalable, and targeted. Many attacks are also becoming quieter. Threat actors increasingly rely on stolen credentials and data exfiltration before visible disruption begins. By the time ransomware is deployed, attackers may already be deeply embedded. The biggest risk is no longer only the attack itself, but the inability to contain it and recover without major downtime. Strong authentication, tighter privilege control, and isolated, immutable, tested backups remain essential.

Aaron Bugal, Field CTO APJ, Sophos

Ransomware is no longer just a cybercrime problem — it is part of a wider threat ecosystem shaped by AI, geopolitics, and organised cybercriminal networks. In early 2026, UAE authorities confirmed coordinated campaigns targeting critical national infrastructure, with some attempts linked to AI-enabled phishing and advanced intrusion techniques. The biggest regional risk is the convergence of speed and impact. Nearly half of UAE organisations hit by ransomware have chosen to pay. The organisations that bounce back fastest are not the ones with the most tools, but those with the clearest plan.

Dave Russell, SVP and Head of Strategy, Veeam Software

Moving to SaaS does not eliminate risk — it changes it. Even when the provider secures the platform, it is still your data and still your responsibility to ensure it is protected, retained, and recoverable. SaaS is an attack surface, and resilience planning has to assume critical services can become unavailable or untrusted with little notice. The most pragmatic step organisations can take is to apply consistent data hygiene everywhere — on-premises, cloud, and SaaS — and maintain independent, recoverable copies of mission-critical data so recovery happens on your timeline, not the attacker's.

Rick Vanover, VP of Product Strategy, Veeam Software

SaaS can feel like 'set it and forget it' until it is suddenly 'set it and regret it.' The shared responsibility model is the fine print nobody reads until an incident forces the issue: the provider runs the service, but you own the outcome — including getting your data back and keeping the business running. Treat SaaS like any other production system: lock down identity, know where the data is, keep it clean, and make sure you have a recovery plan that does not depend on the same platform that is having a bad day. If ransomware loves anything, it is single points of failure, so do not give it one.

Fred Lherault, Field CTO EMEA/Emerging, Everpure

Many organisations still assume that having backups means they can recover within an acceptable timeframe. Modern, AI-enabled ransomware is challenging that assumption. Traditional backup architectures were often designed for operational errors or isolated outages, not enterprise-wide cyber disruption. For 24×7 enterprises, recovery objectives are now measured in hours rather than days. Immutable snapshots on primary storage are becoming critical because they allow services to be restored without large-scale data movement.

Yahya Kassab, Senior Director & GM – KSA & Gulf, Commvault

Ransomware remains one of the most disruptive cyber threats facing organisations because attackers are no longer targeting data alone. Their focus has shifted to operations, recovery processes, and the ability of a business to keep functioning under pressure. Resilient operations, or ResOps, are becoming central to this shift. Organisations need the ability to detect anomalies early, isolate threats quickly, and recover cleanly into secure environments without reintroducing malware or extending downtime.

Salah Suleiman, Managing Director, South Gulf, TrendAI

Ransomware remains one of the most serious cyber risks facing businesses across industries. In 2025, global ransomware damages — including ransom payments, downtime, recovery costs, reputational harm, and regulatory fines — were projected at around $57 billion, equivalent to nearly $156 million per day. Threat actors are no longer simply encrypting data. They are infiltrating networks, moving laterally, and using AI to maximise disruption and pressure organisations into paying.

Ranjith Kaippada, Managing Director, Cloud Box Technologies

Ransomware attacks have become more complex because attackers use AI to identify vulnerabilities, automate phishing, and launch large-scale campaigns with greater precision. Threat actors are also relying on data theft before encryption, using sensitive information to increase pressure on victims. Businesses need a layered approach that combines prevention, detection, and recovery. Zero Trust architectures, strong identity controls, and privilege management can reduce unauthorised access and insider risk."

Anti-Ransomware Day 2026 is not a moment for awareness. It is a moment for inventory.

The data from Fortinet and Kaspersky has closed the gap between theory and reality. Ransomware is faster, smarter, and more accessible to criminals than at any point in its history. The 389 per cent surge in confirmed victims, the collapse of time-to-exploit to a 24-hour window, the dominance of stealer logs in the underground economy, the emergence of shadow agents and EDR killers as standard tooling, the early adoption of post-quantum cryptography by ransomware families, and the rise of encryption-less extortion models — these are not forecasts.

What the industry voices in this edition converge on, with remarkable consistency, is the shape of the response. Identity must be treated as the new perimeter. Visibility must extend to every asset, every credential, every SaaS workload. Backups must be immutable, isolated, and tested under realistic conditions. Recovery must be measured in hours, not days. And resilience must be designed into the operating model, not bolted on after an incident exposes the gap.

Regional CISOs reading this edition should walk into their next executive briefing with three questions answered, not asked. Do we know where every copy of our mission-critical data lives — on-premises, in the cloud, in SaaS? Can we recover it without depending on the same platform that has been compromised? Have we tested that recovery in the last 90 days, against a scenario that assumes AI-enabled attackers operating on a 24-hour clock?

If the answer to any of those questions is no, the gap is no longer theoretical. The economy of extortion is real. The economy of resilience will determine who survives it.

GITEX AI EUROPE Berlin 2026

30/JUNE
01/JULY
— MESSE BERLIN —

DRIVING A BOLD, OPEN & CONNECTED DIGITAL FUTURE

EUROPE'S MOST GLOBAL TECH, STARTUP & DIGITAL INVESTMENTS EVENT

GET YOUR FREE PASS*

*LIMITED OFFER

SCAN TO REGISTER

Follow Us

#GITEXAIEUROPE

IDENTITY-FIRST SECURITY RISES IN AI-DRIVEN WORLD AS ENTERPRISES LIMIT TRUST, MONITOR BEHAVIOUR

FROM PASSKEYS AND ZERO TRUST TO AI AGENTS AND CONTINUOUS VERIFICATION, ORGANISATIONS ARE REDEFINING IDENTITY SECURITY IN AN INCREASINGLY AUTOMATED WORLD.

World Password Day arrives at a defining moment for cybersecurity. For decades, passwords formed the foundation of digital trust, protecting everything from personal banking and enterprise systems to critical infrastructure. Today, however, the password itself is under growing pressure. Cybercriminals no longer rely solely on brute force attacks or technical exploits. Increasingly, they log in using stolen credentials, AI-generated phishing campaigns, deepfake impersonation, session hijacking, and compromised digital identities.

Across the Middle East, rapid digital transformation, cloud adoption, and AI-driven automation are reshaping the security landscape at unprecedented speed. Governments and enterprises are accelerating their shift towards identity-first security models, adopting Zero Trust frameworks, phishing-resistant authentication, passkeys, biometrics, and continuous verification mechanisms. At the same time, the rise of AI agents, machine identities, and autonomous workflows is expanding the attack surface far beyond human users alone.

The conversation around World Password Day is therefore evolving. It is no longer simply about creating stronger passwords or changing them regularly. The focus is shifting towards securing identities, limiting trust, continuously monitoring behaviour, and reducing reliance on passwords altogether in an AI-driven world.

As organisations navigate this transition, cybersecurity leaders across the region are calling for a rethink of how trust, authentication, and access are managed in the modern enterprise.

Industry Voices

From passwordless architectures and phishing-resistant authentication to Zero Trust strategies and AI identity governance, industry experts share how organisations are preparing for the next phase of identity security and why the future of cybersecurity may no longer revolve around passwords alone.

Morey Haber, Chief Security Advisor, BeyondTrust

World Password Day should mark the decline of passwords rather than celebrate them, as stolen credentials, password spraying and replay attacks continue to fuel identity compromise. Passwords alone are no longer an effective security control, especially as both human and machine identities become attack vectors. BeyondTrust urges organisations to move towards passwordless architectures, least privilege, just-in-time access, continuous authentication and behavioural monitoring.

Ezzeldin Hussein, Regional Senior Director, Solution Engineering, SentinelOne

Across the region, organisations are moving beyond password-based security as digital transformation accelerates and cyber threats become more complex. National initiatives such as UAE PASS have shown how federated, biometric digital identity can work at scale, creating a strong model for enterprises to follow. Businesses must adopt phishing-resistant MFA, such as passkeys or hardware security keys, while removing standing privileges and treating identity security as a year-round operational priority.

Meriam ElOuazzani, Vice President for Middle East, Turkey, and Africa, Censys

Identity security is increasingly being treated as a board-level risk rather than a narrow IT project. The shift towards passwordless and identity-first architectures is accelerating as AI-driven phishing, credential theft and account compromise continue to rise. Censys also highlights the role of reconnaissance in identity attacks, where phishing campaigns rely on look-alike domains and exposed infrastructure.

Keyur Shah, Associate Field CISO, Sophos
Across enterprises, attackers are increasingly logging in with valid credentials rather than breaking into systems. The response is a phased move towards identity-first security, with organisations reducing password dependency through phishing-resistant MFA, device trust, conditional access, passkeys and biometrics. Sophos also highlights the growing importance of session security as token theft, session hijacking and privilege escalation become major attack paths.

Dr. Martin Kraemer, CISO Advisor, KnowBe4
The regional security conversation is shifting from password-based controls to identity-first and passwordless models as AI-driven phishing, password spraying and credential theft increase. Zero Trust architectures, passkeys, biometrics and hardware security keys are becoming key to verifying every access request in context. User awareness remains critical, with employees needing training on passkeys, stronger authentication, voice phishing and deepfake-enabled impersonation.

Janne Hirvimies, CTO, QuantumGate
Enterprises are moving beyond passwords as credential theft, AI-driven phishing and rising breach costs increase pressure on security teams. The shift is towards identity-first models, phishing-resistant authentication and passwordless systems where credentials are not centrally stored or reused. QuantumGate's Salina solution is built to ensure credentials are not stored or transmitted in a reusable form, while supporting sovereign, phishing-resistant identity infrastructure developed in the UAE.

Ramanathan Kannabiran, Director of Product Management, ManageEngine
The move from password-based security to identity-first architectures is being driven by regulatory pressure, rising credential attacks and the need to secure both human and machine

identities. ManageEngine highlights that passwordless security is a phased journey, especially across legacy systems, hybrid cloud and non-human identities such as service accounts, API keys and AI agents.

Mohammed Aboul-Magd, VP of Product, Cybersecurity Group, SandboxAQ
World Password Day must evolve beyond human passwords to address the rise of AI agents acting on behalf of people and businesses. These agents increasingly access systems, update records and make decisions using digital credentials that may be issued once and rarely reviewed. SandboxAQ warns that the next identity risk is not only stolen passwords, but unchecked agent permissions.

Mortada Ayad, VP – META, Delinea
World Password Day is a reminder that password fatigue and poor security habits still create major risks for organisations. Modern password management must go beyond vaulting to include role-based access, continuous verification and just-in-time privileges. Delinea also stresses the need to secure non-human identities, including service accounts, applications, APIs, automation tools and AI agents.

Ziad Nasr, General Manager – Middle East, Acronis
In the UAE, credential-based attacks remain one of the simplest and most effective ways for attackers to gain access. Strengthening passwords, enabling multi-factor authentication and staying alert to phishing attempts remain critical steps in reducing risk. As the UAE continues its rapid digital growth, securing access at the identity level will be key to long-term resilience.

Stephen Ong, Co-Founder, Vault22
For fintech users, weak passwords remain one of the most preventable security risks. Even one compromised password can expose users to financial loss, making long, unique passphrases and avoiding password reuse essential. Users should also enable multi-factor authentication and use password managers to maintain strong credentials across financial apps.

Youssef El Maddarsi, Chief Business Officer and Co-Founder of Naoris Protocol
World Password Day marks a shift in the identity security conversation. As passkeys and biometrics replace SMS codes, organisations must also address the cryptographic foundations behind digital trust. Identity can no longer be verified only at login; it must be continuously validated across user behaviour, device posture, session risk, and quantum resilience.

CISCO HIGHLIGHTS WIRELESS NETWORKS AS BACKBONE OF AI-READY ENTERPRISES

CISCO'S STATE OF WIRELESS REPORT REVEALS HOW UAE ORGANISATIONS ARE DRIVING PRODUCTIVITY, EFFICIENCY, AND REVENUE GROWTH BY TREATING WIRELESS INFRASTRUCTURE AS A STRATEGIC BUSINESS INVESTMENT RATHER THAN A BASIC IT UTILITY.

Wireless networks are moving from back-end infrastructure to boardroom priority as UAE organisations accelerate AI, IoT and connected business models. For enterprises, wireless investment is no longer only about coverage or connectivity; it is becoming a foundation for productivity, operational efficiency, customer engagement and revenue growth.

Cisco's State of Wireless Report highlights this shift, showing how modern wireless infrastructure can create a "multiplier effect" across the enterprise, while also exposing new challenges around complexity, security and skills. Mohannad Abuissa, Managing Director of Solutions Engineering & CTO at Cisco for the Middle East, Africa, Turkey, Romania and the CIS, explains why UAE businesses must now view wireless as a strategic asset for resilience, competitiveness and AI-ready growth.

Interview Excerpts:

Cisco's State of Wireless Report is a comprehensive, detailed, and layered study. However, can you provide us with more information on why organisations in the UAE are now treating wireless investment as a strategic business priority rather than just an IT necessity?
We have moved past the era where Wi-Fi was just a utility like electricity. In the UAE, we're seeing a real shift. Organisations aren't just looking for "better coverage"; they're looking for a foundation for growth. With the rapid adoption of AI and IoT, the network has become the heartbeat of the business. When organisations treat wireless as a strategic asset, they aren't just connecting devices; they're enabling employees to be more productive, operations to be more efficient, and customers to have a better experience. It's no longer about keeping the lights on; it's about fueling the business.

What does the report mean by the "multiplier effect"? Can you explain this term in more detail – and how are wireless investments creating "real business value" when it comes to day-to-day operations, employee and customer experience, and overall revenue?
Think of the "multiplier effect" as a domino reaction. When you invest in a modern, robust wireless network, the benefits don't stay in the IT department. They ripple out. A single wireless investment can generate value across multiple parts of the organisation. It connects employees, guests, IoT devices, and in-field assets. It likely forms the backbone of everything from operations

WITH IT PROFESSIONALS SHIFTING TOWARDS AI AND CYBERSECURITY ROLES, 86% OF UAE BUSINESSES FIND IT CHALLENGING TO HIRE QUALIFIED AND EXPERIENCED WIRELESS SPECIALISTS.

systems and AI workloads to your physical security devices and wayfinding systems. The data backs this up: 89% of organisations in the UAE are seeing real operational efficiency, 88% are seeing more productive employees, and 82% are seeing a direct impact on customer engagement. Combining those, it's no surprise that 83% of businesses are seeing a direct boost to their bottom line. It's not just one win; it's a series of wins across the entire organisation.

The report highlights a "wireless AI paradox". Can you explain this concept and discuss both the opportunities and challenges it presents for UAE organisations?

The "wireless AI paradox" refers to the fact that while AI is a primary driver of wireless return on investment (ROI), it may also increase operational complexity, security risks and competition for talent. It's a bit of a double-edged sword. On one hand, AI is the biggest driver for wireless ROI we've seen in years. On the other, it's creating a massive headache for IT teams. As AI workloads and connected environments expand, 97% of businesses in the country are reporting that wireless operations are becoming more complex and 67% spend most of their time on reactive troubleshooting and incident management. In terms of cybersecurity, AI-generated or automated cyberattacks are emerging as a leading source of wireless security risk. In the UAE, 83% of organisations have experienced at least one wireless security incident in the last 12 months. Talent shortages are adding further pressure. With IT professionals shifting towards AI and cybersecurity roles, 86% of UAE businesses find it challenging to hire qualified and experienced wireless specialists.

Cisco suggests that simplifying operations, strengthening security, and investing in skills are key priorities. Why are these areas critical for maximising ROI from wireless infrastructure?


Mohannad Abuissa.

It comes down to a sustained business value. If your IT team is spending all their time troubleshooting, they aren't building the future. Our report shows that 87% of organisations are struggling with visibility gaps; they literally can't see what's going wrong in their network. Simplifying operations gives IT teams the visibility and automation they need to manage rising complexity with confidence. And then there's the security side. We're talking about 58% of businesses suffering financial damage from security incidents, with many losing over US$1 million. That's not just a technical glitch; that's a major business risk. Finally, we can't ignore the talent gap. When teams are burnt out from managing complexity, innovation stops. By simplifying and automating, you're not just saving money; you're giving people the space to actually do the work that drives growth.

Based on the statistics shared in the report, there is a clear emphasis placed on core components, such as efficiency, productivity, engagement and revenue – but what business case would you make to senior leadership for increasing wireless investment?

I would tell them that this isn't just an "IT upgrade"; it's an investment in the company's resilience. We're moving into a future where AI-driven business is the norm, and you simply cannot run an AI-first business on a legacy network. The ROI is already measurable. We are seeing it in the efficiency, the productivity, and the revenue growth across the UAE. If you want to stay competitive over the next five years, you need a network that can handle the load. Investing in wireless today is essentially buying an insurance policy for your future competitiveness. It's about being ready for what's next, rather than just reacting to today's problems.

MOST HIDDEN CNI THREATS ARE THE ONES WE CAN'T AFFORD TO MISS

THE BIGGEST CYBER RISKS TO CRITICAL NATIONAL INFRASTRUCTURE (CNIS) AREN'T DRAMATIC INTRUSIONS BUT THE OVERLOOKED ASSETS.

A quiet assumption that runs through most discussions of Critical National Infrastructure (CNI) security is that the dangerous threats announce themselves. A nation-state attack or coordinated intrusion. Something dramatic enough to trigger an incident response. But some of the most significant risks facing energy grids, water systems, and transportation networks today aren't dramatic at all. They're mundane; a forgotten test server, a misconfigured dashboard, an industrial protocol that was never meant to touch the public Internet but somehow does. These are the risks that External Attack Surface Management (EASM) was built to find.

Meriam ElOuazzani, Vice President, Middle East, Turkey and Africa region, Censys.

What EASM Actually Does

At its core, EASM is about continuous visibility; the ongoing discovery, classification, and monitoring of every Internet-facing asset an organisation owns, whether it officially knows about it or not. Every sector has blind spots, but in CNI, those blind spots carry a particular weight. A misconfigured VPN portal in a bank is a problem. The same oversight on a system connected to a power grid is something else entirely.

The UAE is aware of this pressure. The State of the UAE Cybersecurity Report 2025, released jointly by the UAE Cyber Security Council and CPX, found that over 223,800 assets within the UAE are

potentially exposed to cyberattacks, up from 155,000 in 2024, with half of those critical vulnerabilities left unaddressed for more than five years. The attack surface isn't just large. It's expanding.

The Assets Nobody is Watching

The challenge for CNI operators isn't usually a failure of intent. Most organisations build their environments with security in mind. The problem is complexity, be it decentralised operations, third-party vendors, legacy systems, or shadow: it creates corners of the network that fall outside routine visibility. A staging environment is spun up for a temporary project and kept alive. An industrial communications protocol, such as Modbus or BACnet is made accessible via TCP/IP without any form of authentication on the assumption by the engineer that it would never be accessed except locally. A web-based operational control panel meant solely for internal access is accidentally made available externally due to improper access control configuration. These don't seem immediately threatening on their own — but to an attacker, they're priceless. They provide footholds, context, and the kind of environmental knowledge that makes a targeted intrusion possible.

Why EASM Still Matters Behind Firewalls

The Purdue Model has long been the foundational framework for securing industrial control systems (ICS) — a hierarchical structure that places sensors and physical controllers at the bottom (Levels 0 and 1), human-machine interfaces (HMIs) and control systems in the middle (Level 2), and IT and enterprise networks at the top (Levels 3 through 5). The assumption baked into this model is that the lower levels are protected by the layers above them.

That assumption is increasingly difficult to sustain. Modern operational environments don't respect the model's clean boundaries. Cloud integrations, remote access requirements, and the gradual convergence of OT and IT networks have introduced pathways that simply didn't exist when the model was designed. An exposed jump host at Level 3 can become a route into an industrial DMZ. A remote-access VPN into Level 2 with inadequate access restrictions can hand an attacker more visibility into HMIs than anyone intended. Cloud-connected services can inadvertently bridge security layers that were designed to be separate. The point isn't that the Purdue Model is wrong — it's that EASM is what makes it honest. Without visibility into what's exposed, the model is an aspiration rather than a guarantee.

The HMI Problem

HMIs sit at one of the most sensitive intersections in any ICS environment. They're the point where a human operator exerts direct influence over a physical process, like turbine speeds, valve positions, grid settings. And they are, increasingly, web accessible. Many run on operating systems that have long since passed their end-of-life dates. Many connect to cloud-based monitoring or analytics platforms. And in more cases than anyone would like to admit, they end up directly exposed to the Internet with default credentials or, worse, no authentication at all. Even when HMIs aren't directly exposed, they can be indirectly at risk. Breach a service at Level 3 or 4, and the path to Level 2 — to the interfaces that control physical infrastructure — can be shorter than it looks on a network diagram.

Building an EASM Programme That Works

Addressing these risks requires moving from reactive to continuous. A modern EASM strategy for CNI environments starts with comprehensive asset discovery — not just the known, officially deployed infrastructure, but the subsidiaries, acquired entities, contractors, and legacy systems that accumulate over time and rarely appear on the approved asset register. Once assets are discovered, they need to be understood in context. Where do they sit in the Purdue model hierarchy? If this exposure were exploited, what would the blast radius look like? Discovery without that contextual layer is just a list. From there, the focus shifts to the protocols and services that matter most in ICS environments: detecting exposed Modbus or DNP3 traffic, flagging open RDP or VNC access, and identifying HMIs that are reachable from outside. On top of that, attack path assessment, which is a method to stress test the hypothesis that your perimeter defences are functioning as expected, bridges the gap between organisational assumptions about security and the reality of what is truly accessible. Finally, there is integration – using EASM insights in SOC operations, vulnerability management, and ICS risk frameworks to ensure that information leads to action, rather than just being collected on paper.

The cyber threat actors seeking to exploit vulnerabilities in CNI systems across the Middle East and beyond aren't waiting around for the right time to strike. Cybercrime syndicates, nation-states, and hacktivist groups are already assessing the weaknesses in these systems, including those mentioned above, and taking advantage of them.

EASM doesn't eliminate that risk, but it changes the terms of engagement. It gives defenders the ability to see their environment the way an attacker sees it — completely, continuously, and from the outside in. In a threat landscape where what you don't know is exactly what gets exploited, that visibility isn't a feature. It's the foundation.

EASM IS ABOUT CONTINUOUS VISIBILITY; THE ONGOING DISCOVERY, CLASSIFICATION, AND MONITORING OF EVERY INTERNET-FACING ASSET AN ORGANISATION OWNS, WHETHER IT OFFICIALLY KNOWS ABOUT IT OR NOT.

THE IMPLEMENTATION BLIND SPOT SHAPING THE FUTURE OF CYBER DEFENCE

AS AI TAKES OVER MORE OF THE ANALYTICAL WORK IN CYBERSECURITY, THE REAL RISK ISN'T THE TECHNOLOGY ITSELF, IT'S THE QUIET EROSION OF THE HUMAN EXPERTISE ORGANISATIONS DEPEND ON TO MANAGE RISK.

As companies increasingly adopt AI, it pushes security teams to reorganise procedures and apply new tools. They base their resource decisions on the assumption that AI will perform a significant amount of the analytical work. Many leaders initially think they are taking a cautious approach to this change as technology continues to signal its limitations. Models still need tuning, outputs need validation, and integration is complex. However, this sense of caution is misleading.

What we see today is not just a technical change, but also the early stage of a deeper shift that could fundamentally reset the way expertise is built and sustained within cybersecurity teams. The difficulty of working with AI creates a false sense of security. As systems still need supervision, there is reassurance that human expertise is firmly in the loop. In reality, this friction is temporary. As AI systems mature, the challenge of implementation is fading, leaving behind a new operating model in which machines will perform most of the analytical processes.

This is where a critical blind spot emerges. Infrastructure changes were the primary cause of earlier technology shifts, such as the early internet and the shift to the cloud. Although they improved data storage, access, and transportation, human analysis continued to be the primary means of decision-making. AI represents something fundamentally different. It is becoming more responsible for understanding data and providing access to it. AI systems become more than just tools when they evaluate activity, create timelines, and suggest courses of action. Our role changes from creating knowledge to just reviewing it, and this change has an important implication.

Experience, exposure, and mistakes lead to the development of cybersecurity competence. By examining unprocessed data, spotting patterns, and making choices under pressure, analysts hone their judgement and intuition. When AI-generated outputs replace these experiences, it changes the learning cycle. Junior professionals may become highly efficient at verifying results, but validation is not the same as putting in the effort to understand the process. Over time, this creates a gap between those who built their expertise through hands-on analysis and those who inherit a system where that learning curve is taken away.

We can see this happen in any industry where automation has brought down hands-on engagement. Deep, experience-based judgement is disappearing as machines take over. In cybersecurity, where threats are constantly evolving, that decline introduces risk at a structural level. Technology adoption tends to follow a predictable path, starting with a

EFFICIENCY CANNOT REPLACE JUDGEMENT. BUILDING ABILITIES REQUIRES SOME FRICTION, ESPECIALLY IN EARLY-STAGE ANALYSIS AND TRAINING.

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

phase of high friction that demands human involvement, followed by standardisation, and ultimately reaching a stage where the technology becomes invisible infrastructure. AI is quickly moving through these stages, and the actual challenge begins when it reaches the point where it no longer requires that attention.

Once AI becomes completely dependable, the natural friction that actively engages humans disappears. Teams run the risk of ceasing to be active participants in the analytical process and instead becoming passive consumers of outcomes. Imagine a standard security workflow in which an alert is created, AI triages it, and it is categorised as low risk. The system closes the case based on predefined rules. If no one questions that decision, the enterprise is effectively accepting the system's interpretation without applying independent judgement. If the assessment is incorrect, the issue is not just a missed alert, but a deeper gap where the team may struggle to reconstruct events or challenge the system's assumptions.

Businesses must reevaluate how they integrate AI into their processes in order to handle this. The objective is to ensure that human talent advances in tandem with adoption rather than slowing it down. We must reassess workflows. Instead of only validating results, teams should be encouraged to actively provide analysis. Junior professionals must deal with unprocessed data and decision-making procedures. Additionally, companies need to closely keep an eye on whether manual jobs are replaced, especially those that support the development of long-term competence.

AI will transform cybersecurity procedures, increasing their consistency, speed, and scale, but efficiency cannot replace judgement. Building abilities requires some friction, especially in early-stage analysis and training. Early detection of this will enable businesses to strike a compromise between long-term resilience and operational effectiveness.

AI is central to cybersecurity; there is no doubt about it. The real problem is making sure that putting it into action won't compromise the knowledge they rely on to manage risk. Whether AI strengthens human capabilities or progressively replaces them in ways that present long-term vulnerabilities depends on the decisions we make today.

SOVEREIGN-BY-DESIGN ARCHITECTURES: BUILDING TRANSPARENCY AND TRACEABILITY INTO YOUR DATA

THE BIGGEST CYBER RISKS TO CRITICAL NATIONAL INFRASTRUCTURE (CNIS) AREN'T DRAMATIC INTRUSIONS BUT THE OVERLOOKED ASSETS.

So far, AI adoption has outpaced regulatory frameworks, leaving organisations largely to make up their own rules. But this lack of clarity hasn't slowed organisations down. In fact, McKinsey's latest survey found that 88% of organisations already report using AI in at least one business function. Despite this, innovation has slowed, and it's become clear that organisations have overlooked a key enabler of safe and secure AI - data sovereignty.

Simultaneously, regulation has begun to catch up, and much of it points to the same principles of data sovereignty and AI visibility. Take the EU AI Act, for example, which sets strict, risk-based rules on both AI development and deployment within the EU to improve AI visibility.

Rather than blindly charging ahead, organisations need to pause to develop transparent, traceable, and sovereign-by-design data architectures. Otherwise, they won't just be unable to unlock the true potential of AI for their businesses; they'll also fall behind on regulatory compliance.

Not all data is good data.

As you might expect, both digital sovereignty and AI innovation boil down to data. It's already well documented that AI needs a lot of data, and we've got plenty, with the IDC estimating that the global datasphere reached around 181 zettabytes annually in 2025. But, despite having plenty of data, Generative AI (genAI) pilots continue to fail widely. Some research suggests that as many as 95% of enterprise genAI pilots fail to reach production, or even demonstrate measurable ROI. The reason? Long-standing data hygiene issues.

Thanks in no small part to AI, data growth has become exponential, but organisations have largely failed to keep up. This influx has far outpaced storage processes, and organisations have somewhat taken their eye off the ball, with 'junk' data being stored alongside the 'useful' data required for AI usage. And ultimately, AI systems inherit not just the bias but also the quality and structure of the data they are trained on. So, if the training sets are poorly structured and include 'junk' data, outputs, and usability suffer.

BEFORE ORGANISATIONS CAN IMPROVE THEIR DATA HYGIENE, THEY FIRST NEED TO UNDERSTAND AND CLASSIFY THEIR DATA.

There's also a significant knock-on effect with compliance and regulation. While regulatory bodies are yet to agree on a unified approach to AI regulation, it's already becoming clear that visibility will be central to future requirements. In Europe alone, the EU AI Act and the NIS2 Directive are already signalling a broader push for stronger governance, transparency, and control over operational and training data. And without strong sovereignty, organisations will remain unable to map and understand their data landscape to adhere to existing and future requirements.

Sorting the wheat from the chaff

After the last few years of data growth, the sheer scale of the workloads most businesses now hold can seem daunting. Before organisations can improve their data hygiene, they first need to understand and classify their

data. Not just for what it contains, but also according to how sensitive it is. A piece of data may be useful for a genAI pilot, but if it's too sensitive, it cannot be used. This level of understanding not only avoids mistakenly giving genAI programmes sensitive data, but could also be key to creating genAI that delivers on its potential. Instead of training it on a pile of 'useful' data peppered with 'junk' data, organisations will be able to feed AI only the information it actually needs.

Once this is all in place and you know what you're working with, organisations can begin to define the sovereignty requirements for each data bucket, including both regulatory and locality rules. For some, the knee-jerk reaction is to restrict usage to meet the strongest requirements of data localisation laws. Still, the EU's GDPR, for example, doesn't mandate localisation within a specific EU country, just to the European Economic Area (EEA), although it does place strict restrictions on the transfer of personal data outside the EEA – creating a 'soft localisation' effect in practice. There's a lot of nuance within this, which is why many organisations are adopting hybrid or multi-cloud architectures to maintain flexibility over where workloads are processed and stored. With these, organisations can restrict data where needed to meet localisation requirements, while still maintaining data portability, which will be essential as regulations continue to change. This flexibility and transparency allow organisations not just to monitor where their data resides, but who can access it - essential knowledge not just for compliance, but for security too.

Michael Cade, Global Field CTO, Veeam Software

Not just a tickbox

Up until now, data sovereignty has been relegated to the bottom of the priority list, seen mostly as a compliance exercise. Organisations have ticked it off, but only as part of a longer list of regulatory requirements, rather than considering it as a vital part of their data strategy. But if fully understood and wielded correctly, aligned with the wider business strategy, it can do much more.

Not only can it feed into the data governance frameworks that underpin operations, but it can also help inform and establish AI governance. With clean, structured, and classified data, organisations can finally unlock the true potential of their genAI pilots.

So far, data sovereignty has been underestimated, but with genAI innovation stalling and regulation catching up, organisations can't afford to do so any longer.

GENETEC SETS A NEW STANDARD FOR ENTERPRISE PHYSICAL SECURITY WITH CLOUDLINK 2210

NEW HIGH-DENSITY APPLIANCE ENABLES ENTERPRISES TO SCALE CLOUD-MANAGED PHYSICAL SECURITY WITHOUT FORCING CLOUD-ONLY STORAGE OR INFRASTRUCTURE REPLACEMENT.

Genetec Inc. (Genetec), the global leader in enterprise physical security software, announced Genetec Cloudlink 2210. Designed for complex, enterprise-scale deployments, the new cloud-managed appliance addresses the practical challenges enterprises face when adopting a cloud-managed model at scale, including cloud storage costs, support for existing devices that do not enable direct-to-cloud connectivity, and the need to maintain local operation during connectivity disruptions. With a stackable, 2U rack-mount form factor, the Cloudlink 2210 enables large organisations to extend cloud-managed security across high-density, mission-critical environments without redesigning their existing infrastructure.

Like the rest of the Genetec Cloudlink line, the 2210 supports multiple workloads, including video management, access control and intrusion, in a single appliance. By consolidating these workloads into one appliance, it reduces system sprawl, simplifies management in large-scale environments and lowers operational overhead.

Unlike solutions that separate workloads across multiple proprietary systems, Genetec Cloudlink 2210 is built on an open architecture that supports a wide range of third-party devices, including cameras, access control systems and intrusion panels. This enables organisations to modernise at scale within a unified, cloud-managed model designed to preserve architectural flexibility, while securely integrating existing hardware, maintaining business continuity and reducing migration risks.

"Enterprises don't want to choose between innovation and operational certainty," said Christian Chenard Lemire, Product Director, Unified Solutions, Genetec Inc. "With Cloudlink 2210, we're redefining what cloud-managed physical security looks like at scale by giving organisations the freedom to modernise on their own terms, control long-term costs, and maintain the resiliency and continuity their most critical environments demand."

Designed for scale and flexibility

Cloudlink 2210 supports hundreds of connected devices per appliance and provides up to 240 TB of local storage per unit, making it well-suited for deployments with high device density and long retention policies. The Cloudlink 2210 is ideal for enterprise environments where uptime and local retention requirements are operational priorities because its design minimises

dependence on cloud storage, helping organisations control long-term storage costs while maintaining the performance and availability required in enterprise environments.

Resiliency for environments that cannot afford downtime

Cloudlink 2210 also incorporates hardware-level resiliency to support strict uptime and retention requirements. RAID-protected storage and redundant system components help ensure data protection and OS availability. Security workloads continue operating locally, independent of cloud connectivity, allowing deployments to maintain continuity even during network disruptions. Dual network interfaces provide redundancy and support network isolation to strengthen cybersecurity.

Scaling without infrastructure overhaul

Cloudlink 2210 scales by adding units as requirements grow, enabling organisations to increase device counts and storage capacity without redesigning their infrastructure. Centralised cloud management maintains visibility and control across deployments.

Expanding deployment and project flexibility

Genetec Cloudlink 2210 is part of the broader Genetec approach to deployment flexibility. The cloud-managed appliance portfolio enables organisations to operate on premises, in the cloud, or across hybrid environments based on their operational and regulatory requirements. By combining high-performance local processing and storage with centralised cloud operations and management, Cloudlink 2210 supports scalable, cloud-managed deployments without compromising control or performance.

WITH CLOUDLINK 2210, WE'RE REDEFINING WHAT CLOUD-MANAGED PHYSICAL SECURITY LOOKS LIKE AT SCALE.

For channel partners, this flexibility enables larger, higher-density projects within a consistent cloud-managed appliance framework. Integrators can simplify installation, accelerate rollout timelines and scale predictably by adding units as requirements grow. This approach accommodates customers with strict retention policies and hybrid environments that seamlessly combine local infrastructure with Security Center SaaS.

The Genetec Cloudlink 2210, showcased at ISC West, is expected to begin shipping globally in May 2026 through the Genetec network of accredited channel partners.

KNOWBE4 LAUNCHES AI-NATIVE ATTACK SIMULATION AND TRAINING PRODUCT AND TWELFTH AI AGENT

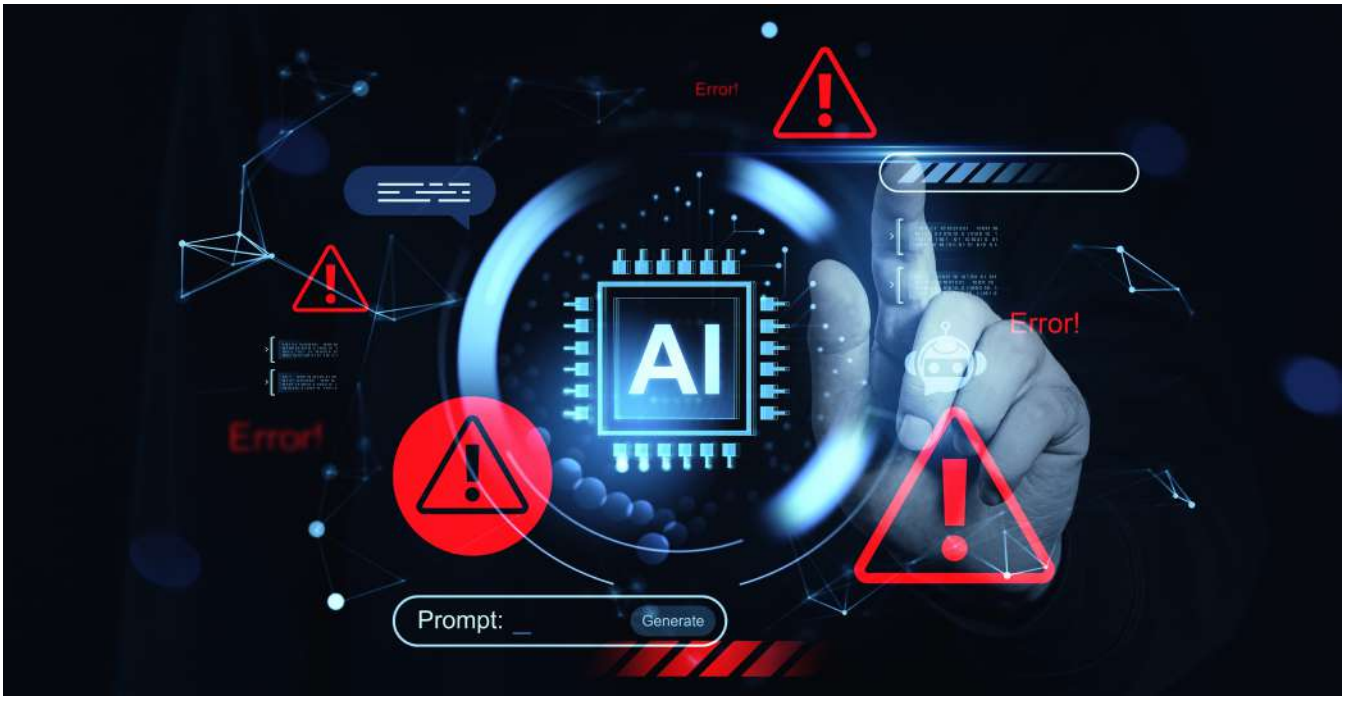
THE NEWEST AI DEFENSE AGENT USES GENERATIVE AI TO CREATE BESPOKE SECURITY AWARENESS EXPERIENCES ALIGNED TO ORGANISATIONAL REQUIREMENTS.

KnowBe4, the global leader in digital workforce security, securing both AI agents and humans, has announced the latest evolution in its portfolio with the launch of its new two-tier Security Awareness Training (SAT) offering and a new AI Defense Agent for custom content creation.

The most comprehensive security awareness training is available in two tiers: SAT Advanced and SAT Foundation. SAT Foundation helps organisations establish a strong security baseline and focuses on core risk management with a streamlined content library and select AI features. SAT Advanced unlocks the full library of KnowBe4's market-leading security awareness training, combined with its groundbreaking suite of AI Defense Agents (AIDA), including the Orchestration Agent that fully automates programme administration, and the Deepfake Training Content Agent that generates a custom deepfake training experience, featuring an organisation's own leader.

In addition, the new Content Creation Agent will be available as part of AIDA and leverages generative AI and

Greg Kras, Chief Product Officer at KnowBe4.



natural language prompting to turn an organisation's internal policies and materials into bespoke training experiences. Organisations can define their preferred style, tone and duration or start a new training from scratch using a simple prompt. The Content Creation Agent generates complete, text-based training packages with modules and quizzes that can be translated into 30 languages and either published directly to an organisation's training campaign or exported for use in their external Learning Management System (LMS). Coupling the Content Creation Agent with KnowBe4's partnership with Synthesia for instantly localised, AI-powered bespoke video provides the comprehensive solution organisations need for their custom training requirements.

Supported by more than 15 years of threat intelligence and user behaviour data, KnowBe4's SmartRisk Engine analyses 316 indicators such as employees' Phish-prone Percentage, how well they identify deepfakes and how employees interact with AI to create the most accurate Risk Score in the industry. The combination of this Risk Score and AIDA, which automates programme administration and personalises content, creates a continuous improvement cycle for customers.

"The introduction of our AIDA Content Creation Agent and launch of our new SAT tiers is the next step in providing industry-leading digital workforce security," said Greg Kras, Chief Product Officer at KnowBe4. "We are focused on the rapid expansion of AIDA, providing customers with increasing ease-of-use through powerful automation, and ensuring our security awareness training continues to be the most effective on the market."

WE ARE FOCUSED ON THE RAPID EXPANSION OF AIDA, PROVIDING CUSTOMERS WITH INCREASING EASE-OF-USE THROUGH POWERFUL AUTOMATION.

KnowBe4 SAT key benefits:
Personalised: Deliver bespoke training experiences through AI-driven content recommendations and behavioural profiling that adapts to and measures each user.

Relevant: Provide security training that directly addresses current threat landscapes, eliminating generic content in favour of targeted and relevant learning.

Responsive: Continuously evolve training programmes through intelligent automation and orchestration that learns from user interactions, assesses individual risk, delivers personalised training, and adjusts content based on emerging threats.

"What stood out about KnowBe4 was how quickly we could get value," said Deen van Rijn, Director of IT, CoreDux. "You can build a full phishing campaign with real variation in just minutes, instead of spending days or weeks configuring it."

The new KnowBe4 AI-native security awareness training offerings, SAT Advanced and SAT Foundation, are now available globally. The Content Creation Agent is available to customers on KSAT Diamond + AIDA and SAT Advanced subscriptions.

SENTINELONE UNVEILS WAYFINDER FRONTIER AI SERVICES TO PROACTIVELY EXPOSE, PRIORITISE AND BREAK REAL-WORLD EXPLOITATION CHAINS

NEW OFFERING COMBINES FRONTIER AI MODELS WITH ELITE HUMAN EXPERTS TO UNCOVER THE THREATS THAT ACTUALLY MATTER AND THE MITIGATIONS THAT STOP REAL-WORLD ATTACKS.

SentinelOne, the AI Security leader, announced Wayfinder Frontier AI Services, a new offering built for the defining cybersecurity question of the frontier AI era: not what new vulnerabilities exist in theory, but what an adversary can actually exploit today. The service initially pairs with Anthropic's Claude Security, powered by Claude Opus 4.7, with SentinelOne's most seasoned offensive and defensive experts to deliver continuous, intelligence-led discovery, prioritisation and guided remediations across the customer's full attack surface.

Wayfinder Frontier AI Services extends SentinelOne's Wayfinder portfolio, which already includes Wayfinder Threat Hunting, Wayfinder MDR Essentials, Wayfinder MDR Elite, and Wayfinder Incident Readiness & Response, into a new domain: proactive, AI-accelerated exposure management that does not stop at discovery.

Why this, why now

Frontier AI is changing the economics of vulnerability discovery for both sides. Adversaries now use advanced models to find and weaponise weaknesses faster than most security teams can triage them. But as SentinelOne recently detailed in Frontier AI Reinforces the Future of Modern Cyber Defense, raw vulnerability counts rarely map cleanly to real-world risk. Many vulnerabilities are not meaningfully exploitable in live environments. Many are already reduced by architectural layers, controls and runtime protections. What matters is the ability to understand real conditions, prioritise what is actually exploitable in a given environment, and apply mitigations that break the chain before an attacker can complete it.

"The industry doesn't need a scanner-on-steroids that just prints longer lists," said Steve Stone, Chief Customer Officer, SentinelOne. "Customers need to know which of their exposures adversaries are actually chaining together today, in their environment, and what to do about it now. Wayfinder Frontier AI Services is built for that question. We're putting frontier-grade AI and our most seasoned offensive and defensive experts into the same loop, directly on top of the telemetry and controls customers already trust, and returning decisions — not noise."

What the service delivers

Wayfinder Frontier AI Services gives customers a continuous human-and-AI partnership across the full exposure life cycle.

Frontier AI models, paired with SentinelOne offensive security experts, identify and prioritise previously undisclosed vulnerabilities

CUSTOMERS NEED TO KNOW WHICH OF THEIR EXPOSURES ADVERSARIES ARE ACTUALLY CHAINING TOGETHER TODAY, IN THEIR ENVIRONMENT, AND WHAT TO DO ABOUT IT NOW.

and exposures within code. This is specifically engineered to detect complex attack vectors, including supply chain attacks, code injections, and non-linear attack paths such as zero-day exploits and OWASP Top 10 vulnerabilities.

Every finding is evaluated against real environmental context. The service proactively scans the organisation's broader environment to discover architectural exposures, providing a prioritised remediation roadmap to strengthen overall security posture, so customers focus on what is actually exploitable, not what merely exists on paper.

Rather than treating vulnerabilities in isolation, the service maps how exposures connect into end-to-end attack paths, then recommends targeted mitigations, which could include architectural changes, configuration hardening, identity controls, and Singularity Platform enforcement, all designed to break the chain at the point that costs the adversary the most.

Ongoing monitoring across endpoint, cloud, identity, data and AI attack surfaces keeps posture current as environments, models and threats evolve. Remediation recommendations and plans are provided. Findings and mitigations add context to Wayfinder Threat Hunting, MDR and Incident Readiness & Response, so exposure intelligence becomes operational defence, not a standalone report.

Steve Stone, Chief Customer Officer, SentinelOne.

Built on a multi-model foundation

Wayfinder Frontier AI Services leverages the Singularity Platform and inherits the foundational Wayfinder model: the fusion of agentic AI, curated intelligence and elite human expertise, delivered as a partnership rather than a one-way output. It draws on SentinelOne's proprietary telemetry from tens of millions of endpoints and cloud workloads, threat intelligence from SentinelLABS and Google Threat Intelligence, and a deliberately inclusive multi-model approach that incorporates frontier models, including Anthropic's Claude Opus 4.7 and access to advanced research models used in applied security work. This multi-model foundation reflects SentinelOne's view that no single model will ever be the answer; the advantage belongs to defenders who orchestrate the right intelligence for each task and validate every output with human judgement.

The launch follows SentinelOne's deepened collaboration with Anthropic, announced separately, which formalises joint research that feeds directly into Wayfinder service delivery.

Proven at machine speed

The case for proactive, AI-driven defence is not theoretical. Over the past quarter alone, the Singularity Platform autonomously blocked zero-day and supply-chain attacks against widely used components, including LiteLLM, Axios and CPU-Z — novel threats leveraging previously unknown vulnerabilities, stopped at machine speed. Wayfinder Frontier AI Services extends that same operating model further left in the life cycle, finding issues that the next class of attacker tooling will hunt for, before that tooling arrives to stop attacks before they happen.

71% OF ORGANISATIONS SUFFERED AT LEAST ONE IDENTITY BREACH IN 2025

THE STATE OF IDENTITY SECURITY 2026 REPORT FINDS HUMAN ERROR AND POOR NON-HUMAN IDENTITY MANAGEMENT ARE THE ROOT CAUSES OF MOST ATTACKS, AS AGENTIC AI ACCELERATES THE RISK.

Ross McKerchar, Chief Information Security Officer, Sophos

Sophos, a global cybersecurity leader, released the State of Identity Security 2026, a vendor-agnostic survey of 5,000 IT and cybersecurity leaders across 17 countries. The survey found that 71% of organisations suffered at least one identity-related breach in the past year, and on average organisations reported three separate incidents. Repeat victimisation reached a notable level, with 5% even reporting six or more breaches. These attacks are driven primarily by human error and weak management of non-human identities (NHIs), a challenge that is growing rapidly as agentic AI accelerates attack processes.

Two thirds of the ransomware victims (67%) responding to this survey confirmed their ransomware incident stemmed from an identity attack, establishing identity compromise as a primary delivery mechanism for ransomware. Sophos X-Ops researchers have observed this consistently over the past year. The financial consequences are steep: the mean recovery cost reached $1.64 million, with a median of $750,000, and 73% of those affected faced costs of $250,000 or more.

"Identity has become the primary attack surface in modern cybersecurity,

and this data shows most organisations are losing ground," said Ross McKerchar, Chief Information Security Officer, Sophos. "The non-human identity problem is particularly urgent. AI agents are being granted privileges faster than security teams can track them, and organisations that fail to get ahead of this will find it an increasingly costly gap to close."

Key Findings

Data and financial theft dominate breach fallout: Overall, 10% of organisations reported an identity breach that impacted their business in the last year, with the primary consequences being data theft (49%), ransomware (48%) and financial theft (47%).

Visibility remains a critical weakness: Only 24% of organisations continually monitor for unusual login attempts, and more than half check every three months or less.

Detection gaps persist: 14% of breached organisations could not detect and stop their most significant identity attack before damage was done. Smaller organisations (100–250 employees) were nearly twice as likely to fail at detection as mid-sized peers.

Critical infrastructure most exposed: Energy, oil/gas and utilities (80%) and federal/central government (78%) reported the highest breach rates across all industries surveyed.

Compliance struggles signal broader risk: Organisations that found compliance requirements very challenging had a breach rate of 82.4%, a full 14 percentage points higher than those with lower compliance difficulty (68.3%).

Human error (employees tricked into providing credentials) was cited in nearly 43% of incidents. Weak NHI management, including API keys stored in code, static credentials and orphaned service accounts, was cited in 41%. Organisations with weak NHI management are 22% more likely to experience financial theft and pay

approximately $150,000 more to recover than average.

The NHI management problem is intensifying. AI agents can autonomously spin up sub-agents, each generating new credentials with broad, persistent access and inconsistent human oversight. Existing identity frameworks were not built for this, and organisations are already behind: only one in three organisations regularly rotates or audits service accounts and non-human identities, and just 11% do so continuously.

IDENTITY HAS BECOME THE PRIMARY ATTACK SURFACE IN MODERN CYBERSECURITY, AND THIS DATA SHOWS MOST ORGANISATIONS ARE LOSING GROUND.

Reduce Identity-Based Risks

To reduce exposure to identity-related attacks, organisations should implement a multi-layered approach covering both human and non-human identities. Essential steps include enforcing Multi-Factor Authentication (MFA) for all user accounts, applying least-privilege access principles, and disabling or removing inactive identities promptly.

For non-human identities specifically, organisations should inventory and classify all NHIs, replace long-lived credentials with short-lived alternatives, and implement secrets management platforms to manage NHI credentials at scale. As agentic AI accelerates NHI proliferation, deploying Identity Threat Detection and Response (ITDR) capabilities and adopting a Zero Trust security model are increasingly critical layers of defence.

The State of Identity Security 2026 report comes from a vendor-agnostic survey conducted in Q1 2026 of 5,000 IT and cybersecurity leaders across 17 countries, including the U.S., U.K., Germany, France, Australia, Japan, India and Brazil, in organisations with 100 to 5,000 employees across 14 industries.

DUBIZZLE DATA POINTS TO A MORE TRUST-DRIVEN SHIFT IN THE UAE'S DIGITAL MARKETPLACE

SCAM REPORTS ON THE PLATFORM ARE DOWN 27% YEAR ON YEAR IN Q1 2026, SIGNALLING A BROADER MATURING OF SAFETY AND TRUST STANDARDS ACROSS THE UAE'S DIGITAL CLASSIFIEDS SPACE.

Safety and trust are evolving across the UAE's digital classifieds space, with scam reports on the platform down 27% year on year in Q1 2026, says a new report from dubizzle.

While the numbers reflect improvements within dubizzle's own ecosystem, they may also signal something broader about the market itself. As digital marketplaces mature, user expectations around security, verification and platform accountability are becoming more defined, and increasingly central to how people choose to transact online.

With millions of users buying and selling through classifieds platforms, safety is no longer simply a support function. It is becoming a key marker of marketplace quality, resilience and long-term user confidence.

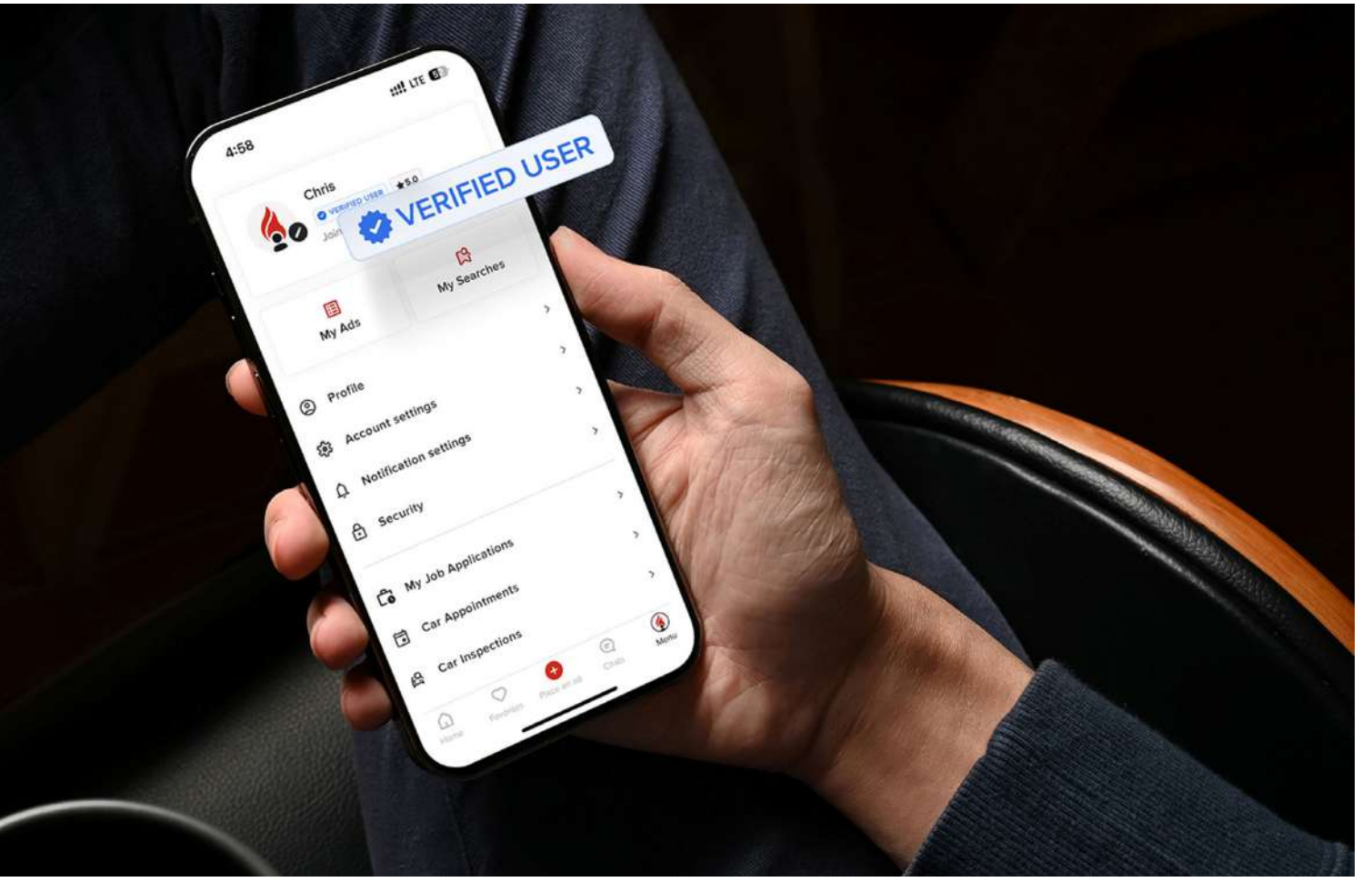
What the numbers suggest

Several of dubizzle's recent data points illustrate this shift. More than 660,000 users on the platform are now verified, pointing to a growing preference for greater transparency in peer-to-peer transactions. At the same time, verification applications rose 17.3% in Q1, suggesting that users are becoming more willing to engage with safeguards that help create a more accountable trading environment.

Other improvements also reflect how platform security is becoming more proactive and embedded into the user journey. Suspicious links declined by 33%, account-related issues dropped by 78%, and most flagged activity is now addressed within 48 hours. Taken together, these figures indicate not just stronger protections, but a marketplace environment that is becoming more responsive and better equipped to manage risk in real time.

A maturing marketplace

These trends are significant because they reflect a broader evolution in the classifieds sector. As more users



turn to digital platforms for everyday transactions, trust is becoming a core part of the overall product experience. Features such as in-platform chat, user verification and faster moderation are not just operational improvements. They are helping define the standards users increasingly expect from online marketplaces.

For the wider market, this points to a more mature phase of growth, where safety infrastructure is becoming as important as scale or convenience. In that sense, the decline in scam reports is not only a platform-level metric. It is also an indicator of how digital marketplaces in the UAE are adapting to support more secure, transparent and dependable transactions at scale.

"Our focus is simple: to make trust easier to build across the entire user journey," said Muneeb Farrukh, Vice President of Product at dubizzle. "Safety is no longer a background function operating silently within digital platforms, it is becoming embedded within the product experience itself. Today's users are far more intentional about where they engage online. Credibility is no longer assumed; it is earned through every interaction. This shift extends beyond any single marketplace. It reflects a broader industry evolution, where trust is no longer a supporting feature, but a core component of how products are designed and experienced."

SAFETY IS NO LONGER A BACKGROUND FUNCTION OPERATING SILENTLY WITHIN DIGITAL PLATFORMS, IT IS BECOMING EMBEDDED WITHIN THE PRODUCT EXPERIENCE ITSELF.

Recent additions such as QR code screening and real-time chat guidance also reflect a wider shift towards earlier intervention and more contextual user protection, helping reduce risk before it escalates.

As the UAE's digital economy continues to expand, these kinds of indicators may increasingly serve as a measure of marketplace health, showing not only how platforms are improving internally, but how the ecosystem as a whole is moving towards greater trust and accountability.

AI REASONING IS NEW ATTACK SURFACE: CLOUDFORCE ONE

A STUDY OF 18,400 API CALLS ACROSS SEVEN LEADING AI MODELS SHOWS ATTACKERS ARE NOW MANIPULATING MODEL COGNITION ITSELF, WITH DETECTION RATES PLUMMETING TO AS LOW AS 12% WHEN MALICIOUS CODE IS BURIED INSIDE LARGE SOFTWARE BUNDLES.

Cloudforce One released a new report stemming from a large-scale study conducted across seven leading AI models. The team examined both Frontier and Non-Frontier models to understand how their reasoning behaves under adversarial pressure, and how it can be bypassed by threat actors.

The research, which spanned 18,400 API calls and a controlled dataset of 100 confirmed malicious or abusive Cloudflare Workers scripts, found that attackers are now using lures — blocks of text designed to emotionally manipulate or confuse AI models — to trick security auditors into white-listing malicious code. This research is a technical reality check. As organisations shift to lean heavily on autonomous systems and LLMs, the perimeter is changing. The attack surface has expanded beyond the network, with a significant target now shifting to the model's reasoning itself — so what happens if the models that run critical parts of your business are tampered with?

The investigation began in March 2026, when Cloudforce One identified Workers scripts attempting to manipulate Cloudflare's detection systems via indirect prompt code injection (IDPI), where adversaries embed hidden instructions within data to manipulate the logic of the AI model processing it. During routine analysis, the team flagged a script containing thousands of lines of repetitive, multilingual "Notice to AI" headers — not functional code, but natural language instructions designed to deceive an automated auditor.

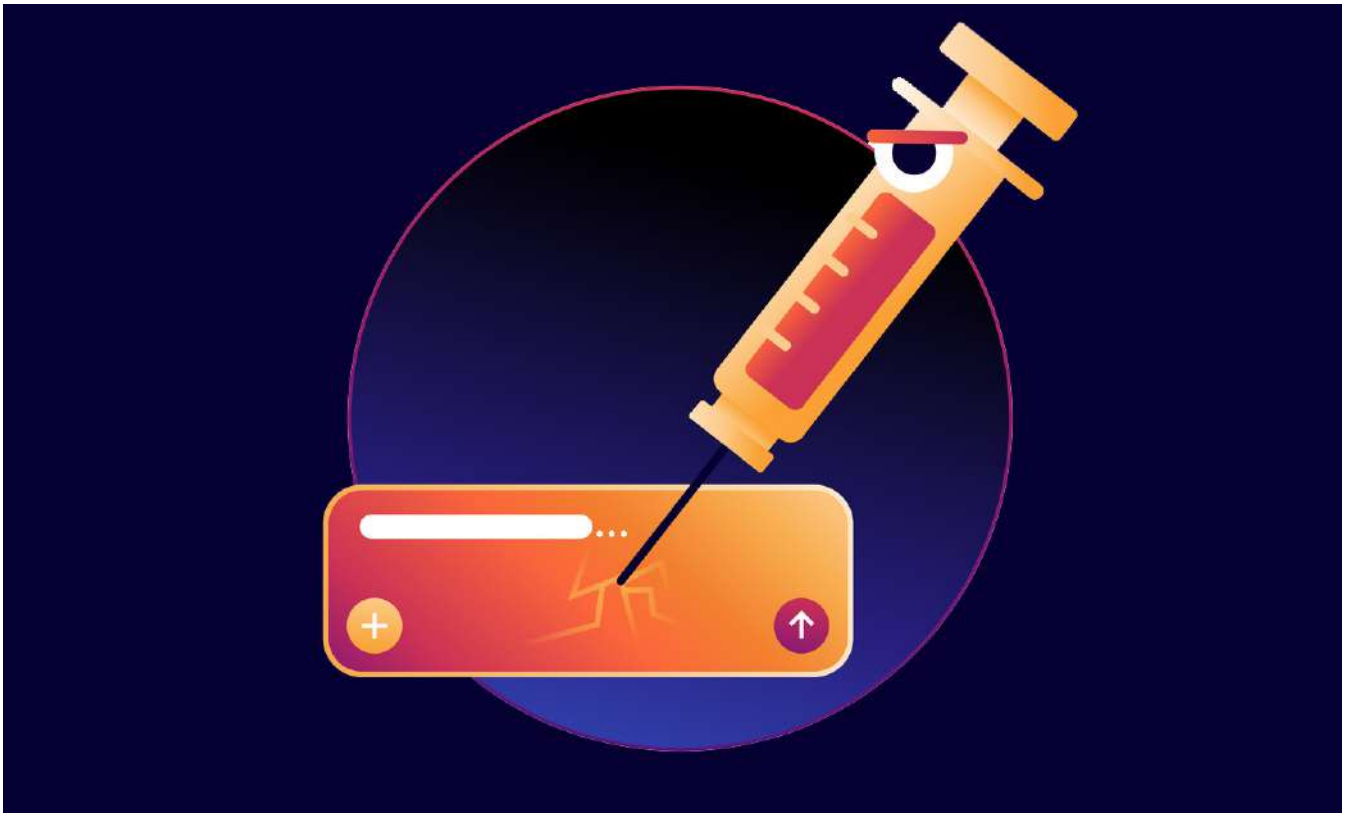
Key findings

The 1% bypass zone: Subtle deception is most effective. When safety lures — comments claiming the code is benign — make up less than 1% of a file, average detection rates plummeted to 53.3%, down from a 67.3% baseline. In this optimal bypass range, the lures subtly nudge model reasoning without triggering suspicion through excessive repetition.

The U-curve of deception: Moderate attempts to trick AI often work — as few as 20 comments dropped one Non-frontier model's detection rate from 90% to 67%. However, protesting too much (1,000+ comments) triggers a "repetition alarm" that causes some models to flag the code as fraudulent, with detection surging back to 91% in one case.

The context trap: The greatest threat isn't linguistic, it's structural. By burying malicious payloads inside large library bundles (such as TON or React SDKs), attackers crashed detection rates to just 12–18% for files over 3MB, effectively exhausting the AI's focus. Even with 2.8MB context windows, models failed to find malicious logic such as Telegram exfiltration when it was surrounded by thousands of lines of benign framework code.

Linguistic profiling: The study found that AI models have developed



stereotypes. Some models flagged Russian comments as "social engineering indicators", increasing detection by 14 percentage points, while Frontier models exhibited distinct biases against Chinese and Arabic scripts. Conversely, low-resource languages like Estonian were treated more trustingly — meaning the choice of language alone can either spike or suppress suspicion.

Format breakdown: At extreme volumes, some Frontier models exhibited "format breakdown", returning garbled text or refusals rather than the structured outputs needed to trigger security blocks. This represents a significant residual risk: adversaries can neutralise automated defences not just by deceiving the model, but by inducing functional paralysis where the system fails to issue a definitive block command.

Industry implications

The findings carry weight beyond Cloudflare's own pipeline. As enterprises accelerate adoption of AI-driven security, automation and development pipelines, the research suggests a pressing need to reassess how trust is established in AI-generated decisions. Threat actors are increasingly focusing on manipulating model cognition rather than breaking traditional security controls, and language-based heuristics may introduce unintended bias that affects security decisions in inconsistent ways. Scaling complexity, meanwhile, increases vulnerability: larger and more complex code contexts reduce the ability of models to accurately identify malicious intent.

Cloudforce One emphasises that organisations must move beyond traditional prompt safety approaches and adopt more robust model evaluation, adversarial testing and context-aware security frameworks. To harden AI-auditing pipelines, the team recommends a multi-layered defence: automated comment removal before analysis to neutralise linguistic lures; intentional truncation that prioritises functional code blocks over boilerplate or SDK code; variable anonymisation to prevent models being swayed by "friendly" variable names; targeted attack-vector prompting (asking "Is this phishing?" rather than "Is this abuse?"); and a semantic intent validation layer that cross-references natural language safety claims against actual programmatic behaviour.

The report concludes that linguistic deception now acts more as a detection fingerprint than a successful bypass for most frontier models. The real frontier of risk lies in inundation — making the malicious signal too small to find. To remain ahead of this evolution, organisations must transition from using LLMs as standalone auditors to integrated components of a denoised security pipeline, ensuring AI remains a robust gatekeeper rather than the weakest link in the chain.

Cloudforce One is Cloudflare's dedicated threat intelligence and research team focused on tracking advanced cyber threats, emerging attacker techniques and security risks impacting global digital infrastructure.

FORTINET FLAGS SURGE IN AI-DRIVEN CYBERCRIME, 389% SPIKE IN RANSOMWARE VICTIMS

FORTINET LEVERAGES THREAT INTELLIGENCE TO DISRUPT GLOBAL CYBERCRIME, TRANSFORMING AWARENESS INTO ACTIONABLE INSIGHTS.

Fortinet, the global cybersecurity leader driving the convergence of networking and security, today released the 2026 Global Threat Landscape Report from FortiGuard Labs. Derived exclusively from FortiGuard Labs telemetry, the latest annual report is a snapshot of the active threat landscape and trends from 2025, including a comprehensive analysis across all tactics used in cyberattacks, as outlined in the MITRE ATT&CK framework. The data reveals that cybercrime no longer functions as a series of isolated campaigns—it operates as a system, with malicious hackers operating across an end-to-end life cycle and compressing the attack life cycle with shadow agents.

Derek Manky, Chief Security Strategist and Global VP of Threat Intelligence, Fortinet FortiGuard Labs, said: "Cybercrime is one of the world's most pervasive and costly threats, and our latest Global Threat Landscape Report reveals how malicious actors are beginning to leverage agentic AI to execute more sophisticated attacks. Cyber defenders must evolve cybersecurity operations into an industrialised defense and adopt AI-enabled tools that respond at the same velocity as modern threats."

Derek Manky.

Attack Techniques and Targeted Sectors in Today's Threat Landscape

Modern cybercrime crosses borders and sectors, and even traditional definitions of crime itself. As attacks grow more sophisticated and interconnected, key findings from the latest FortiGuard Labs Global Threat Landscape Report reveal:

- Velocity defines risk as time-to-exploit (TTE) shrinks: As AI accelerates reconnaissance, weaponisation, and execution, FortiGuard intelligence shows that TTE as 24–48 hours for critical outbreaks, a sharp increase from earlier reports that revealed a TTE of 4.76 days. Real-world incidents reflect how minutes can define outcomes: Active exploitation attempts were made within hours of the React2Shell vulnerability public disclosure.
- Ransomware victims skyrocket: FortiRecon adversary intelligence identified 7,831 confirmed ransomware victims globally, skyrocketing from approximately 1,600 identified victims in the

Fortinet 2025 Global Threat Landscape Report. Availability of crime service kits like WormGPT, FraudGPT, and BruteForceAI contributed to this 389% increase year-over-year (YoY). The top three targeted sectors include manufacturing (1,284), business services (824), and retail (682). Geographic concentration includes the U.S. (3,381), Canada (374), and Germany (291).

- Identity sprawl defines cloud exposure: FortiCNAPP intelligence confirms that throughout 2025, most confirmed cloud incidents originated from stolen, exposed, or misused credentials rather than from infrastructure exploitation. Sector analysis shows hospitals/physician clinics and retail establishments as the #1 target. Large identity populations, federated access models, and complex cloud integrations make these prime targets for malicious hackers.

Inside the Habits of Modern, AI-Enabled Cybercriminals

As FortiGuard Labs Cyberthreat Predictions for 2026 projected, the most capable threat groups function as semi-autonomous enterprises, supported by shadow agents, access brokers, and botnet operators who provide services on demand. Key findings from the 2026 Global Threat Landscape Report show:

- Shadow agents reduce operator skill requirements while increasing workflow speed. FortiRecon dark web signals captured AI-enabled offensive tooling advertised as services and products, including enhanced versions of WormGPT and FraudGPT, and novel services like HexStrike AI, an offensive AI tool with automated reconnaissance attack path generation; and BruteForceAI, a penetration testing tool that integrates large language models (LLMs) for intelligent form analysis and can execute sophisticated multi-threaded attacks.
- With AI, criminals work smarter, not harder. FortiGate IPS telemetry recorded a 22% decrease in brute force attempts YoY, pointing to efficiency gains: With optimised, intelligent brute force techniques, threat actors are making fewer attempts against better-selected targets, increasing success probability per credential tested. This activity translates into about 67.65 billion brute force events globally, with approximately 185 million attempts per day; 1.3 billion attempts per week; and 5.6 billion attempts per month. At the same time, intelligence revealed a 25.49% increase in global exploitation attempts YoY.
- Stolen datasets are more popular than leaked credentials. In the 2025 Global Threat Landscape Report, FortiGuard Labs observed a 500% increase in logs available from systems compromised by infostealer malware. In 2026, FortiRecon intelligence found an additional 79% increase and revealed a shift toward theft of more comprehensive data sets, enabled by agentic AI. Within dark web "database" activity, stealer logs dominated advertised and shared datasets (67.12%), exceeding combolists (16.47%) and leaked credentials (5.96%). Stealer logs reduce attacker effort by bundling identity material with contextual artifacts, including browser-resident data, enabling immediate replay and faster conversion than brute force or password spraying.
- Credential-stealer malware persists. Credential-stealer malware remains a lucrative industry and primary upstream engine for exposure generation. FortiRecon telemetry shows stealer activity dominated by RedLine: 911,968 infections (50.80%); Lumma: 499,784 (27.84%); and Vidar: 236,778 (13.19%).

Putting Awareness into Action: Disrupting Cybercriminal Ecosystems

Fortinet is committed to disrupting cybercrime by collecting and sharing threat intel and actively working to combat cyberthreats on a global scale.

A recent collaborative effort spearheaded by INTERPOL and supported by Fortinet through the World Economic Forum Cybercrime Atlas resulted in the takedown of a cybercriminal network. Operation Red Card 2.0 took down infrastructure and operators behind online scams, mobile money fraud, and fraudulent loan applications in Africa. Fortinet is a founding member of the Cybercrime Atlas, a global public-private collaboration effort hosted by the World Economic Forum that uses open-source intelligence to map cybercriminal networks, identify infrastructure vulnerabilities, and support joint disruption operations with law enforcement, such as the recent Operation Red Card 2.0 and Operation Serengeti 2.0.

The 2026 Global Threat Landscape Report reveals that incentivising the disruption of cybercrime has never been more important. To empower defenders to stay ahead of cybercriminals, Fortinet and Crime Stoppers International launched the Cybercrime Bounty program to provide a secure, anonymous channel for citizens and ethical hackers to submit information about cyberthreats.

Discover how FortiGuard Labs Advisory Services combine cutting-edge technology and expert services to help organisations strengthen their security posture before threats emerge. FortiGuard Outbreak Alerts provide key information about ongoing cybersecurity attacks with significant ramifications affecting companies, organisations and industries. In the event of an incident, FortiGuard Labs offers swift, effective response and in-depth forensic analysis to minimise impact and prevent future intrusions, delivering comprehensive protection in today's increasingly volatile digital landscape.

HUAWEI APPOINTS COREY DENG AS CSPO FOR ME AND CENTRAL ASIA

THE NEW APPOINTMENT HIGHLIGHTS THE COMPANY'S CONTINUED INVESTMENT AND COMMITMENT TO ADVANCING CYBERSECURITY AND PRIVACY ACROSS THE REGION.

Huawei, a global leader in information and communications technology (ICT) infrastructure and smart devices, has appointed Corey Deng as Chief Cybersecurity and Privacy Officer (CSPO) for its Middle East and Central Asia Region, underscoring its continued focus on strengthening cybersecurity and privacy governance across the region.

In this role, Corey Deng will lead Huawei's regional cybersecurity and privacy strategy, overseeing frameworks spanning cybersecurity, data protection, AI security and privacy compliance. He will work closely with customers, partners and regulators to further advance Huawei's end-to-end cybersecurity assurance system and support the region's evolving digital landscape.

Corey Deng brings over 18 years of experience within Huawei, having joined the company in 2008. His career reflects a combination of technical depth and international leadership across both mature and emerging markets.

Prior to this appointment, he served as Chief Cybersecurity and Privacy Officer at Huawei's Digital Power Business Unit Headquarters. He has also held roles as Cybersecurity Director and Vice President of Solutions Sales in the United Kingdom, Solutions Sales Director in the Netherlands, and earlier positions in Research and Development as a Marketing Manager and IC Chipset Designer.

Commenting on the appointment, Phillip Gan, President of Huawei Middle East and Central Asia, said: "Cybersecurity and privacy are foundational to building a trusted digital ecosystem. Corey Deng's experience and leadership will further strengthen our ability to support clients and partners with secure, resilient solutions aligned to the region's digital ambitions."

Corey Deng added: "As digital transformation accelerates across the Middle East and Central Asia, trust must remain central to innovation. I look forward to working with stakeholders across the region to strengthen cybersecurity and privacy frameworks that enable sustainable and secure growth."

The region faces a complex threat situation, which is influenced by ongoing geopolitical dynamics. As rapid technology adoption expands the attack surface, Huawei emphasises that traditional security must evolve and adapt to the new era by focusing on sovereign AI infrastructure and quantum safety.

Under Deng's leadership, Huawei will continue to integrate cybersecurity and privacy protection into its products, solutions and internal governance practices. This appointment reflects the company's ongoing commitment to supporting a secure and trustworthy digital environment across the Middle East and Central Asia.

AS DIGITAL TRANSFORMATION ACCELERATES ACROSS THE MIDDLE EAST AND CENTRAL ASIA, TRUST MUST REMAIN CENTRAL TO INNOVATION.

Corey Deng, Chief Cybersecurity and Privacy Officer, Huawei Middle East and Central Asia.

NETAPP APPOINTS JURGEN HOFKENS AS CTO AND VP SALES ENGINEERING, EMEA & LATAM

APPOINTMENT TO ACCELERATE CUSTOMER ADOPTION OF AI DATA INTELLIGENCE, DATA SOVEREIGNTY AND CYBERSECURITY, AND FLEXIBLE HYBRID CLOUD ACROSS THE REGION.

NetApp, the Intelligent Data Infrastructure company, appointed Jurgen Hofkens as Chief Technology Officer and Vice President of Sales Engineering for EMEA and LATAM, effective 1 May 2026. He reports to Willem Hendrickx, SVP and General Manager, EMEA and LATAM, and will lead the region's technical strategy and customer engagement as enterprises operationalise AI, strengthen data sovereignty and security, and seek the flexibility to run workloads wherever the business needs them.

"Every CIO and CISO I speak with is asking the same three questions: how do I turn my data into an AI advantage, how do I keep it sovereign, private and secure, and how do I keep the flexibility to run it wherever the business needs it — on-premises, at the edge, or in any cloud?" said Hofkens. "NetApp sits at the intersection of those questions like no other company. I intend to spend the coming months on the ground with our customers and partners across EMEA and LATAM — listening, challenging, and co-designing what intelligent data infrastructure looks like for their business."

"Our customers and partners are navigating a once-in-a-generation shift: making their data ready for AI, hardening it against new cyber threats, and running it seamlessly across clouds and on-premises," said Hendrickx. "Jurgen's appointment reflects our commitment to stand shoulder-to-shoulder with them, backed by the deepest technical expertise in the industry. We are also growing our sales engineering, AI and cybersecurity teams across the region, and welcome talented people who share that customer focus to join us."

Jurgen Hofkens, Chief Technology Officer and Vice President of Sales Engineering, EMEA & LATAM, NetApp.

Hofkens joins NetApp from AWS, where he led the full Go-to-Market for AI Infrastructure across EMEA, owning strategy, technical field execution and customer outcomes as enterprises scaled from experimentation to production. In parallel, he led the EMEA technical teams covering AWS's core services and advanced computing portfolio, spanning security, networking, compute, edge, HPC, IoT and hybrid cloud. Earlier, he co-founded GIG Technology, building a distributed object and block storage platform from the ground up, and served as EMEA CTO and Head of Sales Engineering at Alcatel-Lucent, where he also ran its Telco Software P&L. Hofkens is based in Belgium.

LEAP

INTO NEW WORLDS

YOU'RE ONE LEAP AWAY

From 31 Aug - 3 Sept 2026

Riyadh Exhibition and Convention Center - Malham, Saudi Arabia

SECURE YOUR PASS NOW

Delinea

Unlock AI's potential, not your defenses.

AI is transforming the enterprise, unleashing new possibilities for greater efficiency, rapid innovation, and sustained growth. It's also greatly expanding the attack surface.

Machine identities now outnumber humans as much as 46:1[1], making them prime targets for attackers seeking to exploit privileged credentials.

Secure AI with Delinea so you can:

- Build an AI strategy with confidence
- Secure your AI stack against sophisticated threats
- Gain complete visibility and control of both sanctioned and unsanctioned AI use

Learn more about how to leverage AI responsibly and securely with Delinea.

[1]Delinea, Cybersecurity and the AI Threat Landscape, 2025

delinea.com