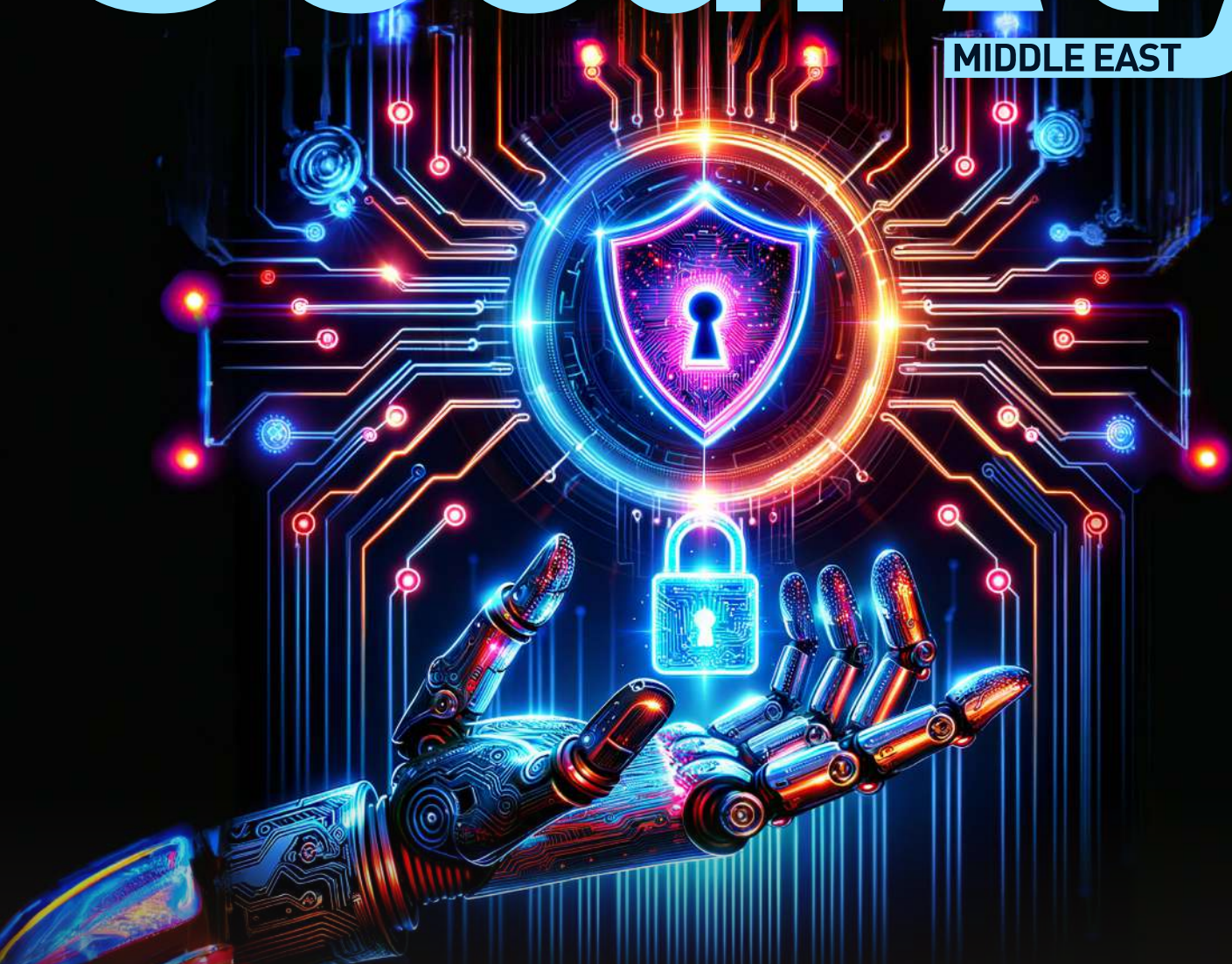


# Security

ADVISOR

MIDDLE EAST



## SEASONAL RISK TRENDS: BEYOND PHISHING AND FRAUD

SHIFTING DIGITAL BEHAVIOUR DURING PEAK ONLINE ACTIVITY IS  
RESHAPING THE CYBER THREAT LANDSCAPE ACROSS THE MIDDLE EAST



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<sup>1</sup>**, 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.**

<sup>1</sup>Delinea, Cybersecurity and the AI Threat Landscape, 2025



## 20 COVER STORY



**17** Microsoft and CPX launch "She Protects" initiative, empowering young women in cybersecurity across UAE

**42** Fraud evolves and so must we - true protection starts with people

**30** PNY Technologies MEA builds backbone of Enterprise AI in Egypt and Middle East

**48** AI assistants are rewriting how brands show up - and blocking bots may be making it worse



# Into New Worlds

You're One LEAP Away

From 13-16 April 2026

Riyadh Exhibition and Convention  
Center - Malham, Saudi Arabia

Secure your pass now

# EDITOR'S NOTE



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

**Sandhya DMello**  
Editor

## RESILIENCE IN AGE OF AI

**R**amadan is not just a season of reflection across the Middle East; it is a predictable shift in digital behaviour. Reduced working hours, heightened evening activity, surging e-commerce, and increased charitable giving create a distinct cybersecurity profile. Threat actors understand this well. Familiar tactics — phishing, credential abuse, delivery scams — are repackaged with cultural precision and timed for maximum impact.

February's cover story explores how CISOs must recalibrate detection models, identity controls, and SOC coverage during this behavioural pivot. Security teams cannot afford to operate on assumptions; telemetry and timing must guide strategy, especially when incidents peak outside traditional business hours. Identity-first detection, adaptive authentication, and clearly defined response authority become critical when executive oversight windows narrow.

Beyond seasonal risk, this issue captures a deeper transformation: AI is now embedded across data, infrastructure and security operations. From securing the AI lifecycle end-to-end to enabling AI-ready smart data and autonomous incident

response, the region is accelerating from experimentation to scaled deployment. Yet ambition must be matched by discipline. Talent shortages, fragmented data estates and legacy architectures continue to slow operational impact.

Deepfakes, voice cloning, and AI-generated identities are fuelling a surge in emotionally manipulative fraud. Dark web marketplaces are evolving into structured service economies. Hybrid work models are expanding the attack surface beyond traditional perimeters. Meanwhile, hyperscale AI infrastructure and sovereign data strategies are redefining enterprise risk exposure.

Resilience, therefore, is no longer a defensive posture. It is a strategic capability. Automation must reduce analyst fatigue without eroding accountability. Governance must evolve as quickly as innovation. Security leaders who align operational coverage with behavioural patterns, strengthen identity controls and integrate AI with clarity — not complexity — will define the region's next phase of cyber maturity.

Preparation, not reaction, will determine advantage in 2026.

### RAMADAN AI RISK SHIFT

#### EVENTS



FOUNDER, CPI  
Dominic De Sousa  
(1959-2015)

Published by **CPI**

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

EDITORIAL  
Editor  
Sandhya DMello  
sandhya.dmello@cpimediagroup.com

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

DIGITAL SERVICES  
Web Developer  
Adarsh Snehanjan  
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

Sales Director  
Sabita Miranda  
sabita.miranda@cpimediagroup.com

Online Editor  
Daniel Shepherd  
daniel.shepherd@cpimediagroup.com

© Copyright 2026 CPI  
All rights reserved

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

## SENTINELONE DELIVERS END-TO-END AI SECURITY FROM DATA TO RUNTIME

New Data Security Capabilities Advance Unified Platform Approach to Securing the Full AI Lifecycle

### SentinelOne, the AI-native security

leader, announced the expansion of its AI Security Platform with new Data Security Posture Management (DSPM) capabilities designed to secure artificial intelligence (AI) systems from data ingestion through runtime execution. As a result, organisations can embrace AI adoption while ensuring they meet privacy and regulatory requirements, derisk data leakage concerns, and empower AI-driven innovation and automation with confidence.

As AI usage moves from experimentation into widespread production, enterprises are facing a new category of risk that directly impacts business velocity, trust, and regulatory exposure. AI systems are increasingly embedded across data, cloud infrastructure, and production workflows, expanding the attack surface. This new AI reality requires a holistic, end to end approach that protects data, infrastructure, and runtime as a single, unified system.

SentinelOne's new DSPM capabilities serve as the first mile of AI security, helping organisations prevent sensitive or high risk data from ever entering AI pipelines, addressing irreversible risks such as data memorisation and pipeline poisoning before training begins.

They build upon SentinelOne's



Gregor Stewart, Chief AI Officer at SentinelOne.

cloud infrastructure posture management (CSPM), AI security posture management (AI-SPM), runtime workload protection, as well as employee GenAI security and agent security, to create the most complete AI Security platform in the market.

This unified approach allows security teams to trace risk across the full lifecycle, prevent lateral movement from data to model logic, and protect AI systems as they operate in real world environments.

"As AI systems become more powerful and more autonomous, security must evolve to match that reality," said Gregor Stewart, Chief AI Officer at SentinelOne. "AI security is not a point problem. It is a lifecycle problem. Data security is the first mile, but true protection requires securing everything AI is built on, from data and infrastructure to runtime behaviour."

**AS AI SYSTEMS BECOME MORE POWERFUL AND MORE AUTONOMOUS, SECURITY MUST EVOLVE TO MATCH THAT REALITY," SAID GREGOR STEWART, CHIEF AI OFFICER AT SENTINELONE.**

---

# NETSCOUT DELIVERS AI-READY SMART DATA FOR COMMUNICATIONS SERVICE PROVIDERS

---

Curated feeds enable scalable agentic ai for improved customer experience and network operations



**NETSCOUT Systems, a leading provider** of observability, AIOps, cybersecurity, and DDoS attack protection solutions, announced the extension of the NETSCOUT Omnis AI Insights solution to communications service providers (CSPs) to deliver the critical data foundation needed to implement agentic AI for customer experience and network operations. Now that NETSCOUT can transform CSPs' raw network data into AI-ready smart data, they can deploy AI agents that improve the customer experience, enable predictive maintenance, and enhance network security with greater efficiency, reduced costs, and decreased risk.

According to a McKinsey & Company C-level survey of telco operators, 64% stated they are scaling their AI efforts, with the introduction of AI agents being a key driver. More importantly, 45% of respondents cited data as the primary inhibitor to their scaling efforts.

NETSCOUT's Omnis AI Sensor for Service Providers delivers curated, AI-ready smart data in real time that CSPs need to optimise customer experience, solve problems faster, and assure service quality across complex digital ecosystems, including 5G, RAN, Core, MEC, and

Transport. It delivers a high-fidelity dataset that enables superior AI/ML outcomes by minimising the human intervention required to correct AI hallucinations, driving greater trust in those insights for better decision-making. This enhanced visibility layer correlates data from across the mobile/fixed network into a single unified, consistent view. CSP teams gain timely, accurate, and complete insights into performance, service impact, and customer outcomes from intelligently normalising network information, continuously linking activity to real subscriber experiences, and precisely aligning events across the network. The result is faster root-cause analysis, more confident operational decisions, improved service quality, and a clearer understanding of how network performance impacts customers across mobile domains.

Omnis AI Streamer for Service Providers enables operational teams to turn overwhelming volumes of network telemetry into actionable intelligence that drives faster detection, analysis, and automated response. It is a powerful, programmable curation engine that transforms sensor data into actionable real-time intelligence

tailored to the specific needs of network, service assurance, and operations teams. By extracting, aggregating, and labeling high-value signals from complex data streams, it enables operators to precisely shape the data they need through an intuitive Playbook Builder. Optional ML-based enrichment can be applied to selected feeds—such as outlier detection, and contextual classification—leveraging high-fidelity, sensor-derived metadata. This produces significantly smaller, faster-to-process curated data streams that external AI agents, analytics platforms, and operational applications can consume directly to drive closed-loop actions at scale.

"AI agents only deliver meaningful outcomes when they are powered by meticulously curated, multi-domain intelligence drawn from real activity across the digital ecosystem," stated Richard Fulwiler, senior director, product management, NETSCOUT. "By dramatically reducing data volume, complexity, and infrastructure demands for storage and processing, while minimising risk by enhancing network security, we help CSPs shift customer service and care from being a cost center to a strategic resource that protects revenue and strengthens loyalty."

## INTERSEC 2026 SETS NEW GLOBAL BENCHMARK FOR SECURITY, SAFETY AND FIRE PROTECTION IN DUBAI

Agreements signed during a recent Finland state visit to the UAE will explore deployment of VentureOne's secure systems throughout critical safety and infrastructure projects in Finland and northern Europe.

### Intersec 2026, the world-leading

exhibition for security, safety and fire protection, has recorded its largest, most internationally diverse and strategically significant edition to date.

The three-day event, which celebrated its 27th edition, was held under the patronage of His Highness Sheikh Mansoor Bin Mohammed bin Rashid Al Maktoum, Chairman of the Dubai Ports and Borders Security Council, and welcomed 44,764 trade visitors from 151 countries, with a 60/40 domestic versus international split, reinforcing Intersec's position as the global meeting point for government authorities, regulators, industry leaders and solution providers shaping the future of security, safety and resilience.

Spanning over 65,000 square metres of gross exhibition space, Intersec 2026 featured 1,180 exhibitors from 56 countries, supported by 10 international country pavilions and a comprehensive programme of 14 conferences and specialist features, reflecting the growing complexity and convergence of physical, digital and human safety and security.

### International participation underscores Intersec's global scale

Global participation remained a key feature of the 2026 edition, with 82% of total exhibitors coming from international markets, underscoring the event's role as a global marketplace. Exhibitor participation was led by the world's foremost safety, security and technology markets, including the United States and China; high-growth economies such as India and South Korea; and Europe's most established industrial and innovative hubs, including France, Germany, Italy,



Intersec 2026 welcomed nearly 44,764 trade visitors from 151 countries and featured 1,180 exhibitors, denoting its largest, most internationally diverse and strategically significant edition to date.

Türkiye, and the United Kingdom.

The United Arab Emirates remained the event's largest and most influential domestic exhibiting market, reflecting the country's growing prominence across the global security, safety and fire protection landscape. This momentum is being driven by bold national initiatives that continue to strengthen regulatory frameworks, accelerate the adoption of advanced technologies, and embed resilience, innovation, and convergence across the entire ecosystem.

### Technology and solutions aligned with global and national priorities

This leadership was clearly reflected on the exhibition floor, where solutions aligned with national and international priorities were brought to life across five core sectors, including Homeland Security & Policing, Cybersecurity, Commercial & Perimeter Security, Fire & Rescue, and Health & Safety. Together,

exhibitors showcased next-generation technologies, integrated systems, and operational solutions that address critical challenges, including infrastructure protection, emergency response, cyber resilience, workforce safety, and crisis preparedness.

### Intersec Global underscores platform's evolution

Intersec 2026 marked a significant milestone, unveiling the new Intersec Global identity during a press conference attended by strategic partners and industry leaders.

As part of the Global platform, the evolution of Intersec's sectors reflects a deliberate macro-to-micro narrative, moving from safeguarding nations to protecting individual lives within a unified international framework. At the macro level, National Security & Resilience supports ministries, police and border authorities shaping sovereign

risk strategy, while Cybersecurity underpins digital governance and critical infrastructure protection.

This extends into Surveillance & Physical Security for built environments and smart cities, and Fire, Rescue & Emergency Response for civil defence and climate-driven readiness. This culminates at the micro level with Safety & Wellbeing, aligned with ESG priorities and workforce protection, safeguarding people in their daily environments and demonstrating how Intersec Global connects national resilience with human-centred safety across its worldwide ecosystem.

Dishan Isaac, Show Director of Intersec at Messe Frankfurt Middle East: "This edition represents a pivotal moment for the platform, highlighting its expanded scale and the increased engagement from the global safety and security community. The launch of the Intersec Global identity reflects the on-the-ground reality, emphasising an international ecosystem rooted in Dubai, with increasing involvement from both established markets and high-growth regions.

"With a significant increase in international exhibitors and visitors, the quality of dialogue has been excellent. From strategic policy discussions to

frontline operational challenges, the focus has been firmly on real-world resilience, readiness and collaboration. The breadth of engagement from government authorities, critical infrastructure operators, emergency services and the private sector reinforces Intersec Global's role as an international platform where meaningful partnerships are formed, knowledge is shared, and industry progress is accelerated."

### **Intersec Awards celebrate leadership and industry excellence**

Industry achievement took centre stage at the Intersec Awards 2026, held during a prestigious gala dinner in Dubai. Now in their fifth edition, the Awards recognised excellence across 17 categories, celebrating leadership, innovation, talent, and impact in security, safety, and fire protection.

Headline winners included Khalid Mubarak of Dubai Municipality, who received the H.H. Sheikh Mansoor bin Mohammed bin Rashid Al Maktoum Emirati Rising Star Award, and Albadr Jannah of Saudi Aramco, named Industry Leader of the Year for his sustained contributions to advancing security and resilience at regional and global levels.

The Women Trailblazers in Security,

Fire Safety and HSE award was presented to Jazyah Aldossary, also of Saudi Aramco, recognising her leadership in driving professional excellence, inclusion and safety culture.

"Now in their fifth edition, the Intersec Awards highlight the individuals and organisations setting the pace for leadership, innovation and impact across security, safety and fire protection. This year's winners reflect the depth of talent shaping the industry, from rising Emirati professionals and women leaders to global figures whose work continues to strengthen resilience and best practice worldwide," concluded Isaac.

### **Government partnership key to future success**

Intersec benefits from the strategic support of key UAE authorities, including the General Command of Dubai Civil Defense (DCD) and the Security Industry Regulatory Agency (SIRA), underlining its alignment with national resilience and safety priorities

The event will return to Dubai from 12-14 January 2027 at the Dubai World Trade Centre, continuing to build on its role as the world's leading platform for advancing safety, security, and resilience across nations, networks, infrastructure, and people.

---

## **MANAGEENGINE LAYS OUT VISION TO ENABLE ENTERPRISES TO BE AI-DRIVEN AND AUTONOMOUS AT USERCONF DUBAI 2026**

---

### **ManageEngine, a division of Zoho**

Corporation and a leading provider of enterprise IT management solutions, today announced its vision to enable enterprises to be AI-driven and autonomous at the 13th edition of the ManageEngine UserConf Dubai, its largest annual gathering of customers in the UAE.

In the rapid adoption of AI-driven, agentic, and autonomous systems, enterprise priorities are shifting from

experimentation to dependable, large-scale operations. As these systems take on more autonomous decision-making, organisations face increasing constraints around reliability, governance, and operational control, which are often the primary barriers to adoption. Successfully deploying AI at scale now requires a layered infrastructure approach where a strong reliability layer is foundational to performance, trust, and long-term sustainability.

"As enterprises move from experimenting with AI to operating autonomous and agentic systems at scale, high performance and security in real-world conditions become nonnegotiable," said Rajesh Ganesan, CEO of ManageEngine. "ManageEngine's evolution into a platform [and, increasingly, a platform of platforms] is about enabling organisations to build reliability into the very fabric of their infrastructure, not bolt it on as an

afterthought, creating a foundation for autonomy across the modern enterprise.”

Key highlights of the conference included:

- “The digital transformation journey: From AI-ready to AI-driven autonomous enterprises,” a keynote address by Ganesan that explored the need for an autonomous, AI-powered digital enterprise management platform.
- A keynote address, “A pause before agentic AI adoption,” by Heba Farahat, offensive security tech lead at Liquid C2 MENA and an award-winning cybersecurity advisor guiding global organisations across sectors.
- A panel discussion, “The role of cybersecurity in the digital transformation journey: From a cost to a competitive advantage.”

“The UAE government’s strong AI vision has already translated into several national initiatives to develop AI readiness across the government and enterprises.

We at ManageEngine are closely aligned with this vision and are helping customers in the region build the reliable, scalable infrastructure needed for AI-driven and autonomous systems. Through this 13th edition of the ManageEngine UserConf Dubai, we are further reinforcing our commitment to preparing



Rajesh Ganesan, CEO, ManageEngine.

for the next phase of AI adoption,” said Nirmal Kumar Manoharan, vice president of revenue operations at ManageEngine.

The UserConf also offered certifications, technical workshops, and networking forums. Panel discussions featuring tech experts from the UAE provided insights into the current state

of AI adoption and how organisations can be AI-ready in the region. Attendees also met with product teams, explored best practices for maximising the value of their solutions, and experienced live technical demonstrations of the company’s comprehensive enterprise IT management solution suite.

## MANAGEENGINE INTRODUCES CAUSAL INTELLIGENCE AND AUTONOMOUS AI TO IT OPERATIONS FOR FASTER INCIDENT RESPONSE

New Site24x7 Capabilities combine domain-aware correlations, autonomous AI, and workflow orchestration to drive self-healing IT operations.

### ManageEngine, a division of Zoho

Corporation and a leading provider of enterprise IT management solutions, today added new causal intelligence and autonomous AI capabilities in Site24x7, its full-stack observability platform. These enhancements transform how enterprises handle outages, shifting from firefighting to autonomous resilience. By drastically reducing mean time to recovery (MTTR) and ensuring service-level agreement (SLA) compliance,

Site24x7 helps IT teams safeguard the customer experience and retain trust.

Modern IT environments are increasingly fragmented across hybrid clouds, microservices, and dynamic networks, generating massive volumes of telemetry and predictive anomaly signals every second. When an incident occurs, this complexity turns troubleshooting into a needle-in-a-haystack search, often leading to prolonged downtime. IT teams struggle to correlate anomaly signals

and events across these layers, delaying the critical fix to restore normalcy, jeopardising brand reputation.

“Hybrid and cloud-native architectures have made IT operations highly interconnected, while IT managers are under constant pressure to resolve incidents quickly amid growing complexity,” said Srinivasa Raghavan, director of product management at ManageEngine.

“By combining predictive anomaly

detection, intelligent event correlation, service dependency context, and AI-driven causal insights, Site24x7 cuts through alert noise to show not just what is broken, but what caused it and what it impacts, helping teams identify the true fault faster and significantly reduce MTTR while minimising service disruption."

"Triaging and resolving incidents in hybrid environments with growing infrastructure complexity can quickly become a nightmare, especially when SLA commitments are on the line," said Pravir Kumar Sinha, IT leader at Synechron, a global IT services company and one of the early customers to access the feature. "With Site24x7 AIOps, we're able to filter out nearly 90% of alert noise, pinpoint issues faster, and accelerate resolution. This helps us achieve stronger SLA adherence, reduce MTTR, and ultimately deliver reliable digital experience for customers."

The introduction of autonomous AI in Site24x7 represent a practical step toward more autonomous IT operations by analysing observability data, reducing cognitive overload, and turning insights into clear, actionable guidance.

"With MCP providing the control and governance layer, we ensure this intelligence is applied securely and within enterprise guardrails. This empowers IT leaders move toward agentic workflows with confidence, stay ahead of the AI adoption curve, and strengthen the resilience of their critical digital services," said Raghavan.

Key capabilities include:



Srinivasa Raghavan, Director of Product Management, ManageEngine.

- Domain-aware causal correlation with predictive anomaly detection: Detects anomalies and correlates related signals across applications, infrastructure, and networks into a single, context-rich problem—so teams can quickly understand what is connected and where to start.
- Customisable AI Agents with governed, task-driven automation: Enables customers to create and tailor AI Agents, set approved guardrails using solution documents, and assign tasks that guide agents from analysis to guided action—making response workflows more consistent across teams.

- Delivers faster root-cause identification with causal intelligence-driven correlation
- Improves incident response efficiency using AI
- Enables controlled remediation at scale through governed workflow orchestration powered by Qntrl

- MCP-enabled agentic foundation for customers: MCP provides the enabling layer for customers to build and operationalise agentic use cases on top of observability data—standardising how agents access data, follow approved guidance, and execute tasks within enterprise-ready controls and auditability.
- Orchestrated remediation with Qntrl: Co-ordinates downstream actions through structured workflows and repeatable runbooks, powered by Zoho's workflow and orchestration platform Qntrl, with approvals and traceability built in to support controlled automation.

These AIOps capabilities are now available for all users in Professional and Enterprise plans.

**HYBRID AND CLOUD-NATIVE ARCHITECTURES HAVE MADE IT OPERATIONS HIGHLY INTERCONNECTED, WHILE IT MANAGERS ARE UNDER CONSTANT PRESSURE TO RESOLVE INCIDENTS QUICKLY AMID GROWING COMPLEXITY," SAID SRINIVASA RAGHAVAN, DIRECTOR OF PRODUCT MANAGEMENT AT MANAGEENGINE.**

## SCHNEIDER ELECTRIC UNVEILS INDUSTRY'S FIRST OPEN, SOFTWARE-DEFINED DISTRIBUTED CONTROL SYSTEM

EcoStruxure Foxboro Software Defined Automation (SDA) delivers openness, embedded cybersecurity, and real-time intelligence, modernising operations without compromise

**Schneider Electric, a global energy technology leader,** announced EcoStruxure Foxboro Software Defined Automation (SDA), the industry's first open, software-defined Distributed Control System (DCS). This breakthrough combines the trusted reliability of Foxboro with the agility of open, software-defined automation, helping hybrid and process industry customers modernise faster, reduce risk, and ensure their operations are future-ready.

For decades, Foxboro DCS has served as the "brain" of industrial operations, enabling real-time control and coordination of complex processes. But today's landscape demands more – greater agility, fewer costly upgrades, and simplified compliance. EcoStruxure Foxboro SDA delivers exactly that: flexibility, scalability, and cost efficiency without sacrificing reliability.

The importance of open industrial systems was highlighted in Schneider Electric's recent global research report with Omdia, which uncovered closed systems cost mid-sized industrial companies 7.5% of revenue through downtime, inefficiencies, and compliance retrofits every year.

"EcoStruxure Foxboro SDA marks a defining moment for industrial automation," said Hany Fouda, Senior Vice President, Process Automation, Schneider Electric. "By embracing openness and software-defined architecture, we're giving our customers the agility to modernise without compromise, protecting their investments while unlocking future-ready capabilities. This evolution is a strategic enabler for digital transformation, and Schneider Electric is proud to lead it."



Developed by listening to real customer challenges; aging systems, rising costs, and the need to do more with less, Foxboro SDA decouples hardware from software to protect existing investments and enable a smooth, lower-risk modernisation path. The result is simpler workflows, faster insights, and sustainable performance gains.

### Key Features

- **Open, Software-Defined Architecture:** Foxboro SDA decouples software from hardware to deliver vendor independence and interoperability, enabling flexible, scalable architectures that simplify
- **Cybersecure & Future-Ready:** Foxboro SDA is built with secure-by-design principles and IEC 62443-3-3 compliance, delivering a future-ready platform that enables IT/OT convergence, AI/ML integration, and

autonomous operations for Industry 4.0 and energy transition.

- **Simplify Operations & Reduce Costs:** Customers can lower CapEx and OpEx, streamline deployment with intuitive tools, and minimises downtime by avoiding obsolescence and enabling predictive maintenance.

As the first software-defined distributed control system, Foxboro SDA is a validated, software-defined automation architecture for distributed control systems powered by EcoStruxure Automation Expert (EAE). It enables interoperability, rapid deployment, and fit-for-purpose configurations while maintaining high availability. The system ensures digital continuity by keeping data connected and consistent throughout the plant lifecycle—from design to production to maintenance. This enables automated workflows, better product quality, and easy integration with analytics for

smarter, real-time business decisions.

Customers benefit from a future-ready upgrade path, built-in cybersecurity, and simplified operations that support IT/OT convergence and advanced technologies like AI and machine learning. Foxboro SDA provides our customers with a control solution that is unbound by hardware, engineered for agility and empowered by data. It's more than a system - Foxboro SDA is a strategic

enabler for digital transformation.

"The launch of EcoStruxure Foxboro SDA marks a major milestone in the evolution of process automation," said Craig Resnick, Vice-President at ARC Advisory Group. "By decoupling control logic from hardware, Schneider Electric is providing manufacturers with the agility to scale, adapt, and simplify their operations. This software defined approach helps to reduce maintenance

costs, protect legacy automation investments, and ensure digital continuity throughout the entire plant lifecycle. With cybersecurity built into its core, and a commitment to open, interoperable standards, Foxboro SDA enables manufacturers to modernise at their own pace, accelerate IT and OT convergence, and increase their adoption of next generation technologies, such as AI, edge computing, and autonomous operations."

## SOPHOS EXPANDS PORTFOLIO WITH WORKSPACE PROTECTION TO SECURE HYBRID WORK AND GOVERN EMPLOYEE AI USE

### Sophos, a global leader of innovative

security solutions for defeating cyberattacks, today announced Sophos Workspace Protection, expanding its portfolio to help organisations secure hybrid work and govern the use of emerging technologies, including AI. Built around the Sophos Protected Browser, powered by Island, the solution enables organisations to protect applications, data, users, and guests wherever work takes place, while providing a unified approach to securing the modern workspace.

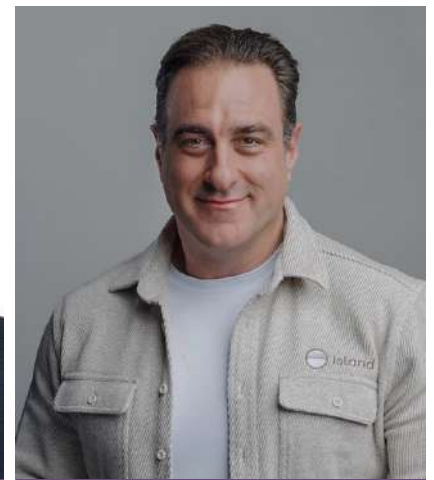
### Rethinking Security for Hybrid Work

Traditional approaches to securing hybrid work, including deploying multiple cloud-delivered SASE and SSE solutions, often require significant infrastructure, specialised expertise, and ongoing operational overhead to deploy and manage. These models can increase cost and complexity while still leaving gaps in visibility and control where modern work now happens.

Sophos Workspace Protection takes a different approach by securing the workspace directly, eliminating the need to backhaul traffic through centralised infrastructure. This reduces the operational burden and cost while enabling protections that follow users, applications, their internet usage, and their data wherever they work, providing organisations at all stages of security



Joe Levy, CEO of Sophos



Mike Fey, co-founder and CEO of Island

maturity with a simpler way to secure hybrid work without added complexity.

At the core of Sophos Workspace Protection is the Sophos Protected Browser, powered by Island and purpose-built to seamlessly integrate with the Sophos Central platform. With 85% of the modern workday now taking place in a web browser, the Sophos Protected Browser was developed to address security needs where modern work happens.<sup>1</sup> It provides organisations with visibility and control at the workspace level, helping them protect sensitive data, manage application access, and enforce policy directly within the browser. By embedding security controls into a familiar user experience,

Sophos Workspace Protection enables organisations to secure work across corporate and remote environments without disrupting productivity.

"Security teams are increasingly impacted by complexity, especially as hybrid work, SaaS adoption, and AI tools continue to expand the workspace," said Mike Jude, Research Director at IDC. "Sophos Workspace Protection reflects a pragmatic shift in the market—delivering core SASE and SSE outcomes through an integrated, endpoint- and browser-centric approach that simplifies deployment, reduces operational overhead, and helps organisations govern application and AI use without adding another layer of infrastructure."

### Governing Shadow IT and Shadow AI

As emerging technologies, including generative AI, become part of everyday workflows, organisations are increasingly challenged to understand how these tools are being used and what data is being shared through them. Recent research shows that more than half of employees worldwide now use AI tools at work, often before formal policies or controls are established, increasing risks associated with Shadow IT and Shadow AI.<sup>2</sup> By providing visibility and control at the workspace level, Sophos Workspace Protection helps organisations assess risk, enforce policy, and govern the safe use of emerging technologies across the hybrid workforce.

### What's Included in Sophos Workspace Protection

Sophos Workspace Protection is delivered as a flexible set of integrated components that organisations can deploy together or individually based on their security and operational requirements. The following components make up the Workspace Protection suite:

- **Sophos Protected Browser:** a Chromium-based secure enterprise browser, powered by Island, that provides controls over application usage, local data handling, and web filtering. It also integrates

Sophos ZTNA for access to private web applications and supports SSH and RDP access for remote administration.

- **Sophos ZTNA:** a Zero Trust Network Access (ZTNA) component that provides secure, posture-based access to private applications by allowing only authorised users and compliant devices to connect while keeping applications hidden from the internet.
- **Sophos DNS Protection:** a cloud-delivered DNS security service that organisations can deploy to individual Windows endpoints as part of Workspace Protection. It provides an additional layer of web and phishing protection by blocking malicious or unwanted domains.
- **Email Monitoring System:** an email security add-on deployed alongside Google or Microsoft email services that monitors email traffic and provides additional detection of unwanted or malicious messages, including phishing.

Together, these components enable several key benefits and use cases for organisations securing modern, hybrid work environments.

"Sophos has long protected remote and hybrid workers with industry-leading endpoint and network security,

but today's work environments demand stronger governance of apps and data," said Joe Levy, CEO of Sophos. "Many SASE and SSE solutions add complexity and operational overhead while still leaving gaps in visibility and control. By combining Island's enterprise browser technology with Sophos' security capabilities and the Sophos Central platform, we are helping organisations govern AI use, protect critical data, and secure hybrid workforces with a solution that is easier to deploy and manage."

"Hybrid work shouldn't mean tradeoffs between security and productivity," said Mike Fey, co-founder and CEO of Island. "Island protects data, secures application access, and helps organisations safely embrace AI, all through the browser people already use. Integrating with the Sophos Central platform lets customers do that with less complexity and more confidence."

### Key Benefits for Organisations

Sophos Workspace Protection helps organisations secure distributed and hybrid workers, govern the use of emerging tools and services, including AI, and support fast, flexible access for contractors and partners. The solution also strengthens defenses against phishing, browser-based threats, and other attacks that target users in the modern workspace.

## CISCO UNVEILS NEW SILICON ONE G300, TO POWER AND SCALE AI DATA CENTRES FOR AGENTIC ERA

New G300-powered Cisco N9000 and 8000 systems, advanced optics and management upgrades deliver hyperscale-level performance, reliability and efficiency for all AI network builders.

**Cisco (NASDAQ: CSCO) has unveiled the Silicon One G300**, a 102.4 Tbps switching silicon designed for massive AI cluster buildouts. The Cisco Silicon One G300 will power new Cisco N9000 and Cisco 8000 systems that push the frontier of AI networking in the data center.

The systems feature innovative liquid

cooling and support high-density optics to achieve new efficiency benchmarks and ensure customers get the most out of their GPU investments. In addition, the company enhanced Nexus One to make it easier for enterprises to operate their AI networks — on-premises or in the cloud — removing the complexity that can hold

organisations back from scaling AI data centers.

"We are spearheading performance, manageability, and security in AI networking by innovating across the full stack - from silicon to systems and software," said Jeetu Patel, President and Chief Product Officer, Cisco. "We're

building the foundation for the future of infrastructure, supporting every type of customer—from hyperscalers to enterprises—as they shift to AI-powered workloads.”

### **Silicon One G300: The Networking Foundation for the Agentic Era**

The new Silicon One G300 is a 102.4 Tbps switching silicon that exemplifies Cisco’s rapid innovation and sets a new standard for AI backend networking. It is designed to power massive, distributed AI clusters with high performance, security, and reliability.

The G300 uniquely offers Intelligent Collective Networking, which combines an industry-leading fully shared packet buffer, path-based load balancing, and proactive network telemetry to offer better performance and profitability for large-scale data centers. It efficiently absorbs bursty AI traffic, responds faster to link failures, and prevents packet drops that can stall jobs, ensuring reliable data delivery even over long distances. With Intelligent Collective Networking, Cisco can deliver 33% increased network utilisation, and a 28% reduction in job completion time versus simulated non-optimised path selection,



making AI data centers more profitable with more tokens generated per GPU-hour.

Cisco Silicon One G300 is highly programmable, enabling equipment to be upgraded for new network functionality even after it has been deployed. This enables Silicon One-based products to support emerging use cases and play multiple network roles, protecting long-term infrastructure investments. And with security fused into the hardware, customers can embrace holistic, at-speed security to keep clusters up and running.

### **Cisco Nexus One: Intelligent AI networking to drive AI infrastructure forward**

Organisations need greater flexibility in where and how they run AI workloads. To address the diverse requirements of these environments, Cisco is advancing Nexus One with a unified management plane that brings together silicon, systems, optics, software, and programmable intelligence as a single integrated solution.

#### **Availability**

The Silicon One G300, G300-powered systems and optics will ship this year.

---

## **QLIK BRINGS AGENTIC ANALYTICS TO GENERAL AVAILABILITY, LAUNCHES MCP SERVER FOR THIRD-PARTY ASSISTANTS**

---

New capabilities in Qlik Cloud unify a unique analytics engine, curated content, and governed data products with transparent reasoning; MCP extends Qlik’s trusted intelligence into leading AI assistants

**Qlik, a global leader in data integration,** data quality, analytics, and artificial intelligence (AI), announced the general availability of its agentic experience in Qlik Cloud, delivered through Qlik Answers as the unified conversational interface. Qlik also announced general availability of the Qlik Model Context

Protocol (MCP) server, enabling third-party assistants including Anthropic Claude to securely access Qlik’s analytical capabilities and trusted data products.

Enterprises are moving past proofs of concept and into production deployments, where the bar is defined by trust,

context, and accountability. Teams need systems that can work across structured analytics and unstructured content, preserve business logic, and show how conclusions were reached. Qlik’s agentic experience is built for that operating reality, pairing AI reasoning with context-preserving engine calculations, governed

data, and transparent responses suitable for real decision workflows.

**In Qlik Cloud, the agentic experience adds four core capabilities:**

- Turn questions into governed, explainable answers. Qlik Answers engages an agentic framework to deliver analytical insights powered by the Qlik Analytics Engine and grounded answers from curated documents, including citations and explanations of reasoning.
- Spot material changes early. Discovery Agent continuously monitors key measures and surfaces meaningful anomalies and shifts so teams can act before issues escalate or opportunities slip away.
- Make trusted data reusable for AI and analytics. Data Products for Analytics provide curated, governed datasets with stewardship and quality signals, giving both humans and AI a reliable foundation for analysis and reasoning.
- Extend Qlik into the assistants people already use. The Qlik MCP server exposes Qlik at the engine, tool, and agent levels, allowing third-party assistants such as Anthropic Claude to securely generate insights and work with governed data through Qlik's APIs.

"In 2026, boards are navigating geopolitical volatility, tightening AI rules, and relentless cost pressure. That changes what enterprise AI has to be: auditable, governed, and able to act inside real workflows," said Mike Capone, CEO, Qlik. "Qlik's agentic experience pairs our unique analytics engine with trusted data products and cited knowledge, and our MCP server opens that intelligence to the assistants people already use. The result is faster decisions with controls you can defend."

Qlik's approach is designed to help enterprises scale adoption without trading off control. The Qlik Analytics Engine preserves context during calculation, enabling more accurate



Mike Capone, CEO, Qlik.

reasoning over enterprise data than approaches that reduce questions to isolated queries. Combined with governed data products and cited retrieval from curated knowledge bases, Qlik gives teams a practical way to use AI in decisions that require traceability.

"AI delivers value when it's built on data that's already curated, governed and trusted," said Mike Krut, senior vice president of information technology, Penske Transportation Solutions. "Qlik's new agentic capabilities extend analytics our teams already use, helping connect insights directly to operational workflows like fleet performance and maintenance, without adding complexity."

"The move from copilots to reasoning systems exposes a critical gap in governed context and explainability for many enterprises," said Michael Leone, Practice Director and Principal Analytics and AI Analyst, Omdia. "Success now requires connecting trusted data

directly to operational workflows with full auditability. Qlik is addressing this by pairing its analytics engine with MCP, effectively establishing the intelligence layer that agents and assistants need to operate across ecosystems."

Qlik's agentic strategy is designed to expand over time, with additional agents planned across data pipelines, data quality, and stewardship, and plans to support additional AI tools and assistants through MCP throughout the year, further extending how teams move from insight to action while staying within enterprise governance and risk controls.

Customers can procure Qlik through AWS Marketplace to streamline procurement under existing AWS agreements.

**Availability**

Qlik Answers agentic enhancements and the Qlik MCP server are generally available now in Qlik Cloud. Discovery Agent and Data Products for Analytics are planned to roll out shortly after.

# MICROSOFT AND CPX LAUNCH “SHE PROTECTS” INITIATIVE, EMPOWERING YOUNG WOMEN IN CYBERSECURITY ACROSS UAE

National programme to inspire, equip, and empower young women in the UAE to shape the future of cybersecurity and drive inclusive growth in an AI-driven world.

**Microsoft, in partnership with CPX** (a G42 company), marked the official launch of “She Protects”, a pioneering national initiative designed to inspire and equip young women in UAE universities with the skills to safeguard the digital future. The programme’s launch event, held at Microsoft’s Dubai offices, brought together leaders from government, academia, and industry to celebrate a new chapter in building a more inclusive cyber workforce.

Timed to coincide with Safer Internet Day 2026, the initiative underscores Microsoft and CPX’s shared commitment to building a safer, more inclusive digital ecosystem by empowering the next generation of cybersecurity leaders.

The launch event featured opening remarks from Microsoft and CPX leadership, and panel discussions with female cybersecurity experts. Attendees participated in LinkedIn career development sessions and networking opportunities, underscoring the programme’s commitment to real-world impact and professional growth.

The shifting economic climate and rapidly evolving threat landscape have placed significant pressure on the global cybersecurity workforce, resulting in both talent shortages and widening skills gaps at a time when demand has never been higher. The need for cybersecurity professionals—particularly those with expertise in generative AI (GenAI)—is especially acute in the UAE, where ambitious national goals are driving the transition toward an AI-native society. Despite a well-documented global talent shortage in the cybersecurity industry, women still feel discouraged from joining it, constituting only about 25% of cybersecurity professionals according to a recent ISC2 report. native society.



She Protects runs from February 2026 to June 2026, offering participants a comprehensive pathway into cybersecurity careers. The initiative features CPX-led webinars on cyber hygiene and threat landscapes, Microsoft’s SC-900 Security, Compliance & Identity certification track, career readiness training through IDEA HR, LinkedIn’s “Rock Your Profile” workshops, immersive cyber labs powered by Cyberbit and supported by INJAZ UAE.

“For more than three decades, Microsoft has partnered with the UAE to expand opportunity through technology. Today, She Protects strengthens that partnership by building the talent that will secure our digital future. At Microsoft, we believe that empowering a diverse new generation of security professionals is essential for safeguarding our communities and driving innovation in an AI-driven era. Through this initiative, we are reaffirming our commitment to equipping young women with the skills, resources and global standards needed to defend against evolving cyber threats and uphold trust in the region’s digital economy.” — Amr Kamel, General Manager, Microsoft UAE

“Despite the opportunities available, young working women still feel discouraged from entering the industry, and through this program, CPX aims at creating awareness to make the sector more inclusive and gender diverse, says Hadi Anwar, CEO at CPX, “Empowering women in cybersecurity is not just about closing a gap—it’s about unlocking new potential for innovation and resilience and building trust in the UAE’s future digital and AI-powered economy.”

By training and upskilling 50 young women, She Protects strengthens the UAE’s cyber talent pipeline and advances diversity in a field where women remain underrepresented. The initiative forms part of Microsoft Elevate UAE, reinforcing Microsoft’s long-term commitment to upskilling talent and supporting the nation’s digital and AI ambitions, while empowering individuals to thrive in a digital-first world.

Endorsed by the UAE Cyber Security Council, She Protects is a testament to the UAE’s commitment to diversity and excellence in technology. By investing in young women, we are investing in the future of cybersecurity.

## OMNIX EXPANDS PORTFOLIO WITH LAUNCH OF DIGITAL TWIN CONSULTING SERVICES



Walid Gomaa  
CEO, Omnix International



Tommaso Stefano Tini  
Senior Manager Digital Twin Market Growth & Consulting  
Omnix International

**Omnix International, a leading** technology solutions provider in the Middle East, announces the launch of its Digital Twin consulting service line to its consulting portfolio. This strategic expansion reinforces Omnix's ambition to strengthen its regional leadership in Digital Twin by complementing its deep technology capabilities with structured, business-focused consulting services.

Digital Twins have emerged as a critical enabler for organisations seeking to improve performance, resilience, and sustainability across complex assets and operations. However, many initiatives struggle to move beyond isolated pilots or technology-driven proofs of concept. Omnix's new consulting offerings is designed to address this challenge by adding Digital Twin initiatives into business strategy, identify measurable outcomes, and long-term operational models.

Walid Gomaa, CEO of Omnix International, said, "Our mission is to expand Omnix's leadership in Digital

Twin by bridging technology excellence with strategic consulting. We want to help organisations translate Digital Twin potential into tangible business outcomes that will drive innovation, efficiency, and growth across the region."

The launch is built on three core pillars. First, Omnix leverages its deep technology expertise developed through long-standing partnerships with leading vendors in the Industry X ecosystem. Second, the company capitalises on its proven delivery experience as a trusted implementation partner for major enterprises across the GCC. Finally, Omnix introduces a structured advisory capability grounded in real industry challenges, helping clients define clear Digital Twin visions, prioritise high-value use cases, and develop executable roadmaps that deliver measurable impact.

In the GCC, many organisations are still developing the internal capabilities required to autonomously design and sustain Digital Twin programs aligned

with national agendas. As a result, Digital Twin initiatives often remain fragmented or disconnected from broader business objectives.

Tommaso Stefano Tini, Senior Manager Digital Twin Market Growth & Consulting, said "Omnix Digital Twin Consulting is designed to guide clients along an end-to-end journey that starts with business strategy rather than technology, ensuring scalability, adoption, and long-term value creation."

Omnix Digital Twin Consulting services will primarily support organisations operating in the GCC, with a strong focus on industries such as construction, manufacturing, energy, healthcare, and large asset portfolios. Looking ahead, Omnix expects Digital Twins in the Middle East to move rapidly from experimentation to execution, shifting from isolated assets to connected, enterprise-level platforms that support performance, sustainability, and ESG reporting.

# CLUDERA UNVEILS NEXT PHASE OF AI INFERENCE AND UNIFIED DATA ACCESS CAPABILITIES

Enabling faster, more accurate enterprise AI and analytics across multi-cloud, edge, and data center environments.

**Cloudera recently announced the** expansion of Cloudera AI Inference and Cloudera Data Warehouse with Trino to on-premises environments, empowering customers to harness advanced AI and analytics directly from within their data centers. The company also announced enhanced AI and analytics capabilities within Cloudera Data Visualization, streamlining AI workflows across cloud, edge, and data center environments.

As enterprises move from AI experimentation to production, the conversation has evolved: it's no longer just about where data is stored, but about providing AI with secure, reliable, and governed access to that data, wherever it resides. According to Cloudera's recent report, *The State of Enterprise AI and Data Architecture*, nearly half of companies store their data in a data warehouse. By guaranteeing that AI applications can access this data securely, organisations can extract meaningful insights without transferring sensitive information outside of protected environments. This approach helps to minimise security risks, limits compliance exposure, and streamlines operations.

With Cloudera AI Inference, powered by NVIDIA technology, now available on premises, organisations can deploy and scale any AI model, including the latest NVIDIA Nemotron open models—from LLMs, fraud detection, computer vision, voice, and more—directly within their data centers. Accelerated by the NVIDIA AI stack, by NVIDIA Blackwell GPUs, NVIDIA Dynamo- Triton Inference Server, and NVIDIA NIM microservices for high-performance, scalable model serving, Cloudera AI Inference enables secure, governed deployment of AI at enterprise scale, delivering superior cost-efficiency and predictable economics



Leo Brunnick, Chief Product Officer at Cloudera

by avoiding the volatile costs of the cloud, organisations gain full control over latency, compliance, and data privacy while ensuring that once AI moves into steady production, long-term costs remain lower and easier to manage.

Cloudera Data Warehouse with Trino - now available in data center environments - enables centralised security, governance, and observability across the entire data estate while accelerating access to insights. With integrated AI-powered analytics and visualisation, enterprises can turn complex data into actionable outcomes without compromising security, compliance, or operational control.

The enhancements to Cloudera Data Visualization empower organisations to gain richer insights and streamline AI-driven workflows in the data center and beyond. These include:

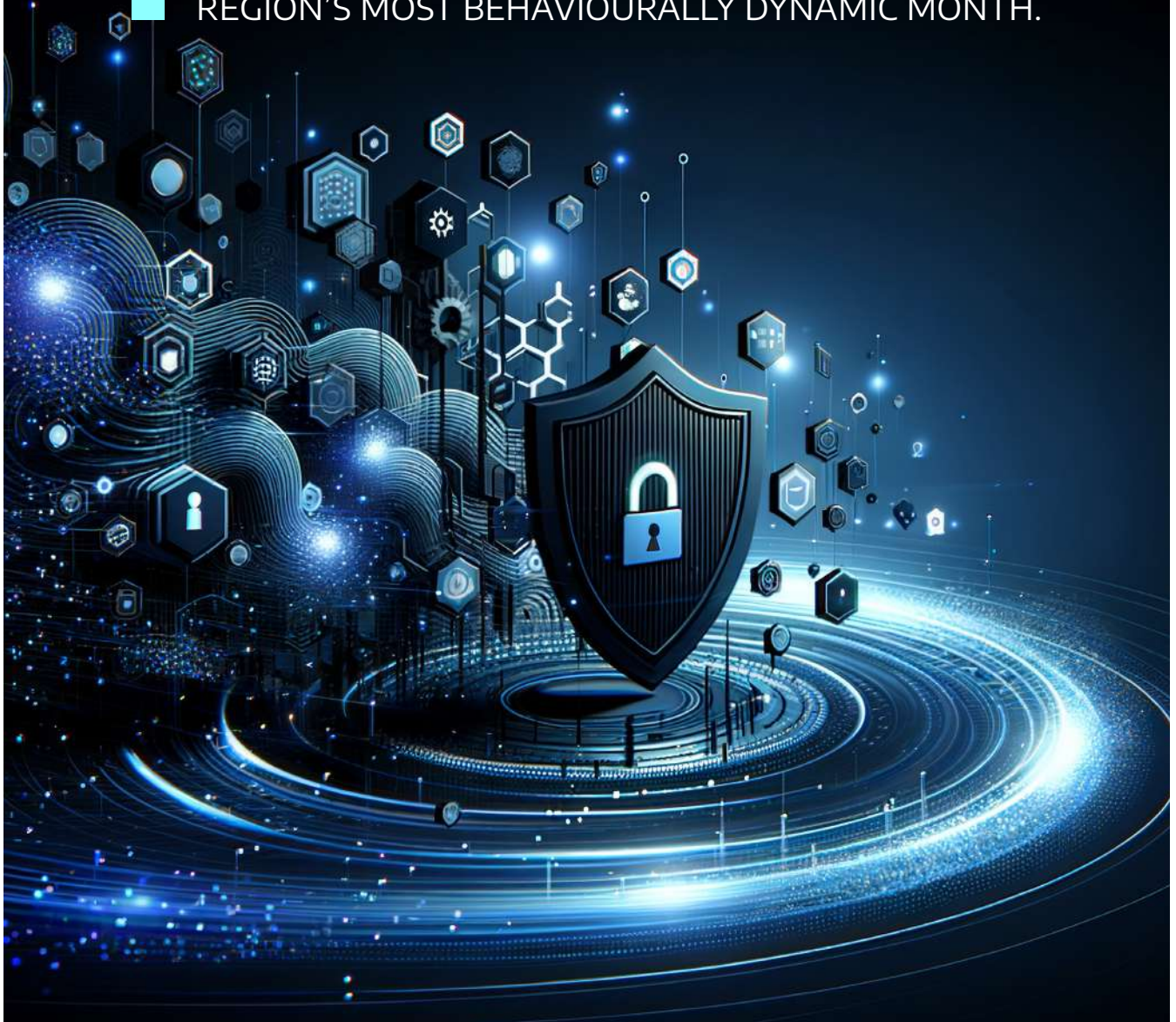
- AI annotation: Instantly generate summaries and contextual insights for charts and visuals, without manual writing, enhancing clarity across your data estate
- Resilient AI features: Robust features now handle transient issues and provide detailed usage analytics for easy monitoring and optimisation
- AI query logging and traceability: Each AI query logs message ID, timestamp, and question for traceability, streamlining transparency and issue resolution
- Simplified admin management: Easily assign admin roles using updated configuration parameters to streamline SSO-based setup by removing hard-coded credentials and manual user promotion

"These advancements provide our customers with a superior level of control and flexibility," said Leo Brunnick, Chief Product Officer at Cloudera. "With Cloudera AI Inference, Cloudera Data Warehouse with Trino, and Cloudera Data Visualization all accessible in the data center, organisations can securely deploy AI and analytics exactly where their most critical data resides. This means enterprises can drive innovation and derive insights without compromising on data security, compliance, or operational efficiency."

"The value of enterprise data is realised when AI can be securely and flexibly deployed where that data lives," said Pat Lee, vice president, strategic enterprise partnerships, NVIDIA. "Our collaboration with Cloudera enables customers to deploy and scale AI inference using NVIDIA Blackwell GPUs, Dynamo-Triton and NIM microservices, delivering control, predictable economics, and data-center efficiency."

# CYBERSECURITY DURING RAMADAN: SHIFTING THREAT PATTERNS AND STRATEGIC RESILIENCE

CISOS MUST RECALIBRATE OPERATIONS, IDENTITY CONTROLS AND DETECTION MODELS DURING THE REGION'S MOST BEHAVIOURALLY DYNAMIC MONTH.



**R**amadan is a period of spiritual reflection, generosity, and community across the Middle East. For enterprises, however, it is also a month marked by distinct operational and behavioural shifts. Reduced working hours, heightened evening digital activity, increased charitable giving, and surging e-commerce transactions create a unique cybersecurity profile that differs markedly from the rest of the year.

Threat actors understand these patterns well; regional threat intelligence consistently shows that Ramadan is not defined by entirely new attack techniques, but by the amplification of familiar tactics adapted to exploit seasonal behaviours. For CISOs across the GCC and wider MENA region, the challenge lies in maintaining resilience during altered working schedules without overextending security teams. Threat actors are not reinventing their methods — they are refining their timing and localisation.

Meriam ElOuazzani, Vice President for Middle East, Turkey, and Africa, Censys, said, “Ramadan brings a surge in online financial activity, making it a key inflection point in the regional threat landscape. With donations and e-commerce transactions rising, attackers register short-lived domains impersonating charities, retailers, banks, and logistics providers, often using Arabic keywords linked to zakat, Eid promotions, and delivery alerts to appear legitimate. Telemetry also indicates heightened credential attacks on misconfigured VPNs and remote access services during reduced working hours.”

The campaigns are increasingly localised, time-sensitive, and financially motivated, relying on disposable infrastructure that can be quickly deployed and abandoned, she added.

During Ramadan, the threat



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

landscape does not necessarily become more sophisticated; it becomes more human-centric. Attackers exploit trust, generosity, and increased night-time digital engagement, focusing on high-velocity social engineering.

Keyur Shah, Associate Field CISO, Sophos, said, “We consistently see charity and Zakat-themed phishing, delivery impersonation via SMS or WhatsApp, and localised Eid-offer scams designed for rapid monetisation. Regional logistics providers are

frequently spoofed to drive credit card harvesting and account takeover. QR-code phishing and mobile-first attacks also rise as users rely more on digital payments. What truly differentiates Ramadan threats is psychology — culturally aligned lures, Arabic messaging, and post-iftar activity patterns that significantly increase engagement and conversion rates.”

#### **Predictable Shift in Digital Behaviour**

The tactics may appear seasonal, but

the underlying intrusion paths remain largely unchanged. Mortada Ayad, Director – Sales Engineering, Delinea, argued that Ramadan should not be mistaken for a quieter period.

“The attacker’s playbook does not fundamentally change. The same identity-led intrusion paths remain. Instead, what changes is the packaging,” said Ayad.

Shorter working hours and more active evenings create predictable digital behaviour. Across markets such as the UAE, Saudi Arabia, and Qatar,

usage of finance, e-commerce, and food delivery applications rises measurably during the holy month. Attackers follow that shift closely, driving spikes in Ramadan and Eid-themed phishing and smishing campaigns tied to charity appeals, zakat donations, exclusive promotions and delivery notifications. The emotional context — centred on generosity, family and community — makes social engineering more persuasive.

Government entities and private-sector organisations across the region

typically implement reduced working hours during Ramadan. At the same time, consumer and employee digital engagement shifts to late evenings and early mornings. Post-Iftar and pre-Suhoor periods often see spikes in mobile usage, online shopping, streaming and social media interaction.

This behavioural pivot creates an unusual asymmetry: digital activity peaks outside traditional business hours, while security operations centres (SOCs) may be operating with leaner staffing models. The result is a compressed response window. Incidents that would normally be identified and triaged during daytime hours may go undetected for longer periods.

**Keyur Shah**  
Associate Field CISO  
Sophos.



### **From Consumer Lure to Enterprise Risk**

The apparent consumer focus of many Ramadan scams can be misleading. Ayad noted that attackers are increasingly targeting individuals rather than organisations directly. “Shorter working hours, more personal device usage in the evenings, and the blurred lines created by BYOD environments create a softer entry point. Compromising a personal account or device can still provide a pivot into corporate systems if identity controls are weak.”

What begins as a charity-themed phishing message or delivery notification can escalate into credential compromise and lateral movement within enterprise environments. Heightened bot activity and availability attacks against e-commerce platforms and digital services further increase exposure, as transaction volumes surge and incentives for fraud and disruption grow. Again, the tactics are not new — the timing and targeting are.

### **Distinct Attack Patterns During Ramadan** **Phishing Leveraging Religious Themes**

One of the most consistent trends

observed across the region is a surge in phishing campaigns exploiting religious sentiment. Fake charity appeals, fraudulent zakat platforms and spoofed donation portals proliferate. These campaigns frequently use culturally authentic Arabic-language templates and impersonate recognised regional organisations.

### **E-commerce and Payment Fraud**

#### **Spikes**

Ramadan represents a peak spending period comparable to major global retail events. Attackers pivot towards card-not-present fraud, account takeovers and fake payment gateway attacks. Smaller retailers, expanding online operations without proportional fraud controls, are particularly exposed.

### **Night-Time Credential and VPN Attacks**

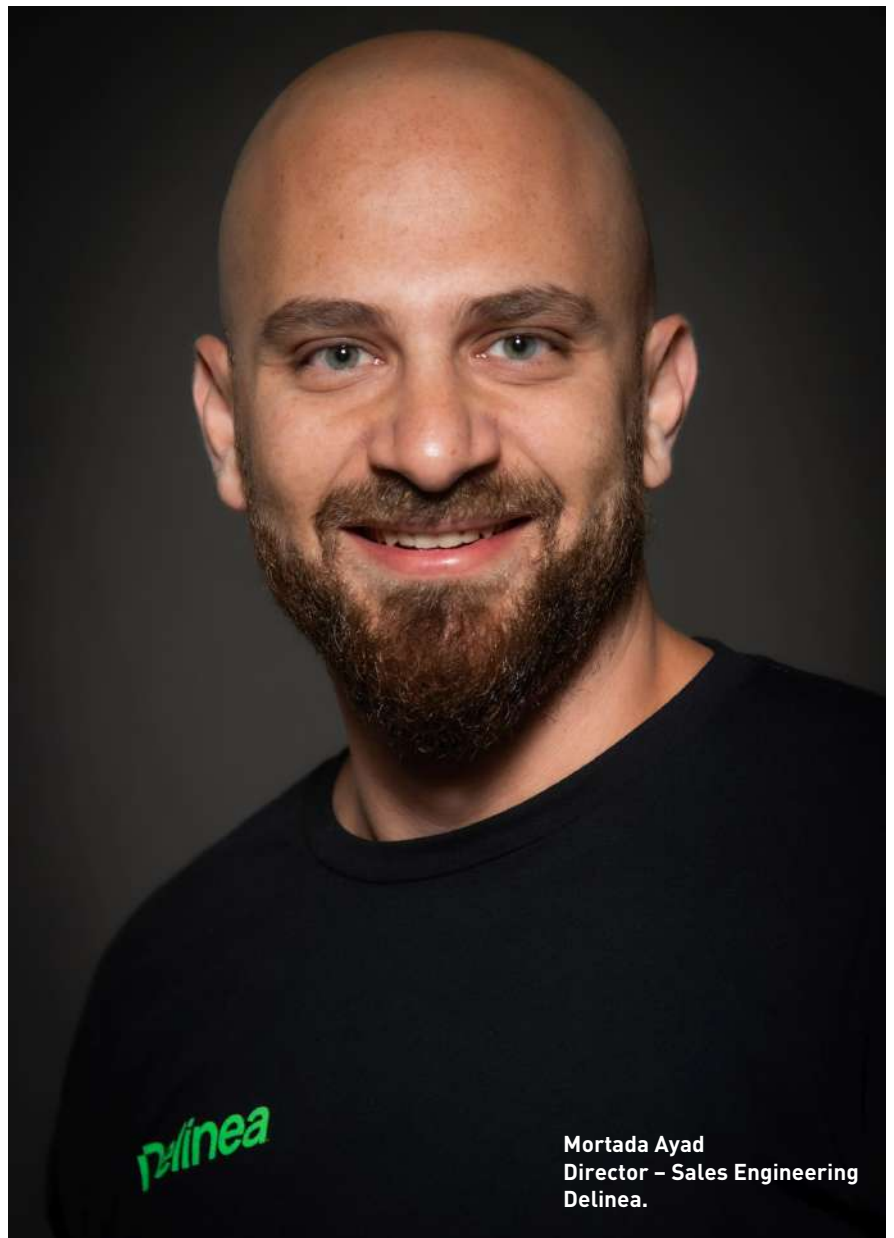
Regional telemetry shows a shift in attack timing during Ramadan. Brute-force attempts, credential stuffing and VPN exploitation are more likely to peak during late-night hours when user activity is high but monitoring coverage may be thinner. Cloud authentication services and privileged access systems become attractive targets.

### **Ransomware Timing Strategies**

Ransomware operators often seek maximum leverage, timing deployments to coincide with weekends during Ramadan or immediately before Eid holidays, when executive availability may be limited.

### **Ramadan Differs from the Rest of the Year**

The techniques remain familiar, but context amplifies effectiveness. Heightened generosity increases susceptibility to donation fraud. Altered sleep cycles reduce vigilance. Remote access from home networks becomes more frequent. Executive oversight windows narrow.



**Mortada Ayad**  
Director – Sales Engineering  
Delinea.

Ezzeldin Hussein, Regional Senior Director, Solution Engineering, META, SentinelOne, said attackers weaponise cultural relevance and timing. “Ramadan introduces a strong behavioural component. We need to be more concerned about psychological precision at scale.”

### **Operational Adjustments for CISOs**

Resilience during Ramadan does not require indiscriminate tool expansion. It requires operational alignment.

Mortada Ayad cautioned against

assuming a slowdown. “Operationally, it is not slower. Activity simply shifts. The first thing CISOs should do is look at their own data from previous years. When did alerts spike? Let telemetry guide shift adjustments rather than assumptions.”

Aligning SOC coverage with post-Iftar peaks, adjusting on-call structures and simplifying operations during high-risk windows are critical steps. Ramadan is not the time for complex migrations or non-essential system changes.

Yet operational alignment alone is

insufficient without proactive visibility into external exposure. Meriam ElOuazzani advised preparation ahead of the surge. Tracking lookalike domains targeting brand assets, payment portals or charity initiatives, and placing automated alerts on certificate and infrastructure changes, can reduce exposure before activity spikes. Visibility across VPN, RDP and cloud services should be expanded, particularly during reduced working hours. AI-driven search and triage tools can improve prioritisation without increasing analyst burden.

Visibility must then translate into sustainable response capacity. Ezzeldin Hussein stressed the importance of automation and clarity in incident response. "Security leaders must adapt to the change in operational rhythm. AI-based detection and automated response reduce manual triage and analyst fatigue. Authority for decision-making should be clearly defined, especially if leadership is not accessible."

Ultimately, resilience depends on recalibrating detection models to match behavioural change. Keyur Shah added that resilience comes from smarter alignment, not additional alerts. "Ramadan doesn't introduce new threats, it changes the tempo of risk. CISOs should prioritise identity-first detection, recalibrate telemetry baselines and pre-define response playbooks."

Strengthening identity governance remains central. Removing standing administrative rights, enforcing least privilege and implementing Just-in-Time privileged access can significantly reduce the impact of a successful phishing attempt. Strong identity controls prevent consumer-facing lures from escalating into enterprise breaches.

### Looking Ahead

The sophistication of AI-generated phishing content is likely to intensify



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

Ramadan-themed campaigns in the years ahead. As digital payment ecosystems expand across the GCC and broader MENA region, cross-border fraud risks will also grow during high-transaction periods.

Ramadan should therefore be treated not as an anomaly, but as a recurring seasonal threat cycle. Organisations that integrate it into annual risk

planning — aligning operational coverage with behavioural shifts, strengthening identity controls and leveraging automation effectively — will enter the holy month prepared rather than reactive.

For cybersecurity leaders in the region, the message is clear: attackers plan for Ramadan. Defenders must do the same. 🔒

 tahawultech.com

# Women in TECHNOLOGY FORUM AND AWARDS

*Give to gain. Powering women in tech*

Gala Dinner Event



30<sup>th</sup> March 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 March 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/>

# CYBER RESILIENCE DEMANDS HUMAN-LED AI, SAYS AMPCUS CYBER

**DEEP CHANDA** OF AMPCUS CYBER ON WHY COMPLIANCE IS NO LONGER ENOUGH IN AN AI-DRIVEN THREAT LANDSCAPE.

Cyber resilience is entering a decisive new phase. Traditional, rule-based compliance frameworks — once considered the backbone of enterprise security — are proving insufficient in a threat landscape shaped by AI-powered attacks, complex digital ecosystems, and expanding regulatory demands. Organisations are under pressure not only to defend against increasingly intelligent adversaries, but also to rethink how security, privacy, and governance intersect across legacy systems, payment networks, and cross-border data flows.

Deep Chanda, Chief Officer at Ampcus Cyber, outlines why resilience today is less about ticking compliance boxes and more about cultivating adaptive, human-led security strategies powered by AI. From the evolving risks within digital payment ecosystems to the practical realities of implementing Zero Trust in legacy environments, he argues that automation alone cannot solve modern cyber challenges.

**REAL CHANGE IS GOING TO BE EMBRACING THAT SECURITY IS NEVER COMPLETELY DONE.**

Security, Chanda suggests, must be treated as an ongoing discipline — one that balances machine speed with human judgement, integrates privacy into operational architecture, and measures readiness not by regulatory alignment but by performance under pressure.

#### Interview excerpts:

#### How is the shift from rule-based compliance to AI-driven, human-led security changing the way enterprises approach cyber resilience today?

There is an emerging theme that AI by itself will be the replacement for traditional security thinking, but this is not exactly what is happening. The real change in cyber resilience is that rule-based compliance was never intended for a dynamic threat environment. AI offers speed and scale, but resilience requires human intelligence. Verizon's research indicates that more than 80 percent of breaches involve a human component that cannot be predicted by any rulebook. Real change is going to be embracing that security is never completely done. It is true that AI facilitates resilience, but humans are still responsible for risk interpretation.

#### With your deep background in PCI and payment security, what are the biggest emerging risks facing digital payment ecosystems right now?

Most people think that the risks

associated with payment security are primarily due to outdated encryption or lax PCI controls. I believe that's a matured layer now, and there are more risks lurking out there. The bigger risks lie outside the payment transaction itself. APIs, third-party dependencies, and real-time payment orchestration are the areas IBM believes the average breach cost is now over \$4.8 million. Payment data breaches are among the most disruptive breaches. We're also seeing AI-powered fraud attacks that evolve much quicker than rule engines can keep up with. Another risk that is often overlooked is the ecosystem's fragility, where a single breached vendor can affect dozens of institutions.

#### How does a Zero-Trust model evolve in real-world enterprise environments that still rely on legacy systems?

Zero-Trust is rarely a clean-slate architecture. Most companies cannot simply walk away from their legacy infrastructure without exposing themselves to risk. Zero Trust does not need to be a complete modernisation effort upfront. Instead, it is an evolutionary process where it begins with identity, access and then continuous verification around the legacy workload. Gartner forecasts that 50 percent of organisations will adopt zero Trust as a fundamental principle by 2028, but not as a finished architecture. The key to success is in the gradual reduction of

implicit trust. Zero Trust is something that can be practiced as a discipline, not a product.

**What common gaps do you see between regulatory compliance and actual security readiness inside large organisations?**

There is a dangerous assumption that compliance equals preparedness. The problem is that regulations are based on minimum standards, not attack scenarios. There is a gap in what is known as vulnerabilities and misconfigurations that continue to be the leading cause of breaches, even in compliant companies. There is also a gap in ownership of the organisation in terms of who is responsible for compliance and who is responsible for security incidents. Compliance is the responsibility of governance teams, while security incidents affect IT and business leaders. The gap will continue until organisations are able to assess their security based on how they perform under pressure.

**How should CISOs balance automation, AI, and human expertise in their defence strategy?**

There is a temptation to automate all things, but full automation should not be the goal. AI is great at pattern recognition and speed, but not so good at context or intent. IBM states that organisations leveraging AI and automation can lower breach costs by more than 20 percent, but only when combined with human expert teams. Humans remain better than machines at business impact assessment and working in uncertain environments. The key is orchestration. Let the machines

**Deep Chanda**  
Chief Officer  
Ampcus Cyber



handle all the noise and the humans make the key decisions. CISOs need to concentrate on enhancing analysts, not replacing them. The best approaches to defence will be a combination of AI, automation, and human intelligence.

**With rising global data regulations and cross-border data flows, how should organisations rethink data privacy governance beyond just meeting compliance checklists?**

Organisations respond to new privacy laws by creating more policies. This is not the most efficient or effective way in the

long run. Just being compliant does not mean privacy is being protected. Gartner predicts that almost 65 percent of the world's population will be protected by privacy laws by 2026, but breaches are still on the rise. The problem is that there is a lack of visibility of the data. Most organisations do not know where the sensitive data is or how it flows. Privacy governance needs to be operational. It needs to be integrated into data architecture and access. Real privacy governance is all about operational insights. When built into systems, it enables good data practices. 🔑

**AI OFFERS SPEED AND SCALE, BUT RESILIENCE REQUIRES HUMAN INTELLIGENCE.**

# DEEPFAKES, VOICE CLONING, AND AI-GENERATED IDENTITIES FUEL SURGE IN ROMANCE SCAMS

**ROB WOODS**, SENIOR DIRECTOR OF FRAUD AND IDENTITY AT LEXISNEXIS RISK SOLUTIONS, EXPLAINS HOW DEEPFAKES, VOICE CLONING, AND AI-GENERATED IDENTITIES ARE FUELLING A SURGE IN EMOTIONALLY MANIPULATIVE FINANCIAL FRAUD ACROSS THE MIDDLE EAST.

Romance fraud has shifted from sporadic online deception to a sophisticated, organised financial crime affecting individuals and institutions across the Middle East. Criminal networks now operate with alarming precision, exploiting emotion, technology, and trust to orchestrate scams that can cause lasting financial and psychological harm.

Advances in artificial intelligence, deepfakes, and voice cloning have significantly elevated the scale and credibility of these schemes. Fraudsters are no longer limited to stolen photographs or fabricated backstories. Highly realistic identity documents, AI-generated images, live video interactions and convincing social media profiles enable scammers to construct persuasive narratives that are increasingly difficult to detect. The result is a more immersive and manipulative experience for victims — one designed to build trust before exploiting it.

Beyond financial loss, romance scams inflict deep emotional trauma. Victims are often groomed into secrecy, discouraged from sharing details of the relationship,

and manipulated through urgent appeals for money under fabricated crises. Shame, embarrassment and psychological coercion frequently prevent reporting, allowing organised networks to continue operating unchecked.

Rob Woods, Senior Director of Fraud and Identity, LexisNexis Risk Solutions, spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, on how romance scams have evolved, the role emerging technologies play in accelerating the threat, the warning signs individuals must recognise, and the immediate steps to take when suspicion arises.

## Interview excerpts:

### **How have romance scams evolved from isolated online cons into a large-scale, organised financial crime across the Middle East?**

The abundant availability of AI and deepfake technology is certainly adding fuel to the fire of scams. Romance scams rely on the scammer weaving intricate stories which, more now than ever before, can be backed up with highly realistic content, such as identity documents, photos, recorded videos, live video chats

and social posts generated by AI to help convince the target they are genuine.

### **What role are AI / deepfakes / voice cloning playing in making romance scams more convincing and harder to detect?**

AI is certainly being harnessed to create convincing and realistic content for a host of scams, and that includes romance fraud. With romance scams, once the target has been groomed for a time, the fraudster will invent reasons why they urgently need cash, for example, to pay for a sick relative's operation or pay a court fine to avoid prison. Bad actors use AI to generate fake documents or photos to add credibility to these stories and convince the target. In the past, romance scammers relied on random photos and information scraped from the internet; now they have far more sophisticated tools at their disposal.

### **Which red flags should people never ignore when forming relationships online, even if the interaction feels genuine?**

One key tell-tale signal that scammers employ is insisting on secrecy, urging the



**Rob Woods**  
Senior Director of Fraud and Identity  
LexisNexis Risk Solutions.

victim not to discuss their relationship with others. This is an important tactic and enables the fraudster to retain control of the scam and influence over the target. Our advice to anyone asked to keep an online relationship secret is to confide in a trusted friend or family member, even if you don't think it's a scam, because, if it is, it's the best way to break the spell. Another common tactic is that the scammer will initially lavish expensive gifts on the target to lull them into a false sense of security. This is simply a tactical investment on the scammer's part as they know it will pay dividends later on.

**Why do many victims suffer in silence after falling prey to romance scams, and**

**what psychological impact does this type of fraud have beyond financial loss?**

Romance fraud is unique in that it may only go on for a few weeks or months, but the emotional impact of the deception can last a lifetime. It's such a pernicious crime because it preys on people's determination to believe that the romance is real and ignore the obvious warning signs. Shame and embarrassment play a big part in the lack of reporting but it's also to do with tactics, as romance scammers tend to encourage targets to be secretive and conceal what's happening from others. They do this to retain control of the scam and influence over the target because generally, if the target tells someone

else what's going on, that person quickly points out the risks.

**If someone suspects they are being targeted or has already been scammed, what immediate steps should they take to protect themselves and others?**

The best advice is really to confide in someone you trust. Even if you don't think it's a scam, another person's perspective can't do any harm. Look for the warning signs, especially if you're being asked to keep the relationship a secret and especially if they start telling you stories about urgently needing money, whether in the form of cash, gift cards or rewards points. These are clear flags that something is amiss. 🚩

# PNY TECHNOLOGIES MEA BUILDS BACKBONE OF ENTERPRISE AI IN EGYPT AND MIDDLE EAST

WITH OVER 25 YEARS AS A GLOBAL NVIDIA PARTNER, PNY IS HELPING ENTERPRISES ACROSS EGYPT AND THE MIDDLE EAST BUILD PRODUCTION-GRADE AI INFRASTRUCTURE.



**Talus Arukalil**  
Regional Manager  
PNY Technologies MEA

Enterprise AI across Egypt and the wider Middle East is entering a decisive new phase. Organisations are moving beyond pilot projects and proofs-of-concept towards production-grade deployments that demand robust infrastructure, sovereign capabilities, and long-term scalability. National AI strategies, growing data centre investments, and a maturing ecosystem of integrators and cloud partners are accelerating this shift from experimentation to enterprise execution.

Against this backdrop, infrastructure readiness has emerged as the defining challenge. Ambition and talent are abundant across the region, yet many organisations require validated, high-performance platforms capable of supporting real-world AI workloads with predictable performance, security, and resilience. At AI Everything Egypt, PNY Technologies positioned itself at the centre of this transformation.

With more than 25 years as a global NVIDIA partner and deep expertise in GPU-accelerated computing, PNY is bringing enterprise-ready AI platforms, integration services, and end-to-end data centre capabilities to support organisations as they transition from experimentation to scalable, production-ready AI.

In the following interview excerpts, Talus Arukalil, Regional Manager, PNY Technologies MEA, outlines how the

company is helping shape Egypt and the wider Middle East into serious markets for enterprise AI infrastructure — and why validated, high-density, and future-ready systems are critical to the region's AI ambitions.

#### **Interview Excerpts**

#### **How does PNY Technologies see Egypt and the wider Middle East evolving as serious markets for enterprise AI infrastructure rather than just AI adoption?**

We see Egypt is fast evolving from an AI adopter into builders of enterprise-grade AI infrastructure. The focus is shifting from experimenting with AI tools to investing in sovereign, scalable, GPU-accelerated platforms that support production workloads. Driven by strong national AI strategies, expanding data center capacity. With a growing ecosystem of integrators and cloud partners, Egypt and the Middle East are becoming strategic markets where enterprise AI infrastructure is designed, deployed, and scaled locally.

#### **What gap in the regional AI ecosystem are you aiming to address by bringing solutions like NVIDIA DGX Spark and RTX PRO Blackwell-powered workstations to AI Everything Egypt?**

We are bridging the gap between strong AI ambition and the availability of enterprise-ready, production-grade infrastructure. Many organisations have clear use cases and growing talent but lack validated platforms to move AI from experimentation to production. By bringing NVIDIA DGX Spark and RTX PRO Blackwell-powered workstations to AI Everything Egypt, we enable organisations to develop, train, and deploy AI locally with predictable performance, data sovereignty, and scalable architectures.

#### **How is PNY working with NVIDIA to help organisations move from AI experimentation to scalable, production-ready AI deployments?**

PNY has been a global NVIDIA partner



for over 25 years, delivering solutions across the full NVIDIA portfolio. Together, we help organisations transition from experimentation to production-ready AI through validated platforms like DGX systems and RTX-accelerated workstations, AI servers & clusters. By combining NVIDIA's technology with PNY's integration expertise and local support, we simplify deployment and enable enterprises to scale AI with confidence.

#### **How does PNY's portfolio help simplify the journey to AI-ready infrastructure?**

Enterprises need high-performance hardware, scalable infrastructure, and secure systems. PNY addresses this with validated solutions, including DGX systems and collaborations with OEMs for HGX platforms, backed by our GPU expertise since the early days. Beyond hardware, we offer a comprehensive data center ecosystem — storage, networking, infrastructure development, and certified technical expertise — simplifying architecture, deployment, and scaling. This end-to-end approach accelerates AI adoption with control, predictability, and performance. Additionally, through our collaboration with Vertiv, PNY has the

capability to deliver complete power and cooling solutions tailored for AI and high-density GPU environments. This ensures that customers benefit from optimised energy efficiency, thermal management, and infrastructure resilience, which are critical for sustainable and scalable AI deployments. This end-to-end approach accelerates AI adoption with control, predictability, performance, and long-term operational stability.

#### **Beyond hardware, how is PNY positioning itself as a long-term AI partner in the region?**

PNY positions itself as a long-term AI partner by delivering end-to-end solutions for HPC, data science, and accelerated computing. With over 25 years as a global NVIDIA partner, PNY has deployed multiple AI clusters regionally and globally and collaborates with all NVIDIA-approved storage, networking, and data center partners. Combined with integration services, reference architectures, and certified local support, this enables organisations to design, deploy, and scale AI efficiently while maintaining control and performance. 🔑

# THE YEAR OF RESILIENCE: WHAT WILL 2026 DEMAND FROM CISOS?

**I** AI-DRIVEN RISK, GEOPOLITICAL DISRUPTION, AND NONSTOP CYBER PRESSURES ARE FORCING CISOS TO RETHINK RESILIENCE, GOVERNANCE, AND BUSINESS CONTINUITY.

Last November, Fortinet published “CISO Predictions for 2026,” which outlined the forces shaping the year ahead, including rapid AI adoption across every business function, escalating geopolitical tension, expanding regulatory pressure, and the continued industrialisation of cybercrime. The conclusion was direct: The attack surface is expanding faster than traditional security models can adapt.

While these predictions explain what is coming, CISOs will have to decide how to address these challenges in an environment where AI accelerates both innovation and risk. According to the World Economic Forum’s Global Cybersecurity Outlook (GCO) 2025, 72% of organisations reported that cyber risk increased over the past year. In 2026, that risk will increasingly be shaped by AI systems making decisions at machine speed, often outside traditional security workflows.

The challenge for CISOs will not

be preventing every failure. It will be ensuring the business continues to function when AI-enabled disruption occurs. Resilience is no longer simply a byproduct of security. It must be the organising principle.

## From CISO to Chief Resilience Officer

The boundary between IT risk and business risk has collapsed, accelerated by AI’s deep integration into operations, decision-making, and customer engagement. AI systems now influence supply chains, financial controls, hiring decisions, and customer interactions, often with minimal human intervention.

As a result, CISOs are no longer responsible only for securing systems. They are responsible for ensuring that AI-augmented business processes remain trustworthy, available, and controllable under stress. In practice, CISOs have already begun operating as chief resilience officers.

This evolution reflects reality. AI increases speed, scale, and dependency. In

that environment, when failures occur, they propagate faster and farther. So in 2026, CISOs will need to assume that disruption will involve AI-enabled components, whether through compromised models, poisoned data, manipulated agents, or automated misuse. Success will be measured by how well organisations absorb and contain those failures.

## What CISOs Are Hearing in World Economic Forum Engagements and Why 2026 Is Different

World Economic Forum Annual Meeting discussions and forum initiative activity have decisively moved AI beyond a purely technological discussion. It is now treated as a governance, risk, and resilience issue with direct implications for economic stability, national infrastructure, and global trust. Conversations increasingly focus on systemic exposure: the concentration of AI capability, reliance on shared models, cross-border data dependencies, and the risk of cascading failure when highly connected and automated systems behave unexpectedly.

Fortinet participates in these discussions, including at this month’s Annual Meeting in Davos, alongside government leaders, industry executives, and security practitioners, because what happens in these forums shapes how risk is understood and managed at a

**THE CHALLENGE FOR CISOS WILL NOT BE PREVENTING EVERY FAILURE. IT WILL BE ENSURING THE BUSINESS CONTINUES TO FUNCTION WHEN AI-ENABLED DISRUPTION OCCURS.**



**Carl Windsor**  
**CISO**  
**Fortinet**

global level. Cybersecurity is no longer framed as an enterprise problem, but as a shared responsibility that cuts across public and private sectors. For CISOs, such conversations matter because they influence regulatory direction, executive expectations, and the standards by which resilience will be judged.

This shift is also reflected in organisational governance models.

CISOs are gaining more direct access to executive leadership because boards now recognise that AI-related risk cannot be delegated to isolated teams. Instead, decisions about AI deployment, data access, automation, and control structures have direct consequences for operational continuity, regulatory exposure, and corporate reputation.

For CISOs, the implication is clear. In

2026, resilience planning must explicitly account for AI-driven scale, speed, and opacity. The question is no longer whether AI will be used, but whether it is being deployed in a way that is secure, transparent, and aligned with business risk tolerance. The discussions taking place in Davos reinforce that this is no longer a theoretical concern. It is a leadership responsibility. 🔑

# FLASH POINT: ADDRESSING CYBERSECURITY SHORTCOMINGS OF OT INDUSTRY'S INHERENT RISK

Over the past decade, the evolution of Operational Technology (OT) has been nothing short of impressive. Industrial environments that were once isolated, opaque and stubbornly analogue have steadily embraced digital transformation. IT/OT convergence has unlocked new levels of visibility and efficiency. Cloud-connected monitoring, advanced analytics, remote operations and predictive maintenance have reshaped how critical infrastructure is managed across energy, utilities, manufacturing and transportation. Cybersecurity, too, has matured, moving beyond basic perimeter defences towards more comprehensive, risk-driven strategies.

Yet for all this progress, some operational approaches remain firmly embedded in OT environments. One of the most enduring, and arguably most problematic, is removable media.

## A Necessary Evil

USB drives, external hard disks and other portable storage devices continue to play a vital role in OT operations, particularly where air-gapped or highly segmented systems are involved. Software updates, configuration changes, diagnostic data and patching often still rely on physical transfer rather than network connectivity. In many facilities, removable media is not just essential; it is operationally unavoidable.

This is why removable media has become the OT industry's inherent risk: it introduces a physical threat vector into an increasingly digitally enabled security strategy. Yet eliminating removable media entirely is neither practical nor realistic. Instead, organisations have embraced its use, integrating it seamlessly into tasks, processes and day-to-day workflows to support operational efficiency.

## Mainstream Security Approaches

Security teams recognise the risks associated with removable media. Over time, most organisations have implemented a range of controls to mitigate the more obvious threats associated with removable media. Access to areas where removable devices are used is carefully controlled, ensuring only authorised personnel can handle sensitive data. Data stored on these devices is protected through encryption, safeguarding information in case of loss or theft. Employees are regularly trained on safe handling practices, while malware scanning tools inspect files before they enter or leave controlled environments.

These measures are commendable and, importantly, effective against a certain class of threat. They reduce the likelihood of infected USB drives introducing malware into critical systems, limit the damage caused by misplaced or stolen devices and help prevent careless or accidental misuse. In

short, they address the opportunistic and unintentional risks that removable media brings into OT environments.

## Insiders: The Overlooked Threat

However, one category of threat remains consistently under-addressed: the insider.

Most removable media controls are designed with external attackers or honest mistakes in mind. They implicitly assume that users with legitimate access will act in the organisation's best interests. Yet history repeatedly demonstrates that insider threats (whether malicious, disgruntled or opportunistic) can be just as damaging, and often harder to detect, than attacks from outside the organisation.

A recently reported case in which a former engineer at Intel allegedly downloaded 18,000 confidential files before disappearing offers a timely warning. While this incident did not occur in an OT environment, it illustrates a universal truth: when individuals have legitimate access to systems and data, traditional perimeter- and device-centric controls only offer limited protection. Once data is copied to removable media, it can be taken anywhere, instantly bypassing millions of dollars' worth of network-focused security investments.

## Where Traditional Removable Media Policies Fall Short

In many OT environments, the same structural weakness exists. Engineers,

**OVER TIME, MOST ORGANISATIONS HAVE IMPLEMENTED A RANGE OF CONTROLS TO MITIGATE THE MORE OBVIOUS THREATS ASSOCIATED WITH REMOVABLE MEDIA.**

**Hussam Sidani**  
Vice President, Middle East,  
Turkey & Africa  
OPSWAT



operators and contractors often require elevated privileges to perform their roles effectively. In these positions, removable media is trusted as a legitimate mechanism for moving data in and out of controlled zones. Yet controls frequently stop short of inspecting what data is being transferred, why it is being moved, or whether that action aligns with the individual's role and responsibilities.

This creates a gap between access and accountability, a gap that insider threats are uniquely positioned to exploit.

**Shifting the Focus from Devices to Context**

Addressing this gap requires a shift in mindset. Rather than treating removable media as a binary risk, i.e. either permitted or prohibited, organisations need to focus on context. Key questions to consider include: Who is transferring the data? What type of data is it? Where is it going? Based on the answers, organisations can then evaluate whether the transfer is appropriate given the user's role and the task being performed.

This is where role-based access and content-aware controls become critical. Instead of assuming that any authorised user has the right to move any file, organisations should enforce policies that align data movement with job function and data sensitivity. An engineer, for example, may legitimately need to transfer configuration files to an approved device, but have no operational justification for copying large volumes of sensitive documentation or proprietary data. A contractor may require time-limited access to specific assets, but not unrestricted use of removable media across systems.

**Why Inspection, Visibility and Auditability Matter**

Content inspection plays a complementary role. By scanning files before they are copied to removable media, organisations can identify sensitive or regulated information such as intellectual property, personal data or credentials and prevent



it from inappropriately leaving controlled environments. Crucially, this shifts enforcement from the network perimeter to the point of action, ensuring that controls remain effective even in air-gapped or offline scenarios.

Visibility is the another critical piece of the puzzle. Many organisations still lack a comprehensive audit trail of removable media usage. Knowing which device was connected, by whom, at what time, and what data was transferred provides invaluable context. It enables security teams to detect anomalies early, such as repeated attempts to copy data or the use of unauthorised devices. Just as importantly, it creates accountability, reinforcing that removable media usage is governed, monitored and intentional.

**Strengthening Security Without Disrupting Operations**

None of these efforts eliminate insider risk entirely. No single control or technology can. However, a layered approach that combines role-based policies, content awareness, auditability and the ability to intervene in real time,

significantly raises the bar. It transforms removable media from a blind spot into a managed, controlled process.

For OT environments, this approach offers a further advantage by respecting operational realities. Air-gapped systems remain air-gapped. Engineers can still perform critical tasks. Legacy workflows do not need to be dismantled overnight. Instead, organisations add intelligence and governance around a practice that is unlikely to disappear in the foreseeable future.

**Old Tool Adapted to New Realities**

In a world where cyber threats are increasingly digital, it is easy to overlook the physical pathways through which data travels. Removable media may feel old-fashioned, but its security implications remain critical. Treating it as a necessary evil is no longer sufficient. By acknowledging insider risk and embracing role-based, context-aware controls, OT organisations can finally bring one of their oldest operational tools into alignment with a modern cybersecurity strategy. 🔒

# KSA FUTURE ENTERPRISE AWARDS 2026



12<sup>th</sup> April  
2026



Radisson Blu Hotel & Convention Center  
Riyadh Minhal



06:30 PM onwards

**#KSAFEA2026 | #tahawultech**

In November, 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 SPONSORS



**AHAD**  
Securely Transform

**logitech®**

## OFFICIAL PUBLICATIONS

**cnme**  
computer news middle east

**Reseller** MIDDLE EAST  
THE JOBS OF THE CHANNEL

**Security** MIDDLE EAST  
SECURITY

## 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/>

# DATA SOVEREIGNTY: AN EXISTENTIAL ISSUE FOR NATIONS AND ENTERPRISES

**GEOPOLITICS, REGULATION AND CLOUD DEPENDENCY ARE REDEFINING CONTROL, JURISDICTION AND DIGITAL RESILIENCE.**

**D**ata has long been recognised as an organisation’s most valuable asset, arguably more important than physical infrastructure or even brand. This is reflected by intangible corporate assets, primarily data including R&D and intellectual property, exceeding \$60 trillion in value in 2024. When used effectively, data unlocks competitive advantage, new markets, better decisions, and helps deliver transformative customer experiences.

Given how critical data is to the day-to-day operations of modern businesses, it needs to be managed, and safeguarded, more than ever. As global geopolitical uncertainty persists, the topic of data sovereignty has become top of mind for governments, regulators, and businesses.

## **Data residency, data sovereignty**

Defined as the principle that data is subject to the laws and governance structures of the country in which it is collected or stored, data sovereignty concerns who has the authority to dictate how data is managed, accessed, and used, particularly in an increasingly interconnected and data-driven world.

For a long time, companies believed data sovereignty simply meant where their data resided, but amid geopolitical shifts and AI’s impacts, organisations now need to distinguish between data residency – where data is physically

stored, and data sovereignty – who has legal jurisdiction over that data.

## **Data sovereignty risks; a perfect storm**

Today, new risk factors are reshaping the data sovereignty landscape and pose new questions over access to and use of business-critical data. Geopolitical conflicts, emerging regulations, international competition and the desire for tighter control of data to power innovation, are forcing company leaders to reconsider their business-critical data’s location, who has authority over it, and how this impacts operations.

Until recently, the idea that an organisation’s digital operations or services could be interrupted by a third-party ‘kill switch’ would have seemed impossible. However, conditions now exist for governments or global businesses’ core operations being interrupted or revoked without warning via foreign laws or regulations. Examining three factors in particular shows that service disruption or outages are no longer just hypothetical.

## **Geopolitical tensions**

As conflicts between countries and economic sanctions increase, nation-states are restricting the flow of goods, services and data, trade, collaboration and free information exchange. OECD/ WTO research estimates that disruptions to cross-border data exchange alone could reduce global GDP by 4.5%. Today’s uncertain geopolitical landscape has introduced a heightened risk of

service disruption for organisations that depend on services from non-domestic providers—stressing the importance of considering where data is located and managed and where services originate.

## **Regulatory pressure**

Law-making bodies have in recent years sought to regulate data flows to strengthen their citizens’ rights – for example, the EU bolstering individual citizens’ privacy through the General Data Protection Regulation (GDPR). This kind of legislation has redefined companies’ scope for storing and processing personal data. By raising the compliance bar, such measures are already reshaping C-level investment decisions around cloud strategy, AI adoption and third-party access to their corporate data.

## **Critical infrastructure**

Changes in individual governments’ policies are causing uncertainty for cross-border data governance, cloud access and international regulatory harmonisation. Across all regions, organisations are seeking greater control, visibility, and jurisdictional alignment in their data infrastructure – not just for compliance, but for achieving business objectives, operational resilience, and maintaining trust. Many enterprises are re-evaluating their supply chain and infrastructure locations, vendor jurisdiction, and legal risks, especially when operating in heavily regulated sectors such as healthcare.

**Patrick Smith**  
Field CTO EMEA  
Pure Storage.



**CHANGES IN INDIVIDUAL GOVERNMENTS' POLICIES ARE CAUSING UNCERTAINTY FOR CROSS-BORDER DATA GOVERNANCE, CLOUD ACCESS AND INTERNATIONAL REGULATORY HARMONISATION.**

### **Leaders rethink risk**

New research commissioned from the University of Technology Sydney (UTS) examined enterprise leaders' views of the changing landscape. It shows how data sovereignty has moved from a background compliance requirement to a board-level priority.

There was universal agreement (100% of respondents) that sovereignty concerns, such as service interruption, have forced their organisation to review where data is located. More than nine out of ten (92%) said geopolitical changes have increased the risk of enterprises failing to fully address data sovereignty questions. Company leaders fear their data sovereignty could be compromised: 92% fear reputational damage, and 85% fear they could ultimately lose customer trust.

Faced by anything from potential service outages to existential threats to their business, leaders have acted: 78% are embedding sovereignty in core processes, migrating from multiple service providers to investing in sovereign data centres, and

putting governance clauses in contracts.

### **Containing data sovereignty risks**

Faced with dynamic data sovereignty risks, enterprises have three main approaches ahead of them:

First, they can take an intentional risk assessment approach. They can define a data strategy addressing urgent priorities, determining what data should go where and how it should be managed – based on key metrics such as data sensitivity, the nature of personal data, downstream impacts, and the potential for identification. Such a forward-looking approach will, however, require a clear vision and detailed planning.

Alternatively, the enterprise could be more reactive and detach entirely from its non-domestic public cloud service providers. This is riskier, given the likely loss of access to innovation and, worse, the financial fallout that could undermine their pursuit of key business objectives.

Lastly, leaders may choose to do nothing and hope that none of these

risks directly affect them. This is the highest-risk option, leaving no protection from potentially devastating financial and reputational consequences of an ineffective data sovereignty strategy.

### **Ensuring data sovereignty**

Given today's converging geopolitical, regulatory and operational risk factors, company leaders have quickly grasped that data sovereignty no longer equates to data residency; it is a more complex principle, encompassing legal authority over data, how it is accessed or shared, and whose jurisdiction it falls under. True data sovereignty goes beyond physical location to include operational control, governance, and an organisation having full authority over its complete digital ecosystem.

Forward-looking companies can successfully navigate data sovereignty challenges by implementing data strategies that define what data should go where while managing all relevant infrastructure, partner, supply chain and regulatory risks. **🔑**

# RESILIENCE GAP BEHIND THE COMPLIANCE BADGE

**N**o one enters the cybersecurity sector expecting serenity. The pace is relentless, and the stakes are high.

According to the World Economic Forum, the weekly number of cyberattacks has more than doubled, now hovering just below 2,000. That figure might seem exaggerated until you consider how many high-profile breaches have made headlines recently - and those are just the ones we know about.

What's more concerning is the speed at which attackers are evolving. AI, once a theoretical threat, is now a practical weapon. Phishing techniques have become disturbingly sophisticated, and attackers are even weaponising chatbots to develop malicious code as they innovate at pace. Thankfully, governments have responded with commendable urgency. New regulations are emerging across the globe, and law enforcement has successfully dismantled several major threat groups. But these victories can be misleading. They create a sense of calm that's not only temporary but dangerous. Cyber threats don't vanish - they adapt.

## No getting off this ride

The one constant in cybersecurity is

change. Just last year, it seemed like the industry was on a big high, with major cyberthreat groups like LockBit, Black Cat, and Black Basta either being shut down, disappearing, or simply ceasing operations. Across Europe, we also saw two major cybersecurity regulations in the form of NIS2 and DORA, seeking to improve resilience for organisations in general, and for the particularly hard-hit financial sector. Some countries even took steps towards more decisive measures. In the UK, consultation was carried out on a potential ransomware payments ban for critical national infrastructure and public sector organisations. Taken alone, you could almost forgive organisations for thinking they could take their foot off the gas a little.

But there have been plenty of lows too. In recent months, we've seen a spree of successful attacks across Europe, most notably targeting the retail sector. While ransomware payments might have dropped again, it doesn't mean attackers are sitting back, relaxing. The takedown of established groups last year opened up room for smaller groups and even individual 'lone wolves'. With these new attackers comes a whole new set of motives. Money might still be a driver, but many of these newcomers are more focused on targets that can cause the

most disruption, rather than who might pay the biggest ransom. Today, you can split the market largely in two. Those high-cost, targeted attacks are still very much present, aiming at larger enterprises at deeper pockets. But on the other side, you've got volume-driven Ransomware-as-a-Service attacks, driven by those smaller groups and lone wolves, aiming to create as much chaos as possible.

So while on the surface, it might seem like an improved landscape, the same threats are still very much present, and new ones are already here.

## Making the right choices

Luckily, regulation hasn't just sat still in the face of this. As already mentioned, in the EU alone, we've had two major regulations, NIS2 and DORA, both targeting data resilience. NIS2 was particularly impactful, enshrining resilience squarely as a responsibility for the C-suite. No longer can organisations push resilience into the corner; now senior leadership must actively manage cybersecurity risks, making it as much of a business priority as profit and strategy. It also introduced new standards for organisational risk management and mitigation, and incident reporting in particular, an essential element with attacks on the

rise. While DORA was restricted to the financial services sector, it addressed some of the most pressing issues, like third-party risk, in an attempt to bolster one of the most targeted sectors.

Despite the measures required being essential for developing mature data resilience that can withstand the current pressures from threat actors, compliance is easier said than done. Ahead of NIS2, 66% of organisations expected to miss the deadline for compliance, and six months on from DORA, 96% of EMEA financial services organisations still felt they needed to improve their resilience in order to meet the requirements.

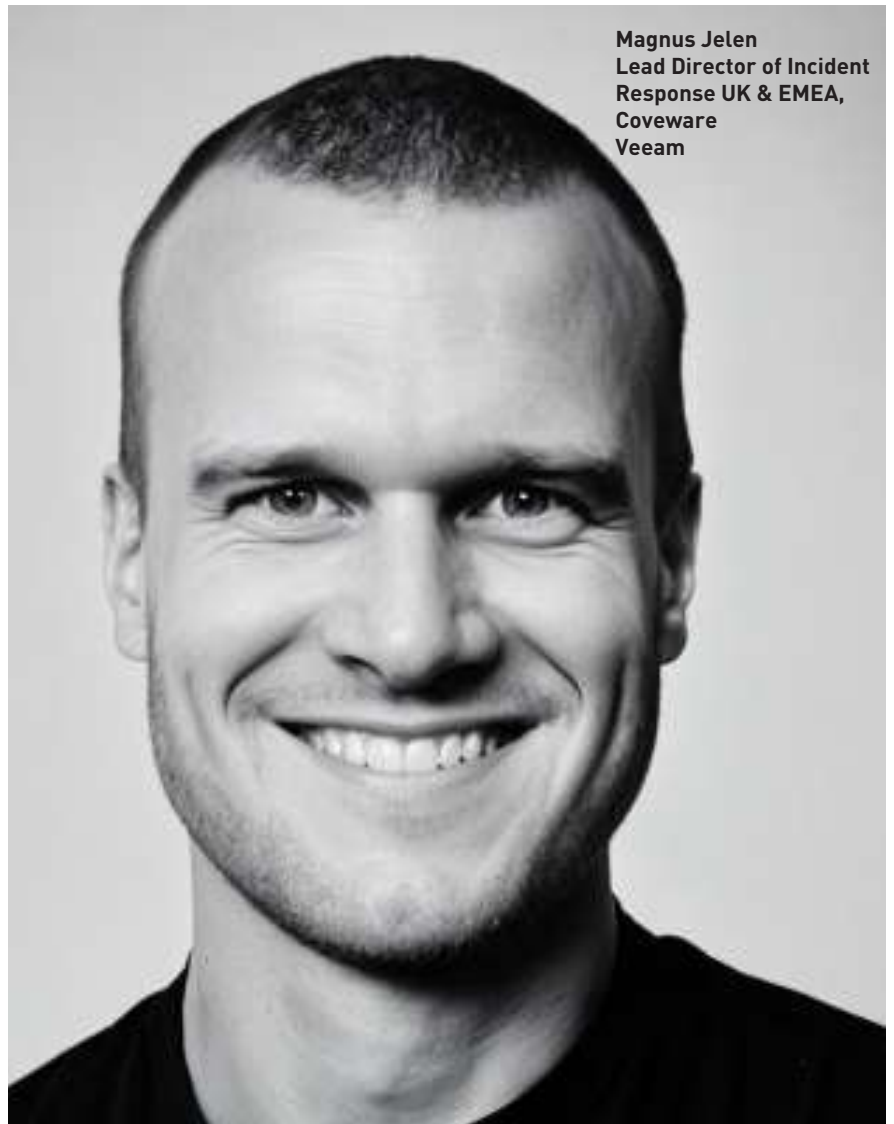
With so much work needed to reach compliance, when organisations do reach that threshold, the response is often to stop. But it's vital to remember that being compliant does not equal being secure.

### Keeping moving

Right now, the sector is sitting in the middle of a perfect storm. Big-name takedowns are lulling organisations into a false sense of security, while new attackers emerge from the wings using new and improved tools. And, the focus on regulatory compliance is at risk of misleading organisations and obscuring the true scope of improvements that could be made to their data resilience.

In times like this, organisations need to turn their attention inwards. Rather than scrambling to react to attacks with one hand, while also trying to meet compliance deadlines and keep day-to-day operations running smoothly with the other, they should try a different approach.

Using data resilience maturity models, organisations can not only better understand their current data resilience



**Magnus Jelen**  
Lead Director of Incident  
Response UK & EMEA,  
Coveware  
Veeam

level but also create a path to improve it. Instead of looking at every aspect of data resilience separately, these models bring them together, focusing efforts and creating a tide that lifts all boats, rather than the more typical patchwork approach to resilience.

With attacks more frequent than ever, and with attackers arguably as unpredictable as they've ever been,

special attention also needs to be paid to recovery. While having mature data resilience should always be 'plan A', your recovery 'plan B' needs to be just as developed, if not more so. Data resilience is a journey that can't be completed overnight, and attackers won't wait until you get yours up to scratch before they strike.

Ask yourself - right now, how long would it take my organisation to recover from an attack? Take a long, hard look at the answer, and if you wouldn't be able to wait that long without a severe business impact, perhaps you need to take a look at your recovery plan before the storm hits. 📌

**IN RECENT MONTHS, WE'VE SEEN A SPREE OF  
SUCCESSFUL ATTACKS ACROSS EUROPE, MOST  
NOTABLY TARGETING THE RETAIL SECTOR.**

# FRAUD EVOLVES AND SO MUST WE - TRUE PROTECTION STARTS WITH PEOPLE

**A**s scams become more sophisticated and increasingly personal, traditional fraud detection tools are struggling to keep up, the industry must rethink its entire approach to fraud management and why the next era of protection starts with understanding people, not transactions.

## A New Type of Fraud Crisis

Fraud today looks very different from what many institutions spent years preparing for. The threat has shifted from tampering with transactions to manipulating people and that shift is catching organisations off guard. In my conversations with banks, regulators, and industry leaders across the region, one message consistently stands out: fraudsters aren't attacking systems anymore; they're attacking human trust.

## Why Traditional Detection Falls Short

For decades, fraud engines were built to detect anomalies the unusual transfer, the unexpected location, the outlier that didn't fit established patterns. These systems performed exactly as designed. But they were never built to understand human behavior. They can't identify fear, pressure, or manipulation the very elements modern scams rely on.

Today's fraudulent transactions look completely legitimate. Victims use their own device, credentials, and banking channel. The payment aligns with their usual activity. But behind the scenes, they're being coached or guided by someone posing as a trusted figure. The transaction looks normal because the

manipulation happened long before it was made.

## Synthetic Identities: Fraud That Learns to Blend In

Alongside social-engineered scams, stolen and synthetic identities have become more sophisticated than ever. Created with patience and precision, these identities build credible histories and behave like real customers until the moment they strike. Static, rules-based detection simply cannot differentiate between a legitimate customer and a synthetic profile crafted to look identical.

## AI vs. AI: The New Intelligence Race

We've now entered a new era of fraud management: AI versus AI.

As institutions deploy advanced analytics to protect their customers, fraudsters are leveraging generative AI to scale their attacks. Voice cloning, deepfake videos, and AI-generated messaging allow scams to be hyper-personalised and nearly impossible for the untrained eye to detect. At the same time, institutions are training AI to recognise subtle behavioral deviations and hidden identity links.

This is no longer a game of reacting. It's a race of adaptation and speed matters.

## Why Human-Centric Detection Is the Way Forward

Despite the complexity, I remain optimistic. We finally have the tools to defend against fraud at the level where it actually happens the human level.

Behavioral intelligence allows us to detect the subtle signs that someone is under duress. Adaptive machine learning identifies new scam patterns in real time. Network analytics exposes synthetic identity ecosystems. And AI-powered platforms continuously adjust to evolving threats.

This is the shift the industry needs: from transaction-centric to behavior-centric detection.

As I often highlight to leadership teams:

"The future of fraud prevention is understanding people as deeply as we understand data. When we combine behavioral insight with adaptive intelligence, we shift from reacting to threats to staying ahead of them."

## A Call for Industry Action

The industry is at a turning point. Legacy tools, no matter how optimised, cannot keep pace with modern threats. Financial institutions must modernise fraud operations, invest in adaptive AI, and place behavioral intelligence at the core of customer protection.

This isn't about technology for technology's sake. It's about safeguarding people who are being targeted in ways they've never experienced before.

Modern scams are evolving rapidly. Our defenses must evolve even faster.

The responsibility lies with all of us leaders, innovators, regulators, and partners across the financial ecosystem.

It's time to rethink, rebuild, and deploy solutions designed for the sophistication of the world we operate in today. **i**

**Abed Hamandi**  
Senior Director, EMEA Consulting, Fraud  
and Security Intelligence Practice  
SAS



# DARK WEB REVEALED: NEW STUDY SHOWS PROBLEMS MOUNTING FOR CYBERCRIMINALS

**I** DARK WEB FACILITATES LARGE-SCALE CRIMINALITY BY MAKING IT EASY FOR ANYONE WITH SUFFICIENT IT SKILLS TO OBTAIN THE KNOWLEDGE AND TOOLS TO DEFRAUD INDIVIDUALS AND BUSINESSES

**R**esearch from LexisNexis Risk Solutions takes a deeper look into how cybercriminals operate using the dark web in its latest report, *Fraud for Sale: Untangling the Dark Web*, part of the annual *Global State of Fraud* report. The insights stem from a proprietary study of the dark web commissioned in 2025.

## Key findings

The study concludes that the dark web facilitates large-scale criminality by making it easy for anyone with sufficient IT skills to obtain the knowledge and tools to defraud individuals and businesses. Regulators and law enforcement repeatedly close down illicit marketplaces on the dark web only for replacements to spring up to meet the unwavering demands of the criminal underworld.

“The hidden nature of the dark web has appealed to the criminal underworld for more than a decade, arming and sheltering fraudsters from detection,” said Kimberly Sutherland, global head of fraud and identity, LexisNexis Risk Solutions. “Now we can shed new light, not only on what cybercriminals do on the dark web, but on the fraud controls they are least able to bypass. Fraudster

feedback tells us exactly what interferes most with their criminal exploits to hamper their success: real-time liveness checks, account activity, phone and email analysis and device fingerprinting, to name a few.”

## The AI frustrating fraudsters

The use of AI and deepfakes in fraud is well documented. Yet, the report uncovers dark web chat forums awash with users venting their frustration with the latest AI-driven deepfake detection systems employed by banks and others that can scan for blood flow and micro

- Fraud-as-a-Service ‘superstores’ expanding to meet huge criminal demand for tools to beat modern anti-fraud systems
- Know your customer (KYC)-ready bank accounts, ‘fraud for beginners’ tutorials and plug-and-play fraud kits amongst range of available services
- Criminal-on-criminal attacks driving changes to dark web marketplaces as fraudsters grapple with AI challenge
- Social media platforms emerging as a threat to the dark web as criminals value convenience

muscle movements. Such technology appears to present a specific hurdle for would-be fraudsters, with one commenting “There is no bypass.” The research also found related forums involving some imaginative attempts to circumvent checks, such as with latex masks.

Several marketplaces were found selling established email accounts and devices capable of passing basic fraud checks. Many also offer ‘fraud-ready’ bank accounts supplied with login details and pre-completed identity checks.

Sutherland continued, “Our research reveals the dark web to be a de-facto fraud superstore giving bad actors easy access to the knowledge and tools to conduct all manner of criminal acts. With these tools they can apply for bank accounts, overdrafts and credit, set up retail accounts and make purchases without fear of consequences.

“It’s also worrying that many of the solicitations come complete with tutorial videos, showing ‘newbie’ scammers how it’s done, thereby creating a new cottage industry of amateur fraudsters across the globe. The good news is that we are not powerless against cybercriminals. As quickly as they adopt new technology it is increasingly apparent how those same AI innovations can thwart their activities.”



**Kimberly Sutherland**  
Global Head of fraud and identity  
LexisNexis Risk Solutions.

**No safe harbor for cybercriminals**

In an ironic twist, the study also finds the dark web is no safe haven for criminals. Exit scams are rife, where dark web marketplace administrators abruptly cease trading, taking their customers' funds with them. This has led some marketplaces to take measures to demonstrate legitimacy by calling out bad behavior, barring users and banning the sale of certain items known to be worthless to buyers. As a consequence, the report found some evidence of alternative, easier access versions of these dark web marketplaces selling similar products cropping up on mainstream popular social platforms. 🔒

→ **THE HIDDEN NATURE OF THE DARK WEB HAS APPEALED TO THE CRIMINAL UNDERWORLD FOR MORE THAN A DECADE, ARMING AND SHELTERING FRAUDSTERS FROM DETECTION.**

# 70% OF UAE FIRMS PLAN AI-DRIVEN SOCS— BUT TALENT AND DATA GAPS STALL PROGRESS

**I** ORGANISATIONS CLEARLY RECOGNISE THE VALUE AI CAN BRING TO SOCS BUT THE TRANSITION FROM EXPERIMENTATION TO REAL SOC IMPACT STILL REMAINS CHALLENGING.

**A**lmost all companies planning to establish a Security Operations Center (SOC) regard artificial intelligence (AI) as a must-have component. However, despite high expectations, organisations face significant challenges in deploying and operationalising AI effectively. These include a lack of high-quality training data, a shortage of AI-skilled personnel, substantial integration costs and emerging AI-related threats.

To explore how companies build and maintain processes in SOCs, Kaspersky conducted a comprehensive global study which highlights, among other things, priorities, expectations and challenges associated with leveraging AI to elevate SOC performance. The findings reveal that an overwhelming 99% of respondents plan to incorporate AI into their security operations. Among them, nearly three quarters (70%) in the UAE say they will probably do so and nearly a third (30%) state they will definitely do so. This underscores the widespread perception of AI as a vital driver for enhancing threat detection, accelerating investigation processes and boosting overall SOC efficiency.

When it comes to practical use cases,

organisations in the UAE primarily expect AI to strengthen threat detection capabilities through automated analysis of data to identify anomalies and suspicious activities (58%) and to facilitate response automation, enabling rapid execution of predefined incident response scenarios (46%). These expectations align closely with the top motivations driving AI adoption in SOCs: improving overall threat detection effectiveness (46%), automating routine tasks (39%) and increasing accuracy while reducing false positives (52%). Large enterprises consistently report broader and more ambitious plans for applying AI across multiple SOC functions.

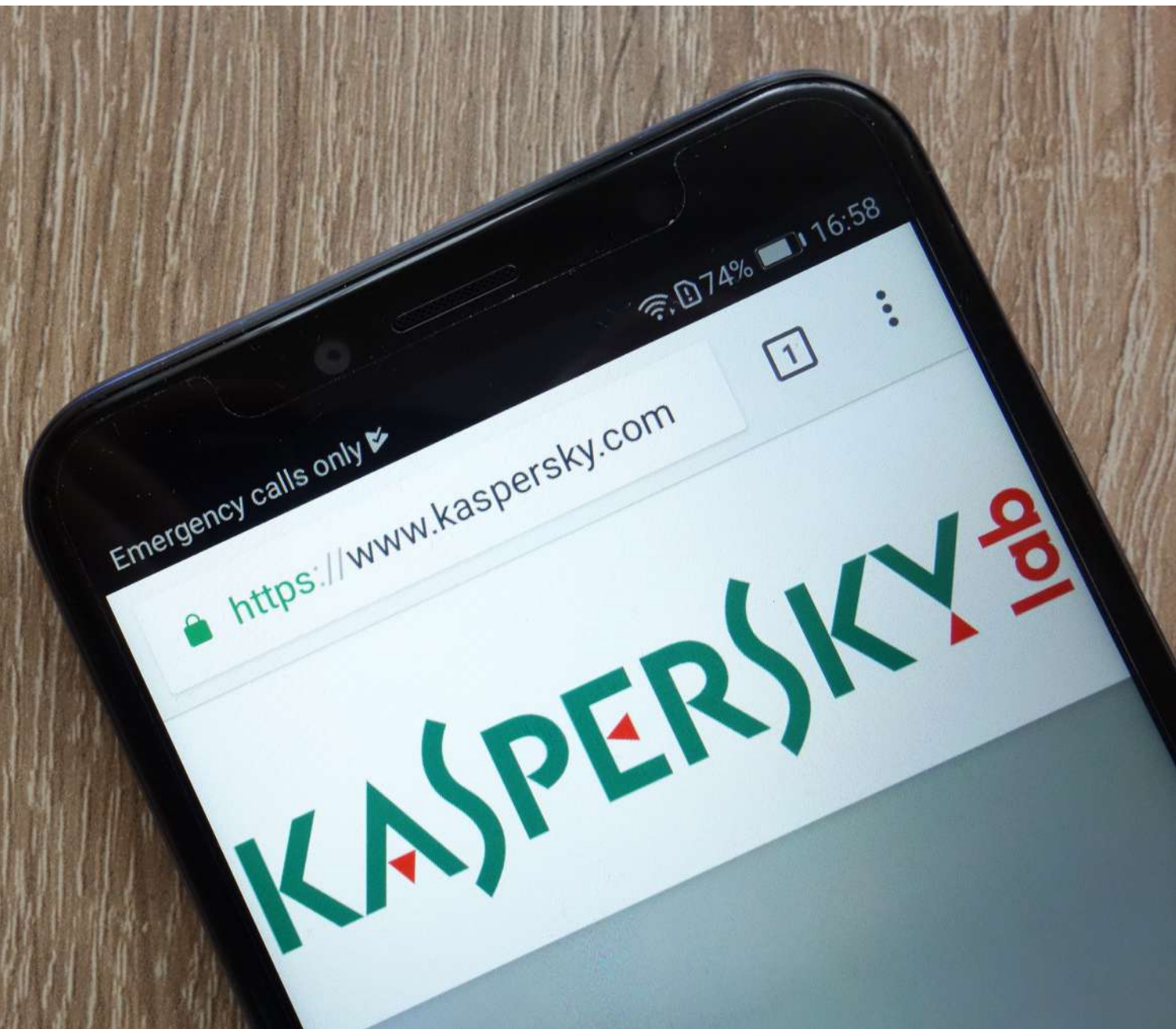
However, a clear execution gap appears when it comes to AI implementation, characterised by several critical and widespread challenges. Foremost is the lack of high-quality training data, a barrier cited by 32% of organisations in the UAE as a fundamental obstacle that hampers the accuracy and relevance of AI models. This issue is further compounded by other critical concerns: a shortage of qualified AI experts within internal team (43%), the emergence of new threats and vulnerabilities related to AI usage

(27%) and the high costs associated with developing and maintaining AI-driven solutions (32%). Together, these factors create a barrier that prevents organisations from turning their AI strategy into operational success, underscoring the necessity for a structured and well-supported approach.

“Organisations clearly recognise the value AI can bring to SOCs but the transition from experimentation to real SOC impact still remains challenging. Given the cybersecurity talent shortages—and AI talent being scarce as well—introducing in-house AI capabilities in a SOC remains a coveted but hard-to-achieve goal. This is why cybersecurity companies are investing in AI-powered features across their leading products. Over the past year, Kaspersky has introduced a comprehensive suite of AI-powered tools across its B2B portfolio to meet the rising demand for timely detection of more advanced threats, while also making our solutions more efficient and user-friendly,” says Anton Ivanov, Chief Technology Officer at Kaspersky.

To build and operate a successful and reliable SOC, Kaspersky recommends the following:

- Engage with Kaspersky SOC



Consulting during the initial setup or when enhancing your existing security operations. Our comprehensive consulting services are designed to help companies build a robust SOC and streamline its processes.

- Boost your security performance with Kaspersky SIEM, powered by advanced AI capabilities. This solution aggregates, analyses and stores log data across your entire IT infrastructure, providing contextual

enrichment and actionable threat intelligence insights. Recently, this solution was empowered by AI capability to identify signs of dynamic link library (DLL) hijacking.

- Protect your company against a wide range of threats with solutions from the Kaspersky Next product line that provide real-time protection, threat visibility and AI-driven investigation and response capabilities of EDR and XDR for organisations of any size and industry.

- Equip your cybersecurity team with in-depth visibility into cyber threats targeting your organisation. The latest Kaspersky Threat Intelligence delivers rich, contextual insights throughout the entire incident management cycle, enabling timely identification of cyber risks. Recently, it was strengthened by AI-enhanced open-source intelligence search, enhancing your team's ability to uncover and respond to emerging threats with greater precision. 🔗

# AI ASSISTANTS ARE REWRITING HOW BRANDS SHOW UP - AND BLOCKING BOTS MAY BE MAKING IT WORSE

AS COMPANIES RUSH TO BLOCK AI BOTS, DATA SUGGESTS THEY MAY BE PUSHING PRICING, BRAND MESSAGING, AND CUSTOMER DECISIONS INTO AI SYSTEMS BEYOND THEIR CONTROL.

Companies trying to protect their content from artificial intelligence may be weakening their control over how customers see their brands. A new analysis by Hostinger, a no-code AI Agent-driven platform for building and growing online businesses, reveals a rapid expansion of AI assistant crawlers – the systems used by tools like ChatGPT and Siri to summarise, compare, and recommend products. This expansion is occurring even as businesses are aggressively blocking bots designed for AI training. The analysis is based on 66.7 billion verified bot interactions across 5 million websites.

The result: AI assistants are reading and summarising more business websites, even as companies reduce their ability to influence how those systems understand and present them.

For decades, the commercial internet ran on a predictable model. Search engines indexed websites and sent users back. Brands controlled pricing context, messaging, and attribution inside owned channels. That model is breaking. AI assistants increasingly answer questions directly, replacing visits with summaries and recommendations. Discovery no longer guarantees traffic – and often

ends before a website is reached.

Hostinger's data shows this shift accelerating. Over a five-month period, OpenAI's SearchBot expanded from 52% to 68% of websites, while Applebot doubled from 17% to 34%. Traditional search crawlers remained broadly stable, indicating that AI is not replacing search but adding a new decision layer above it.

## Blocking AI – just not the right kind

At the same time, companies are sharply restricting access by AI model-training crawlers. OpenAI's GPTBot fell from 84% website coverage in August to just 12% by November. Meta's ExternalAgent dropped from 60% to 41%.

Hostinger's analysis shows that training crawlers and assistant crawlers serve different roles, but are often treated as the same.

Training crawlers collect data to improve AI models over time. Assistant crawlers fetch content in real time to answer user queries. Blocking the former does not stop the latter from summarising, ranking, or recommending a company's products and services.

The net effect is that AI assistants are mediating more customer decisions, while companies have fewer signals shaping how those systems learn from their content.

As AI assistants increasingly mediate discovery and comparison, companies are losing control over more than traffic:

- Pricing context, as AI responses summarise offers without full commercial nuance
- Brand safety, as messaging is reframed outside approved guidelines
- Advertising effectiveness, as paid acquisition loses visibility upstream
- Ecommerce attribution, as customer journeys end inside AI interfaces

These risks affect marketing teams first, but extend quickly into revenue forecasting, compliance, and operations.

## From blocking to governance

Some companies are beginning to adjust, moving from blanket blocking toward selective AI governance – explicitly managing how AI assistants access and interpret content, while still restricting bots that pose cost or IP risks.

That includes tools such as llms.txt, a machine-readable file that guides AI assistants to authoritative pages and priorities, and AI-ready site interfaces that expose current, structured content rather than inferred summaries.

"With AI assistants increasingly answering questions directly, the web is shifting from a click-driven model to



Tomas Rasmus  
Head of AI  
Hostinger.

an agent-mediated one,” said Tomas Rasmus, Head of AI at Hostinger. “The real risk for businesses isn’t AI access itself, but losing control over how pricing, positioning, and value are presented when decisions are made.”

**Methodology**

Hostinger analysed 66.7 billion anonymised log entries from 5 million websites, collected during three six-day windows in June, August, and November 2025. Only verified crawler

traffic was included, classified using publicly documented user agents, observed behavior patterns, and open-source AI crawler registries. Human traffic and unrelated noise were excluded. [i](#)

# OVER 40% OF UAE ORGANISATIONS RANK AS AI LEADERS, MATCHING GLOBAL FRONT-RUNNERS

**42% OF ORGANISATIONS NOW QUALIFY AS AI LEADERS, REFLECTING STRATEGIC INVESTMENTS IN AI INFRASTRUCTURE AND COMMITMENT TO THE AI 2031 STRATEGY.**

**T**he UAE has positioned itself as a leading AI market, with 42% of organisations now qualifying as AI Leaders according to a comprehensive new study by Boston Consulting Group. The report, "Unlocking Potential: How GCC Organisations Can Convert AI Momentum into Value at Scale," reveals that UAE organisations are not only matching global peers but demonstrating exceptional progress in enterprise-wide AI deployment.

The study, which surveyed 200 C-suite executives and assessed 41 digital and AI capabilities across seven industries, shows that 37% of UAE organisations have reached the critical 'Scaling' AI maturity stage, signaling a decisive shift from experimental pilots to comprehensive enterprise-wide implementation. With an average AI maturity score of 46, the UAE is positioned at the forefront of its regional peers with only 13% of its organisations scoring at the stagnating level.

"The UAE's emergence as a significantly advanced AI market, with 42% of organisations now qualifying as AI Leaders, is a direct reflection of the nation's strategic investments in AI infrastructure and unwavering commitment to its AI 2031 Strategy," said Dr. Lars Littig, Managing Director & Partner and ME Leader of the Tech & Digital Advantage practice at Boston Consulting Group. "When we see GCC organisations, including in the UAE,



**Dr. Lars Littig**  
**Managing Director & Partner and**  
**ME Leader of the Tech & Digital**  
**Advantage practice**  
**Boston Consulting Group.**

delivering significantly higher returns through AI adoption, it validates that these countries' substantial public and private sector investments are translating into measurable enterprise value. The alignment between national AI ambitions and business outcomes positions the UAE as a regional pioneer, and more significantly as a global benchmark for how strategic AI investments can drive economic transformation."

Across the broader GCC region, the report demonstrates remarkable progress in closing the AI adoption gap

with global markets. According to the report, 39% of all GCC organisations now qualify as AI Leaders, compared to the global average of 40%, representing a fundamental transformation in how regional businesses approach artificial intelligence. The GCC region demonstrates exceptional AI leadership, with its Public Sector achieving the highest AI maturity levels globally across all surveyed markets. While TMT continues to lead in AI maturity within the GCC, there is rapid advancement occurring in other critical sectors

including Financial Institutions, Health Care, Industrial Goods, and Travel, Cities, and Infrastructure, highlighting the region's broad-based AI transformation.

The financial impact of AI leadership proves substantial, with AI Leaders across the GCC delivering up to 1.7 times higher total shareholder returns and 1.5 times higher EBIT margins compared to AI Laggards. This performance differential underscores the critical importance of moving beyond pilot programs toward scaled implementation. This success is directly linked to higher AI investment levels - AI Leaders are dedicating 6.2% of their IT budgets to AI in 2025 compared to only 4.2% by Laggards. As AI budgets continue to grow, the value generated by AI Leaders is expected to be 3-5x higher by 2028, not only amplifying their competitive advantage but also significantly widening the performance gap between Leaders and Laggards.

### **GCC AI Leaders: Pursuing AI-First Models and Unlocking Agentic AI Value**

While the GCC has demonstrated advanced digital maturity in recent years, AI maturity has surged by 8 points between 2024 and 2025, now trailing overall digital maturity by just 2 points. The study reveals that successful AI Leaders distinguish themselves through five critical strategic moves: pursuing multi-year strategic ambitions with 2.5 times more leadership engagement than laggards, fundamentally reshaping business processes rather than simply deploying off-the-shelf solutions, implementing AI-first operating models with robust governance frameworks, securing and upskilling talent at 1.8 times the rate of competitors, and building fit-for-purpose technology architectures that reduce adoption challenges by 15%.

Looking toward frontier technologies, 38% of GCC organisations are already experimenting with agentic AI, positioning the region competitively against the global average of 46%. The value generated from agentic AI initiatives, currently at 17%, is projected

**Wietse Bloemzaad**  
**Managing Director & Partner**  
**BCG X**



to double to 29% by 2028, driven by continued experimentation and strategic deployment.

Despite this strong momentum, GCC organisations continue to face barriers to AI adoption, with AI Laggards 18% more likely than AI Leaders to encounter people, organisation, process challenges stemming from limited cross-functional collaboration on AI, unclear AI value measurement, misalignment with enterprise strategy, or lack of leadership commitment. AI Laggards are also 17% more likely to face challenges in algorithm implementation, especially around limited access to high-quality data, and 10% more likely to encounter technology constraints, such as security risks and RAI implementation, in addition to a general constraint in the availability of local GPUs, further increasing burden on organisations.

"While the GCC has demonstrated advanced digital maturity over recent years, we're witnessing remarkable acceleration in AI maturity, marking a fundamental commitment to AI as a core value creator," added Wietse

Bloemzaad, Managing Director & Partner at BCG X, the tech build and design unit of BCG. "However, the journey ahead requires addressing key organisational challenges: AI Laggards are more likely to face cross-functional collaboration barriers and more likely to struggle with data quality issues. The promising news is that many GCC organisations are already experimenting with agentic AI, with value generation projected to double by 2028. Success will depend on sustained executive engagement, comprehensive talent development, and the courage to move beyond pilots toward enterprise-wide transformation."

The report emphasises that sustained AI leadership requires continued focus on executive engagement, comprehensive talent development, responsible AI governance, and strategic alignment between AI initiatives and broader business objectives. As UAE organisations continue their AI transformation journey, their success in moving from pilot programs to scaled implementation positions them as regional pioneers in the global artificial intelligence evolution. 🌱

# TRUST AND DATA KEY TO SCALING AI PILOTS, SAYS ALTERYX RESEARCH

**SURVEY OF 1,400 LEADERS REVEALS HOW ORGANISATIONS ARE UNLOCKING AI PILOT SUCCESS AMID GROWING INVESTMENTS**

**A**lteryx, Inc., a leading AI-ready data and analytics company, released new research revealing that while enterprises are ramping up investment in AI and automation, trust and data challenges continue to slow adoption.

The research finds a growing disconnect between AI ambition and real-world impact. Despite heavy investment in AI, most organisations are failing to move AI beyond pilot programs, held back by low trust in AI outputs, poor data quality, and legacy technology that can't support scale. Fewer than one in four AI pilots successfully operationalise into production.

## Key Findings:

- Trust remains a major barrier to adoption: While nearly half of respondents say they trust AI to automate repetitive tasks, draft content, and monitor systems, fewer trust it for strategic decisions. Only 28% trust AI to support decision-making, and just 27% trust it to facilitate forecasting or planning, highlighting a significant gap in confidence for high-impact applications.
- Data quality is critical for agentic AI impact: Nearly half (49%) of leaders cite high-quality, accessible, and well-governed data as the top factor for agentic AI to achieve its full potential.
- AI workflow ownership is shifting across the business: Business and IT leaders expect responsibility for AI workflows to move away from centralised teams to individual lines

**Andy MacMillan**  
CEO  
Alteryx.



of business by 11% over the next three years.

- Growing AI adoption: 48% of leaders plan to boost AI spending on AI infrastructure and tools, with 89% maintaining or increasing budgets in 2026. AI platforms now make up a larger portion of data stacks, projected to grow from 33% in 2024 to 51% in three years.

Together, the findings point to a deeper issue behind stalled AI initiatives: trust breaks down when AI is deployed without the business context and logic required to produce consistent and explainable results. Many organisations are layering generative AI directly on top of raw data sources, leading to hallucinations, inconsistent outputs, and responses that change from one query to the next, undermining confidence in AI for real business decisions. As a result, organisations should double

down on the foundations needed to make AI trustworthy at scale. This includes governed data, defined metrics and workflows that combine the creativity of generative AI with deterministic rules – and the ability for the business to quickly adapt them as needs change. In fact, 28% of leaders plan to prioritise data governance improvements.

“AI adoption is accelerating fast,” said Andy MacMillan, CEO of Alteryx. “Our research shows that compared to a year ago, two-thirds of business and IT leaders are using AI more in their roles. We’re also seeing AI move closer to individual departments. Over the next three years, leaders expect responsibility for AI workflows to shift to specific lines of business, rising from 22% today to 33% by 2028. The most advanced organisations are doubling down on improving data quality and integrating AI across their operations.” 🔑

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



# MIDDLE EAST AND AFRICA'S



SCAN HERE



GET FREE  
 VISITOR PASS

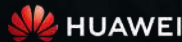
#gisecglobal  
 gisec@dwtc.com

## SPONSORS & PARTNERS

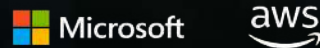
OFFICIAL DISTRIBUTION PARTNER



LEAD STRATEGIC PARTNER



STRATEGIC PARTNER



DIAMOND SPONSOR



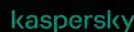
PLATINUM SPONSOR



GOLD SPONSOR



SILVER SPONSOR



BRONZE SPONSOR





# Empowering Cybersecurity Across the Middle East & Africa

Cybersecurity is more than technology, it's trust, collaboration, and local expertise.

We empower our partners through presales consulting, enablement, training, and technical support, ensuring seamless deployment and measurable business outcomes.

Through our presence in UAE, Saudi Arabia, Kenya, and beyond, EVAD continues to simplify cybersecurity adoption and drive digital resilience across the region.

## → Regional Reach, Global Partnerships

Connecting leading global vendors with the MEA region cybersecurity ecosystem.

## → End-to-End Enablement

From consulting to deployment, empowering partners every step of the way.

## → Trusted Expertise

Delivering localized support, training, and innovation through a team of regional specialists.

## Partnering with the Best to Deliver Advanced Cybersecurity Solutions

DATAPATROL

CLOUDMON

FourCore

fileorbis

efficient iP

LEVO

Discover more at [evad-me.com](http://evad-me.com)