

Security ty

ADVISOR

MIDDLE EAST



2026: CYBER CONFIDENCE MEETS REALITY



ASUS ExpertBook B5 B5405

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



AI-empowered
productivity



Light weight and portable



Long Battery Life



Accelerate business success

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



18 SANS Gulf Region 2025 highlights skills reshaping cybersecurity in AI-driven GCC

40 Phishing evolves into scalable cybercrime business, says Ro'ya Hatamleh

36 Veeam positions trusted data as foundation for scaling safe AI, says CEO Anand Eswaran

50 Building cyber resilience through collaboration: Why it matters more than ever in Middle East



Fortify Your Cybersecurity

Fortinet
Global Cybersecurity Leader

The Fortinet Security Fabric is the industry's highest-performing cybersecurity platform, delivering broad, integrated, and automated cybersecurity capabilities supported by a large, open ecosystem. The Fortinet Security Fabric empowers organizations to achieve secured digital acceleration outcomes by reducing complexity, streamlining operations, and increasing threat detection and response capabilities.

Learn more at fortinet.com

EDITOR'S NOTE



Talk to us:

E-mail:
sandhya.dmello@cpimediagroup.com

Sandhya DMello
Editor

GOODBYE 2025, WELCOME 2026: FROM CYBER CONFIDENCE TO CYBER PROOF

The close of 2025 delivers a clear message to the cybersecurity community across the Middle East: confidence is no longer the benchmark—proof is. The region’s rapid embrace of cloud, AI, smart infrastructure, and digital-first governance has accelerated opportunity, but it has also exposed a new reality. Cyber maturity today is measured by demonstrable resilience, verifiable recovery, and the ability to operate securely across increasingly complex ecosystems.

This December issue of Security Advisor Middle East reflects that shift. Across sectors and geographies, security leaders are being challenged to move beyond point controls and static assurances toward evidence-led security postures. Boards, regulators, and insurers are asking tougher questions. Adversaries are exploiting the spaces between platforms, identities, data, and suppliers. The result is a decisive transition: cybersecurity must now stand up to scrutiny under real-world pressure.

Our cover story, Goodbye 2025, Hello 2026! Cyber maturity moves from confidence to proof, explores this inflection point in depth. From non-human identities and AI-driven attacks to data resilience, OT security, and post-quantum readiness, the region is redefining what trust means in an era where assumptions fail fast. The weakest link is rarely a single system—it is

the gap between environments, partners, and governance models.

Readers should not miss our extensive Black Hat MEA 2025 coverage, which captures the region’s cybersecurity momentum in real time. From AI observability and OT resilience to data-centric security, fraud intelligence, and post-quantum preparedness, our on-the-ground interviews reveal how Saudi Arabia and the wider GCC are shaping security strategies at national and enterprise scale.

This issue also features exclusive interviews with Microsoft, Veeam, and SANS

Institute, offering critical insights into the forces reshaping cyber defence in 2026. Microsoft examines the

industrialisation of phishing and the rise of AI-driven cybercrime.

Taken together, the stories in this issue point to a shared conclusion: identity is becoming the new control plane, data the foundation of AI trust, and collaboration the engine of resilience. Compliance is evolving into a strategic enabler, and recovery—clean, fast, and within jurisdiction—is emerging as the ultimate test of cyber maturity.

The year ahead will be decisive. 2026 will reward organisations that can prove resilience, not just promise it. We look forward to continuing this journey with you—clear-eyed, evidence-driven, and resilient by design.

PROVING RESILIENCE IN 2026

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
prajiith.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 2025 CPI
All rights reserved

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

GITGUARDIAN ENTERS SAUDI ARABIA TO STRENGTHEN CYBERSECURITY FOR VISION 2030



GitGuardian

GitGuardian, global leader in non-human identity cybersecurity, has officially entered the Saudi Arabian market by completing a 12-day strategic immersion under Business France's Booster Grow Global program. This marks GitGuardian's first structured entry into the Kingdom, during which the French Tech-certified company engaged with government agencies, giga-project leaders, and major enterprises across Riyadh, Jeddah and Dammam. The immersion paved the way for potential partnerships and demonstrated GitGuardian's commitment to supporting Saudi Arabia's cybersecurity transformation in line with Vision 2030.

Founded in 2017, GitGuardian is recognised as a breakthrough innovator, aligned with the France 2030 initiative, and is trusted by over 600,000 developers and companies worldwide to secure the identities of machines and the secrets they hold (API keys, credentials, etc.) in today's cloud-driven and AI-powered environments.

Saudi Arabia is rapidly emerging as a global technology hub. Ambitious initiatives like NEOM, Qiddiya, and the upcoming Expo 2030 in Riyadh are driving a wave of digital acceleration across the Kingdom. Correspondingly, the Saudi cybersecurity market is experiencing explosive growth. It reached approximately \$6 billion in 2024 and could exceed \$17 billion by 2030. In fact, Saudi Arabia now ranks #1 worldwide on IMD's 2024 Cybersecurity Index, reflecting its

maturity as a cyber-secure nation. At the same time, threat activity is intense: the Kingdom endures tens of millions of cyberattack attempts annually (over 160,000 attacks per day in one recent study), making it the most targeted country in the Middle East.

This momentum is reinforced by strong government action. The National Cybersecurity Authority (NCA) continues to introduce comprehensive frameworks, including the CyberIC Program to build national cybersecurity capabilities, helping raise operational standards across public and critical sectors. Combined with business-friendly policies, these initiatives create an enabling environment for advanced cybersecurity solutions.

GitGuardian's selection as a laureate of Booster Grow Global KSA 2025 aligns perfectly with these national priorities. The company's all-in-one NHI security platform directly addresses emerging risks in Saudi Arabia's digital landscape. By offering a solution to secure automated accounts and detect leaked secrets, GitGuardian arrives with a clear mandate: to help fortify Saudi Arabia's digital transformation initiatives (smart cities, e-government services, industrial digitization) against the latest cyber threats.

"As Saudi Arabia accelerates its digital transformation and invests in smart infrastructure, we are excited to partner with local innovators and enterprises to help secure this next era of growth," said

Eric Fourrier, CEO of GitGuardian.

Roadmap in Saudi Arabia

GitGuardian has entered Saudi Arabia through a phase expansion strategy. In the first stage, the company is focusing on priority sectors such as energy, telecom, finance, government, and healthcare, where the risks are the most urgent. Through pilot projects, targeted demos, and support aligned with local time zones and compliance requirements, GitGuardian aims to deliver immediate value. The Booster Grow Global program, designed to accelerate French companies' entry into Saudi Arabia, provided fast-track access to key stakeholders during the mission.

The next phase will focus on building a local ecosystem. GitGuardian plans to onboard distributors and systems integrators, co-develop solutions with Saudi IT providers, and roll out training and certification programs to accelerate local adoption.

Cutting-Edge Technology for Secure Innovation

GitGuardian is bringing to Saudi Arabia a unique technology that sets it apart in the cybersecurity arena. It is currently the only platform offering truly end-to-end security for Non-Human Identities essentially, the accounts and credentials used by applications, automation tools, cloud services, and other machine agents. The platform's capabilities span from advanced secrets detection (finding

hard-coded passwords, API keys, tokens, and other sensitive data hidden in code repositories, configuration files, or logs) to full lifecycle governance of machine identities (tracking which services have access to what, rotating or revoking credentials, and enforcing policies across CI/CD pipelines and cloud infrastructure).

Built for modern DevOps and cloud-native environments, GitGuardian integrates seamlessly into developers'

workflows. This developer-first approach means security is embedded without slowing down innovation: developers receive instant alerts and guided remediation steps when a secret is exposed, enabling fixes within minutes. Powered by artificial intelligence, GitGuardian delivers highly accurate detection, and the benefits are tangible: companies resolve secret-related incidents up to 60 times faster.

By securing the surge of machine identities and secrets that accompany digital transformation, GitGuardian's platform empowers Saudi businesses and government entities to innovate safely and sustainably. Now, GitGuardian is poised to help shape the future of cybersecurity in the Kingdom, working hand-in-hand with local partners and stakeholders to address Saudi Arabia's priorities in protecting data and digital assets.

NOZOMI NETWORKS RECOGNISED AS COMPANY TO BEAT FOR AI IN CYBER-PHYSICAL SYSTEMS SECURITY

Nozomi Networks, offering solutions in OT, IoT and CPS security, announced it has been recognised as the company to beat for AI in Cyber-Physical Systems Security in the Gartner report for AI Vendor Races.

According to Gartner, "Native and embedded CPS capabilities and whole life cycle coverage out Nozomi at the head of the pack." The report notes, "Nozomi's early approach of embedding machine learning (ML) capabilities natively during the earliest stages of product development in 2013 has given its Nozomi CPS security product an operational head start in enabling AI to support CPS discovery, analysis and alerting capabilities."

"We are proud to be recognised by Gartner Research as the Company to beat for AI in cyber-physical systems protection," said Nozomi Networks CEO Edgard Capdevielle. "We believe this recognition is a testament to our team's dedication to safeguarding the world's most essential systems and our ongoing commitment to innovation in AI-driven cybersecurity."

Refined in-house for more than a decade, Nozomi Networks' AI-powered platform empowers organizations to proactively detect, respond to and mitigate cyber threats targeting



Edgard Capdevielle

industrial and critical infrastructure. Nozomi's AI engine uses a variety of techniques to enrich asset profiles, baseline normal behavior, raise issues and provide actionable to

deliver robust visibility and security for complex cyber-physical systems across energy, manufacturing, transportation healthcare and other sectors.

TECHBRIDGE MEA OPENS NEW OFFICE IN OMAN, EXPANDS REGIONAL PRESENCE, GROWTH STRATEGY

Strategic expansion reinforces commitment to GCC market as Oman emerges as the fastest-growing economy in the region.

TechBridge MEA, a leading Channel Value-Added Distributor (CVAD) specialising in mobility, cybersecurity, and networking solutions, announced the opening of its newest office in Oman, marking a significant milestone in the company's regional growth strategy and strengthening its presence across the GCC.

The Oman office underscores TechBridge MEA's commitment to delivering localised support and full compliance across the Gulf Cooperation Council, positioning the CVAD to capture opportunity in one of the region's most dynamic and expanding technology markets.

Exponential growth

Since its establishment in November 2023, TechBridge MEA has experienced robust expansion, onboarding over 20+ vendors and many more strategic channel partners, delivering consistent year-on-year revenue growth, driven by strong demand for its Channel focused value-added distribution model. The company has achieved 50% quarter-on-quarter growth throughout the year, reflecting the market traction of its offerings across mobility, cybersecurity, and networking solutions. Responding to significant regional demand, TechBridge MEA is opening a physical presence in Muscat where over 40 partners have actively sought localised support – highlighting Oman's importance as an emerging technology hub. TechBridge's move positions it ahead of many competitors who have yet to establish a formal presence in the market. TechBridge MEA has also been recognised for excellence in distribution, being awarded Newland Distributor of the Year 2025 and previously winning their



Steve Lockie, Managing Director, TechBridge MEA and Dennis Oomen, Director of Sales & Business Development, TechBridge MEA.

marketing excellence award – affirming its impact and leadership across the region's distribution ecosystem.

Strategic timing and market momentum

Oman represents a compelling opportunity for regional technology distributors. The Oman ICT market was valued at approximately US\$5.31 billion in 2023 and is projected to reach around US\$8.22 billion by 2028 with a compound annual growth rate (CAGR) of 9.12%, highlighting sustained expansion in digital infrastructure and enterprise adoption. Beyond technology adoption, Oman is demonstrating broader economic transformation. According to regional economic data, the country's economy continued to grow through 2025, supported by expansion in non-oil activities and diversification efforts, with services and industrial sectors contributing to overall GDP growth. Oman Vision 2040 further emphasises sustainable diversification across logistics, green energy, tourism, and technology – bringing long-term structural growth that aligns seamlessly with TechBridge MEA's regional strategy.

“Opening our Oman office is a natural evolution of our regional growth strategy,” said Steve Lockie, Managing Director, TechBridge MEA.

“The country's diversified economic focus and expanding digital transformation ecosystem create an ideal environment for our partners to thrive. We are not here to just test the market, we're investing in its long-term success.”

The new Oman office will provide localised regulatory compliance – including withholding tax, VAT, and corporate governance—as well as on-the-ground technical support, partner account management, and logistics coordination. This presence will accelerate response times and deepen engagement with partners throughout the market.

Dennis Oomen, Director of Sales & Business Development, TechBridge MEA, said: “The response from partners in Oman has been overwhelmingly positive. With more than 40 partners requesting our presence here, it reinforces that our CVAD model adds real value where others have not yet prioritised. We believe this office will become one of the most dynamic hubs in the GCC.”

SUSE POWERS NEW ERA OF INNOVATION WITH FORMAL ENTRY INTO SAUDI ARABIA

The expansion brings power of open source software to fuel growth, innovation and digital sovereignty across the Kingdom.

SUSE, a global leader in enterprise

open source solutions, today formalises its operations in the Kingdom of Saudi Arabia. This marks a significant milestone in SUSE's long-term commitment to the region, and reinforces the Kingdom's central role in the company's Central Europe, Middle East and Africa (CEMEA) growth strategy.

The formal entry into the market will deepen SUSE's local presence, accelerate customer adoption of open technologies, and drive the development of high-skilled local jobs and technical training across Saudi Arabia. The move comes as the Kingdom's information and communications technology (ICT) market is entering a period of rapid expansion, estimated at around \$50.6 billion in 2024 and projected to reach \$76.05 billion by 2029. The country's data centre sector is also seeing significant growth, with expectations that it will exceed \$3.9 billion by 2030, supported by a cloud-first government strategy and large-scale public investment aligned with Vision 2030.

SUSE's presence in the Middle East is already well established, and this formal entry into Saudi Arabia complements existing regional activities, partner networks and customer relationships. The new entity will enable SUSE to deliver even closer support to enterprises and public sector bodies seeking to advance their digital transformation and data sovereignty goals.

"This is a defining moment for SUSE and for our customers and partners in Saudi Arabia. Our formal entry into the market signals our support of the Kingdom's vision and in its ambition to become a global technology hub,"



Ismail Ibrahim, General Manager, Central Eastern Europe, Middle East and Africa (CEMEA) at SUSE.

said Ismail Ibrahim, General Manager, Central Eastern Europe, Middle East and Africa (CEMEA) at SUSE.

"SUSE's mission is to empower enterprises and government entities to innovate freely with secure, open and interoperable infrastructure that reduce vendor lock-in and unlock real value. By putting people and skills at the heart of this expansion, we are creating the jobs and capabilities that will underpin digital sovereignty, resilience and long-term economic growth."

The Saudi expansion forms part of SUSE's wider CEMEA growth strategy, which prioritises localisation, ecosystem development and long-term regional investment. Establishing a formal entity in the Kingdom positions SUSE to support national priorities, from public sector modernisation to private sector cloud and edge

deployments, while strengthening the local innovation ecosystem through developer engagement, skills programs and collaboration with universities and partners.

"Saudi Arabia's Vision 2030 is built on a foundation of innovation, empowerment and partnership. SUSE's decision to invest and establish a local entity in the Kingdom demonstrates international confidence in our digital transformation journey," said Saleh Alharbi from Human Resources Development Fund.

"Open source technologies play a vital role in fostering agility, local talent development and knowledge transfer, all of which are essential for building a diversified and competitive digital economy. We look forward to working closely with SUSE to advance these shared goals."

CISCO INTRODUCES CISCO IQ, UNIFIED AI INTERFACE TO ACCELERATE TIME TO VALUE



Cisco has announced the launch of Cisco IQ, a breakthrough AI-powered digital interface that brings real-time insights, on-demand assessments, troubleshooting and personalised learning, automation and agents from across professional services and support into one powerful experience. Cisco IQ is expected to be generally available in Cisco's H2, FY2026.

Purpose-built for the AI era, where technology complexity can hinder essential operational agility, Cisco IQ brings together automation, AI-powered intelligence, and decades of deep Cisco expertise in a single digital experience, helping customers to plan, deploy, manage, secure, and optimise technology investments faster and more easily. Its proactive, predictive, and highly personalised features put customers a step ahead, helping them to reduce complexity, boost resiliency, and deliver measurable business outcomes.

"Cisco IQ is our boldest step yet in reimagining how customers interact with Cisco—from planning and design to optimisation and transformation," said Liz Centoni, Executive Vice President and Chief

Customer Experience Officer, Cisco. "With AI at its core, Cisco IQ doesn't just react. It intelligently anticipates, personalises and transforms how you assess, deploy and operate, providing one connected experience to reduce complexity and empower IT teams to act with clarity and confidence."

Cisco IQ helps to address this reality by transforming services and support from reactive fixes to strategic, predictive enablers — helping to reduce operational friction and cognitive load and enable earlier intervention. For customers, the result is a more resilient IT operation that can help focus resources on innovation and business transformation.

From Firefighting to Foresight

- Cisco IQ unlocks a new level of simplicity, resiliency and time to value, helping ensure trust and security via Cisco's transparent AI architecture and human oversight by design. It helps IT teams to:
- Anticipate and prevent issues with on-demand assessments covering security advisories, configurations, compliance, regulatory, quantum readiness and custom checks.
- Simplify operations and provide

dynamic, real-time visibility of entire asset inventory with planning for last day of support and lifecycle management.

- Accelerate resolution using AI-supported troubleshooting and streamlined case management.
- Benefit from hyper-personalised support with AI that adapts to each customer's unique environment.
- Realise deployment flexibility — SaaS, on-prem tethered, or on-prem air-gapped — with the ability to integrate Cisco IQ into existing systems.

Empowering partners to win in the AI era

Partners are at the heart of how Cisco delivers services and support to customers worldwide. With Cisco IQ, partners can address their customer needs across deployment modes and across the entire technology lifecycle. By equipping partners with advanced AI-powered capabilities, Cisco IQ can help them deliver more value to customers. Together, Cisco and its partners can help customers reduce complexity, make better-informed decisions, and keep pace with change — turning technology management into a strategic driver of business success.

SANS INSTITUTE PARTNERS WITH UAE CYBERSECURITY COUNCIL TO ENHANCE NATIONAL CYBER CAPABILITIES AHEAD OF QUANTUM ERA

SANS Institute, the global leader in

cybersecurity training and certifications, announced a landmark strategic partnership with the UAE Cybersecurity Council to advance the nation's cybersecurity readiness and reinforce the UAE's long-term vision for a secure and resilient digital future. The agreement was formalised during CyberQ 2025 in the presence of His Excellency Dr. Mohammed Alkuwaiti, Head of the UAE Cyber Security Council, and Ned Baltagi, Managing Director – Middle East, Turkey and Africa at SANS Institute.

This strategic partnership unites both entities under a shared commitment to strengthen national cybersecurity capabilities through cooperation across critical ICT and cybersecurity domains. The primary focus is to elevate national preparedness in cyberattack prevention, detection, and response, while deepening knowledge of emerging threats, and enhancing technical expertise across the workforce. As part of this initiative, SANS Institute conducted a workshop on 'Cybersecurity in the Quantum Era'. Going forward, the company will introduce future-oriented training programmes in Secure AI and Quantum Security that will equip cybersecurity professionals to navigate next-generation technological risks.

The MoU establishes a comprehensive framework for workforce development, providing access to globally recognised

- MoU signed during CyberQ 2025 to advance national cyber resilience
- Partnership expands access to advanced cyber training and globally recognised certifications
- Joint initiatives to prepare UAE's workforce for emerging and quantum-era threats



certifications, hands-on learning experiences, and expert-led technical workshops. This association will benefit professionals across the public and private sectors, from early-career practitioners to senior cybersecurity leaders, strengthening national capabilities through joint training sessions, specialist missions, and educational exchanges that expand exposure to advanced defence methodologies and global best practices.

Ned Baltagi, Managing Director – Middle East, Turkey and Africa, SANS Institute, said, "We are honoured to collaborate with the UAE Cybersecurity Council on this important national mission to enhance cyber resilience and support the country's digital transformation agenda. This MoU marks a significant milestone in our shared efforts to empower cybersecurity professionals with advanced expertise and future-ready skills. Through initiatives such as the Quantum Security program and our ongoing capability-building activities, we are committed to supporting the UAE as it strengthens its position as a

global leader in cybersecurity."

SANS Institute and the UAE Cybersecurity Council will also cooperate in key areas such as information sharing, capacity building, awareness initiatives, and advisory support, all aimed at strengthening national security priorities. Built on principles of equality, reciprocity, and mutual benefit, the partnership enables structured exchanges of expertise and operational insights to enhance the UAE's resilience against increasingly sophisticated cyber threats.

Both SANS Institute and the UAE Cybersecurity Council will continue to align their joint initiatives including technical workshops, cross-sector training programmes, and the exchange of threat intelligence and incident-response insights, reinforcing the nation's vision for a secure, innovative, and resilient digital future. The MoU is an important step forward in developing a highly capable national cyber workforce and ensuring the long-term safeguarding of the UAE's digital infrastructure and assets.

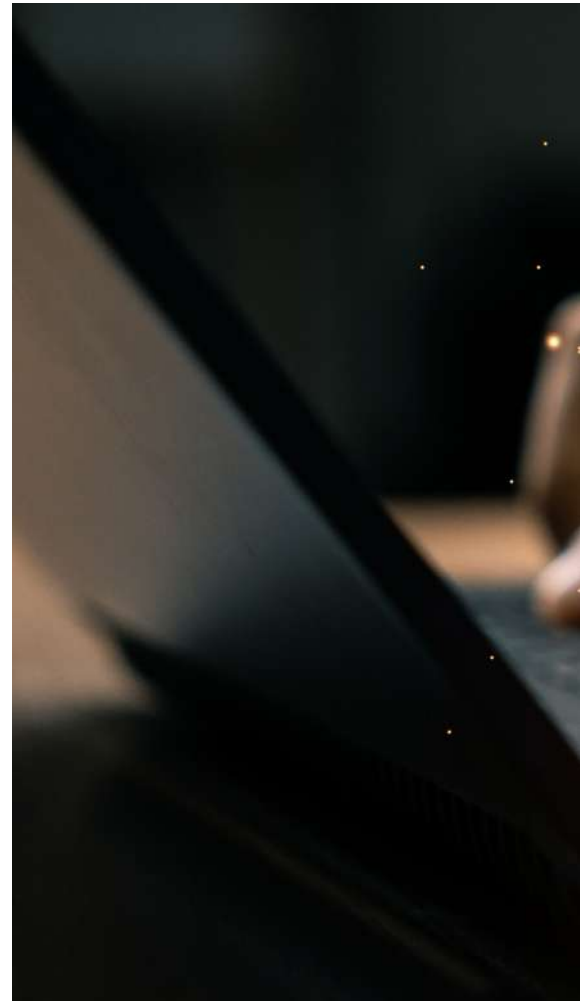
GOODBYE 2025, HELLO 2026! CYBER MATURITY MOVES FROM CONFIDENCE TO PROOF

CYBERSECURITY IN THE MIDDLE EAST IS SHIFTING FROM POINT CONTROLS TO ECOSYSTEM RESILIENCE. ATTACKERS ARE EXPLOITING THE SEAMS BETWEEN CLOUD PLATFORMS, AI-DRIVEN APPLICATIONS, PARTNERS, AND SUPPLIERS — WHILE BOARDS AND INSURERS DEMAND PROOF THAT CRITICAL DATA CAN BE RECOVERED CLEANLY, QUICKLY, AND WITHIN JURISDICTION. IN 2026, CYBER MATURITY WILL BE MEASURED, NOT ASSUMED.

If 2025 delivered a clear lesson for security leaders, it was that modern attacks no longer respect the tidy boundaries implied by organisational charts or technology stacks. Threats rarely arrive as a single, isolated strike against one system. Instead, they move through the spaces in between — connecting cloud platforms and SaaS environments, linking AI-driven applications with data stores, crossing organisational perimeters via suppliers, and exposing the gap between security

assumptions and real-world system behaviour under pressure.

Across the region, this shift is already taking shape. Cyber resilience in 2026 will be defined less by standalone controls and more by the strength of the digital ecosystem and the operational capabilities supporting it. Attackers increasingly focus on the gaps between platforms, partners and data flows, where visibility is weaker and accountability is shared, rather than repeatedly attacking a single, well-fortified asset.



“Cyber maturity is only as strong as your weakest link,” says Gregg Petersen, Regional Director for the Middle East at Cohesity. It is a line that sounds familiar — almost obvious — until you view it through a 2025 lens. The weakest link is no longer just a missed patch, a careless click, or a stale credential. It might be a supplier’s cloud configuration, a partner’s data handling practice, a shadow AI workflow no one is monitoring, or an internal legacy system that quietly undermines an otherwise modern security programme.

Goodbye 2025, then. Hello to 2026 — the year when cyber maturity stops being a slogan and becomes something organisations must prove.

Confidence is high. Recoverability is harder

On paper, many organisations feel ready.



In practice, readiness is being challenged by the realities of distributed data, multi-cloud operations, and increasingly complex third-party relationships.

Cohesity's research, conducted on the sidelines of GITEX Global 2025, captures the tension playing out across the UAE. Sixty-six percent of organisations report full compliance with national data protection laws. Yet one in three still struggle to keep up with evolving regulations. Compliance has improved, but the bar keeps rising.

A second shift is even more telling. Nearly seven in ten organisations now review their AI governance practices every six months or less. AI oversight is rapidly becoming a continuous operational requirement rather than an annual audit exercise. The driver is not abstract ethics. It is operational risk:

shadow AI usage, volatile data flows, and the fear that AI systems could introduce new exposure points that traditional governance was never designed to spot.

Eighty-seven percent of organisations believe they can recover quickly from an incident. Yet many still struggle to validate the integrity of their data across multi-cloud environments and external service providers. Recovery is not the same as recoverability — and it is certainly not the same as verified, jurisdiction-aligned restoration under pressure.

The sovereignty conversation is evolving in parallel. Cohesity's research shows 62 percent of UAE organisations now monitor compliance directly across third-party suppliers. This signals a sovereignty-first mindset: organisations are taking ownership of governing their

wider ecosystem, rather than assuming partners have it covered.

Yet despite the investment, 57 percent of UAE organisations still classify themselves as "at risk". That disconnect matters. It suggests the region is moving forward on compliance frameworks and governance, but operational resilience — the ability to restore clean, uncompromised data at speed and keep the business running — remains the hardest part to mature. The lesson is not that organisations are failing. It is that maturity is moving from what you deploy to what you can demonstrate

2026 will reward proof, not posture

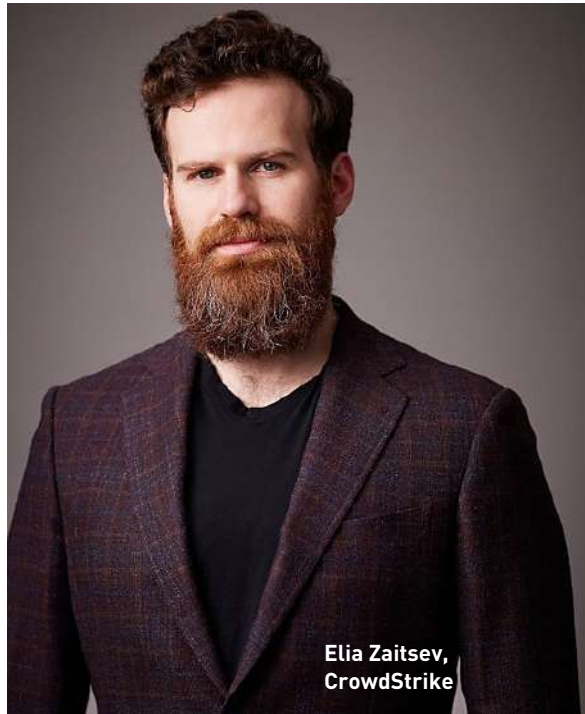
If 2025 was the year of rising cyber confidence, 2026 will be the year of scrutiny. Data risk posture is set to become a board-level priority, driven by

stricter expectations, AI-generated data flows, and increasing pressure to demonstrate oversight across cloud and third-party environments. In many organisations, “data” has long been treated as an IT asset, while “security” is treated as a technical function. Boards are increasingly focused on what happens during disruption: where critical data resides, how quickly it can be restored, and whether it can be restored cleanly.

This is where the concept of verified recoverability becomes a defining theme. Assumed recoverability is no longer enough — not when ransomware and wiper-style disruptions force organisations to demonstrate clean, sovereign and jurisdiction-aligned restoration. End-to-end data protection is becoming non-negotiable, with organisations expected to prove that critical datasets are recoverable across on-premises, cloud and edge locations.

The biggest shift, however, is conceptual. Cyber maturity in 2026 will be less about the strength of individual defences and more about the collective integrity of the digital ecosystem. It is a team sport — not in the motivational-poster sense, but in the operational sense: suppliers, platforms, identity systems, data governance, and recovery

**THIS IS THE ERA
WHERE IDENTITY
SECURITY MEANS
PROTECTING ENTITIES
THAT DON'T HAVE A
PULSE.
ELIA ZAITSEV,
CROWDSTRIKE**



**Elia Zaitsev,
CrowdStrike**

playbooks must work together under stress.

AI is not inventing but accelerating

In the public imagination, AI is often framed as a wave of brand-new threats. In the trenches, many practitioners see it differently: AI is not replacing the threat landscape — it is compressing time and expanding volume.

Eric Doerr, Chief Product Officer at Tenable, challenges a common assumption. “There will be no truly new attack vectors in 2026,” he argues. “AI is not a magic wand — it amplifies traditional attack methods by reducing the cost of attack generation and increasing volume.” The implication is blunt: security remains a numbers game, and AI simply broadens attackers’ reach. In that environment, basic cyber hygiene remains one of the most effective defences.

That does not diminish the risk. It reframes it. The greatest threat to organisations is acceleration. AI-fuelled attacks can start and finish before a ticket is even created. When speed becomes the weapon, the “who, what, how and why” matter less than whether

a security programme can move quickly enough to make attacker speed irrelevant.

Kaspersky’s late-December 2025 predictions reinforce the same trajectory from another angle. Deepfakes are becoming mainstream, and awareness will continue to grow. Organisations are discussing synthetic-content risks more openly and training employees to reduce the likelihood of being fooled. But as awareness rises, so does the range and quality of deepfakes — particularly as realistic audio improves and the barriers to creating convincing fakes keep dropping.

The result is an uncomfortable normalisation. AI can produce well-crafted scam emails, convincing visual identities, and polished phishing pages.

Meanwhile, brands are adopting synthetic materials in advertising, making AI-generated content look familiar and visually “normal”. Distinguishing real from fake becomes harder for humans and automated detection alike.

Kaspersky expects AI to become a cross-chain tool in cyberattacks, used across most stages of the kill chain — from preparation and communication to assembling malicious components, probing for vulnerabilities and deploying tools. Threat actors will also work to hide signs of AI involvement, making operations harder to analyse.

At the same time, AI is becoming a tool for defenders. Agent-based systems will increasingly scan infrastructure, identify vulnerabilities and gather context for investigations, reducing manual routine work. Over time, SOC teams shift from manually searching for signals to making decisions based on already-prepared context. Natural-language interfaces are likely to spread, enabling prompts instead of complex technical queries.

The key point for 2026 is not whether AI is “good” or “bad”. It is that it is now part of both the problem and the solution

— and it amplifies the importance of operational readiness.

The new cyber boardroom: outcomes, sovereignty, and accountability

AI hype gives way to operational reality, boards are becoming less interested in novelty and more interested in outcomes.

SAS calls 2026 “a great AI reality check” — a year of accountability, when organisations and vendors will be pressed to demonstrate ROI and confront ethical and economic questions head-on. The honeymoon phase of “AI innovation at any cost” is fading, replaced by tougher questions about accuracy, cost, measurable savings and governance. Trustworthy AI is not just a compliance story; it is a performance story. Without strong data management and oversight, AI cannot come of age inside the enterprise.

This intersects directly with sovereign AI, which is accelerating as organisations, cities and nations seek greater control over how data is stored, processed and governed within borders. Keeping data within corporate or geographic boundaries strengthens privacy, compliance and autonomy. But it also raises a new leadership test: can organisations balance sovereignty with innovation, interoperability and cross-border collaboration?

For Middle East enterprises operating across multiple jurisdictions and cloud environments, sovereignty is not a checkbox — it is an operating principle. And it is increasingly tied to the question insurers are asking: not just “How protected are you?” but “Can you recover within the rules that apply to you?”

Cyber maturity is rewriting the insurance playbook

If you want a clear indicator of where 2026 is heading, look at the

insurance market.

Johnny Karam, Managing Director and Vice President, International Emerging Markets at Cohesity, argues that by 2026 cyber insurance will no longer be a reactive safety net. It will be a proactive barometer of digital resilience, linking cover and cost directly to measurable maturity.

The same GITEK Global 2025 research paints the picture. Sixty-six percent of UAE organisations report full compliance with national data protection laws, yet a third still struggle with evolving regulations. Sixty-two percent monitor compliance across third-party and multi-cloud providers, signalling that sovereignty has shifted from a regulatory requirement to a core operational priority. And although 87 percent believe they can recover quickly, distributed data flows are challenging that confidence in practice.

Karam points to the disconnect that insurers increasingly focus on. Even as organisations strengthen compliance

CYBER MATURITY IS ONLY AS STRONG AS YOUR WEAKEST LINK.
GREGG PETERSEN, COHESITY

and governance, many still struggle to restore clean, sovereign, uncompromised data at speed during disruption. The practical consequence is straightforward: insurers are tightening requirements and placing more emphasis on verified recovery capability when determining coverage and cost.

Three shifts are likely to define the UAE cyber insurance landscape in 2026.

First, recovery-led underwriting. Insurers will prioritise evidence of rapid, reliable recovery. Organisations that can demonstrate strong recovery discipline, integrity validation and mature backup foundations will be positioned for better coverage terms and more favourable pricing.

Second, sovereignty-driven risk scoring. Data sovereignty becomes a central factor in risk evaluation. Insurers will seek assurance that sensitive information can be recovered within national boundaries and in line with local regulations. Fragmented cross-border data arrangements will invite stricter requirements.

Third, operational resilience over individual tools. Insurers increasingly accept that even well-protected organisations can still be breached. What matters more is the ability to maintain operations, isolate clean backups and validate data integrity across cloud providers and suppliers.



Gregg Petersen,
Cohesity

In this model, resilience is not just risk reduction. It is a measurable asset.

Identity time bomb: non-human identities and AI agents

If data and recoverability are one pillar of 2026 cyber maturity, identity is the other — and it is expanding far faster than governance.

Liat Hayun, SVP Product Management and Research at Tenable, warns that non-human identities — service accounts, tokens, APIs and machine credentials — are set to become the number one cloud breach vector. The primary risk shifts away from misconfigurations or missing patches and towards vast numbers of over-permissioned machine identities that attackers — or autonomous agents — can exploit for silent lateral movement.

This is where 2026 becomes uncomfortable for organisations that still treat identity as a human problem. Permissions governance and large-scale identity clean-up move from “technical backlog” to “business continuity”.

CrowdStrike’s CTO, Elia Zaitsev, takes the point further. In 2026, AI agents and non-human identities will explode across the enterprise and dwarf human identities. Each agent could operate as a privileged super-user with OAuth tokens, API keys and continuous access to previously siloed datasets — making them powerful and potentially dangerous entities in the environment.



Eric Doerr, Tenable

The crux is accountability. Identity security built for humans will not survive this shift. Security teams will need real-time visibility, instant containment, and the ability to trace agent actions back to the human who created or authorised them. When an agent wires money to the wrong account or leaks intellectual property, “the AI did it” will not be an acceptable answer.

This is where cyber maturity stops being about technology and becomes about governance design: how permissions are granted, how actions are logged, and how decisions are audited.

Prompt injection and new AI attack surface

The AI interaction layer is becoming its

own security frontier. Zaitsev describes prompt injection as a frontier security problem: adversaries embed hidden instructions to override safeguards, hijack agents, steal data and manipulate models — turning prompts into a new attack surface. In this landscape, organisations will increasingly need visibility into prompts, responses, agent actions and tool calls to contain AI abuse before it spreads.

The direction of travel is clear even if broad adoption takes time: as EDR became essential for endpoints, AI-centric monitoring and response capabilities will become increasingly important as organisations operationalise agentic systems.

The warning for 2026 is practical: if an organisation cannot observe what its AI systems are being asked, what they are doing, and what they are touching, it cannot claim mature governance — regardless of how polished the AI deployment looks.

Agentic SOC: 2026 — Pilot year

The industry is entering what many leaders describe as the “utility phase” of AI — less novelty, more outcomes.

Bob Huber, Chief Security Officer at Tenable, expects security leaders to move beyond off-the-shelf AI tools and focus on building customised AI solutions tailored to their organisation’s needs. Done carefully, these tools can improve security operations and reduce burnout — a key concern in a region where skills shortages remain persistent.

Huber also suggests a mindset shift around automation. Automatic remediation, mobilisation and mitigation will become less taboo. For years, teams avoided automation out of caution. But as attack speed and surface area expand, organisations will challenge the belief that “automatic is forbidden”.

AI IS NOT A MAGIC WAND — IT AMPLIFIES TRADITIONAL ATTACK METHODS BY REDUCING THE COST OF ATTACK GENERATION AND INCREASING VOLUME.
ERIC DOERR, TENABLE

Still, the best leaders will balance ambition with readiness. Hayun cautions that despite hype, agentic security tools will not see broad adoption in 2026. Most organisations are not yet ready to entrust critical decisions to AI due to gaps in data quality, governance, platform consolidation and trust. The year ahead is likely to be defined by pilots, controlled experiments and building the foundations for wider adoption from 2027.

CrowdStrike's view aligns: defenders evolve from alert handlers to orchestrators of an agentic SOC — agents that reason, decide and act at machine speed, under human command. But success depends on prerequisites: environmental context, mission-ready agents trained on expert decisions, validation benchmarks, customisation, and coordinated collaboration between analysts and agents.

In other words, the agentic SOC is not a product. It is an operating model — and it demands maturity first.

Ecosystem-first thinking and the end of standalone categories

Axis Communications' technology trends point to an "ecosystem-first" approach becoming increasingly central: the first decision is defined by the solution ecosystem a customer commits to, with integration, management, scalability and lifecycle support becoming easier within an ecosystem.

This thinking mirrors what is happening in cyber. Tool sprawl is under pressure. CISOs are pushed to reduce duplicated spend and operational drag. In that environment, categories that once stood alone begin to converge.

Hayun predicts that CSPM will disappear as a standalone category in 2026 as unified exposure management platforms consolidate identity risk, posture, runtime and network context. The goal is not just fewer logos on an architecture slide. It is a clearer, unified view of risk across cloud, hybrid environments and third parties — the very seams attackers exploit.

The practical message for 2026 is to treat integration, visibility and lifecycle support as security controls in their own right. A fragmented ecosystem creates blind spots. A coherent one makes governance and operational resilience more achievable.

2026 operational resilience playbook

So what does cyber maturity look like when it is measured rather than assumed? Across the themes from Cohesity, Tenable, CrowdStrike, Kaspersky, SAS, and Axis, six priorities stand out for 2026 — not as trends, but as operating requirements.

1) Make data risk posture a board-level agenda item.

AI-generated data flows and regulatory expectations will force boards to demand clarity: where critical data is, who touches it, and how risk is managed across cloud and third parties.

2) Make end-to-end data protection non-negotiable.

Organisations must be able to protect and recover critical datasets across on-premises, cloud and edge locations — not as a best effort, but as a requirement.

3) Replace assumed recoverability with verified recoverability.

It is no longer enough to believe you can recover. You must be able to demonstrate clean, uncompromised, jurisdiction-aligned restoration — including integrity validation — during ransomware or destructive attacks.

4) Treat AI governance as a core resilience pillar.

Continuous oversight of model behaviour, monitoring AI-driven data flows and enforcing guardrails will become standard. And as AI is deployed across diverse workforces and markets, organisations must ensure models operate effectively across major languages rather than relying on English-first deployments that can create

governance blind spots.

5) Accelerate sovereign AI adoption — but balance it.

Sovereign AI strengthens privacy and strategic autonomy by keeping data within corporate or geographic boundaries. Long-term value will depend on balancing sovereignty with interoperability, innovation and cross-border collaboration.

6) Practise operational resilience. Routinely.

Resilience will be defined by real-world readiness: testing applications, identity systems and recovery playbooks to reduce downtime and keep critical services running when disruption hits.

The leaders of 2026 will be those who recognise that resilience is built collaboratively, not defensively — across partners, platforms and policies.

Goodbye 2025, hello to measurable maturity

If 2025 exposed the vulnerabilities in modern ecosystems, 2026 will expose something else: whether organisations can execute.

In the Middle East's cloud-first, AI-forward environment, attackers will continue to target the seams — between systems, suppliers, identities and data flows. Boards will demand outcomes, not activity. Insurers will price verified recovery, not confidence. And AI will continue to accelerate both attack speed and defensive capability, forcing security teams to rethink how they operate.

Cyber maturity in 2026 will not be about the strength of individual defences. It will be about the collective integrity of the ecosystem — and the ability to prove, under pressure, that operations can be restored safely, quickly and within the rules that matter.

In that sense, the goodbye to 2025 is not sentimental. It is strategic.

Because the future belongs to those who treat resilience as a team sport — and cyber maturity as something you can measure. 🧑

SANS GULF REGION 2025 HIGHLIGHTS SKILLS RESHAPING CYBERSECURITY IN AI-DRIVEN GCC

I DRAWING ON SANS GULF REGION 2025, NED BALTAGI EXPLAINS WHY AI SECURITY, CLOUD DEFENCE, AND ADVANCED INCIDENT RESPONSE ARE CENTRAL TO THE GCC'S CYBER READINESS.

Governments and enterprises across the GCC are accelerating AI adoption, cloud transformation, and smart-city initiatives, driving a sharp shift in cybersecurity priorities toward advanced defence, operational resilience, and skills development. SANS Institute has been at the forefront of this evolution, playing a critical role in building future-ready cyber talent across the Middle East, Turkey, and Africa.

Ned Baltagi, Managing Director – Middle East, Turkey and Africa, SANS Institute, spoke to Sandhya D'Mello, Technology Editor, Security Advisor Middle East and shared about the key themes, participation trends, and insights from SANS Gulf Region 2025, highlighting how AI security, cloud and Zero Trust architectures, incident response, and critical infrastructure protection are shaping the next phase of regional cybersecurity readiness.

Interview excerpts:

What was the key theme and focus of SANS Gulf Region 2025 this year? How do they reflect the current cybersecurity priorities in the GCC?

The central theme of SANS Gulf Region 2025 was advancing future-ready



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



cybersecurity capabilities for an AI-driven and increasingly automated world. With regional governments prioritising AI, smart-city infrastructures, cloud expansion, and advanced digital economies, the event focused heavily on AI cybersecurity, GenAI and LLM security, offensive AI, critical infrastructure resilience, and advanced cyber defence operations. This directly aligns with regional priorities. With the UAE, KSA, and broader GCC accelerating digital transformation, the region requires a highly skilled workforce capable of defending national digital initiatives. SANS is building the GCC's advanced cyber talent to safeguard AI adoption, smart-city ecosystems, and critical national infrastructure, ensuring that organisations can protect sensitive data, maintain trust, and stay ahead of increasingly sophisticated adversaries.

Could you give us insight into which training programmes, talks, or courses gained the most traction and why?

Among the 14+ specialised courses offered, certain domains gained noticeably higher traction among participants, reflecting strong interest and engagement in these areas

- The high demand for GenAI & LLM Security course reflects the rapid

adoption of AI across government and enterprises in the Middle East region. The cybersecurity professionals demonstrated a keen interest in understanding more about AI-driven phishing and content generation attacks; adversarial AI and model manipulation; as well as secure deployment of LLM-based applications.

- As GCC countries expand towards public and private cloud investments, participants gravitated towards understanding Cloud and Zero Trust Security in-depth with focus on multi-cloud security, identity governance, and implementation of zero trust architecture.

SANS IS BUILDING THE GCC'S ADVANCED CYBER TALENT TO SAFEGUARD AI ADOPTION, SMART-CITY ECOSYSTEMS, AND CRITICAL NATIONAL INFRASTRUCTURE.

- Digital Forensics and Incident Response (DFIR) is a priority aligned with national cybersecurity mandates. We saw high subscription from participants for hands-on lab in IR, memory forensics, and ransomware investigations, showcasing the need for operational expertise.
- With the regions reliance on energy, utilities, and industrial sectors, ICS security courses were also a priority especially for professionals safeguarding essential services.

The Community Night Talks featuring experts Frank Kim, Mattia Epifani, and Ahmed Abugarbia drew a lot of interest and engagement. The sessions addressed topics such as cybersecurity leadership, AI cybersecurity, cloud security, threat intelligence, and advanced defence strategies, that gave attendees strategic and technical insights meaningfully complementing their curriculum.

How was the participation this year compared to previous editions?

This year's edition, spanning over three weeks, saw high levels of engagement across all delivery formats. The combination of in-depth courses, NetWars tournaments, and interactive labs kept participants deeply involved



throughout the event. Participants also highlighted that the event served as an excellent opportunity to network with industry peers, exchange perspectives, and build professional relationships across sectors, an added value that strengthened the overall experience. The instructors found the sessions interactive with participants contributing to the discussions with great questions and deliberations, making the learning process interesting and engaging.

What was the feedback from participants on the event, the training, demos, and Night Talks?

The feedback from participants were consistently positive and encouraging. They found the hands-on sessions highly relevant, especially the real-life scenario presented during the lab sessions that closely reflected current evolving threat landscape, including AI-driven attacks. SANS Instructors' expertise was frequently commended for their clarity, practical experience, and ability to present complex concepts in an applied and accessible manner. Participants also highlighted that the Community

Night Talks provided forward-looking perspectives on cybersecurity leadership, emerging threats, and operational best practices.

"Overall, delegates expressed strong satisfaction with the experience, citing the programme's structure and pacing, the quality of digital and print resources, and the added value of earning CPE credits and progressing toward GIAC certifications."

What were the key insights shared by SANS instructors during the entire duration of the event?

SANS Instructors shared several core insights throughout the course duration and in interactive sessions. Offensive AI is rapidly enabling attackers to scale and automate complex operations, making it vital for defenders to understand and anticipate AI-driven attacks. Zero Trust was consistently reinforced as a foundational requirement rather than an optional approach for organizations managing extensive cloud and identity ecosystems. Various discussions also highlighted that modern SOCs must adopt automation and advanced analytics

to remain effective against increasingly sophisticated threat actors. In parallel, ICS security was identified as needing to evolve from largely passive monitoring models to proactive defence strategies, particularly as critical infrastructure systems become more interconnected. The importance of adapting digital forensics to new and advanced attack techniques, especially those designed to obscure malicious activity and evade detection, was another recurring theme. Finally, the sessions emphasised that mature cybersecurity leadership is essential to ensure governance, resource allocation, and strategic priorities keep pace with rapid technological and threat landscape changes. SANS Gulf Region 2025 reaffirmed SANS Institute's leadership in shaping the cybersecurity talent landscape of the Middle East. By offering world-class training, global instructor expertise, competitive NetWars simulations, and deep-dive discussions on AI and future threats, SANS continues to serve as the region's gateway to cutting-edge cybersecurity knowledge and sustained professional advancement. 📌

CYBERSECURITY'S GLOBAL STAGE



REGISTER FOR YOUR FREE PASS TODAY

DATA-CENTRIC SECURITY TAKES CENTRE STAGE IN SAUDI ARABIA'S DIGITAL TRANSFORMATION

I SECLORE'S URAZ FARUKH EXPLORES HOW THE KINGDOM'S REGULATORY DIRECTION AND AI ADOPTION ARE SHAPING THE FUTURE OF COMPLIANCE AND CYBER RESILIENCE.

Saudi Arabia's rapid digital expansion is reshaping how organisations approach governance, risk, and compliance, creating a transformative moment for cybersecurity in the Kingdom. With national regulators strengthening frameworks and enterprises accelerating cloud, AI, and data-driven initiatives, the demand for mature, adaptive, and intelligence-led security models has never been greater. Compliance is no longer viewed as a checkbox exercise — it has become a strategic pillar that supports innovation, sovereignty, and long-term digital resilience.

Within this evolving landscape, Seclore is playing a significant role in helping organisations secure sensitive data across decentralised, multi-cloud, and AI-enabled environments. Speaking to Daniel Shepherd, Online Editor, Tahawultech.com at Black Hat MEA 2025, Uraz Farukh, Vice President Sales – MENA, shared a detailed perspective on Saudi Arabia's cybersecurity maturity, emerging gaps and opportunities, and how Seclore's product strategy aligns with the Kingdom's national digital transformation agenda. Farukh also reflects on the strategic value of Black Hat MEA as a platform for collaboration,

customer engagement, and shaping the region's cybersecurity dialogue.

Interview excerpts:

How do you see the Saudi compliance landscape evolving over the next few years?

Saudi Arabia has made tremendous progress in advancing national cybersecurity standards.

Regulators have strengthened guidelines to ensure organisations adopt robust frameworks, enforce data governance, and build resilience against emerging threats. As AI, cloud, and next-generation technologies continue to enter the market, compliance will evolve to accommodate new models of risk and data flow. Organisations will increasingly need to integrate data-centric controls, adaptive security, and continuous monitoring to remain compliant as technologies become more complex. The direction is clear: Saudi Arabia is pushing toward stronger cybersecurity sovereignty while enabling innovation at scale.

What is your assessment of cybersecurity maturity in the Kingdom of Saudi Arabia, and where do you see the most significant gaps or opportunities?

Saudi Arabia has emerged as a regional

— and increasingly global — leader in cybersecurity maturity. Enterprises and government bodies have invested heavily in frameworks, technologies, and talent.

The biggest opportunities now lie in:

- advancing AI-driven security
- integrating identity and data governance
- strengthening automation within security operations
- addressing gaps introduced by cloud expansion and decentralised data flows

AI, in particular, is a major enabler. New innovations introduce fresh challenges and require security architectures capable of scaling with these emerging risks. Saudi organisations are ambitious and forward-thinking, and we see the Kingdom playing a leadership role in defining the future of secure digital transformation.

How does Seclore's product strategy align with Saudi Arabia's national visions and ongoing digital transformation initiatives?

Saudi Arabia's digital ambitions — from giga-projects to AI-native smart zones — require new approaches to protecting data in motion and at rest.

Seclore aligns directly with these national priorities by delivering



Uraz Farukh
Vice President Sales – MENA, Seclore

continuous visibility, intelligence, and control over data as it moves across increasingly complex ecosystems. Whether organisations are adopting sovereign cloud, scaling AI, or modernising infrastructure, Seclore provides the security backbone that supports innovation without compromising compliance or sovereignty. The Kingdom's leadership in regulation and its bold digital roadmap make it an ideal environment for Seclore's platform.

What strategic value does Seclore gain by participating in Black Hat MEA 2025, and how does it support your engagement with regional stakeholders?

Black Hat MEA offers a unique opportunity to meet customers, regulators, and industry leaders who are driving cybersecurity transformation in the region.

For Seclore, it is a platform to:

- demonstrate the relevance of our technologies

- deepen engagement with strategic customers
- collaborate with local partners
- understand emerging sector-specific challenges
- contribute to national cybersecurity dialogue

Participation helps us stay close to the regional ecosystem and ensure our roadmap continues to align with the ambitions of the Kingdom and wider Middle East. 🇰🇸

FORESCOUT OUTLINES OT SECURITY PRIORITIES AS SAUDI ARABIA ACCELERATES DIGITAL INDUSTRIAL GROWTH

MOHAMMAD TAHMAZ, COUNTRY SALES MANAGER – KSA, DISCUSSES HOW REAL-TIME VISIBILITY, SEGMENTATION, AND THREAT INTELLIGENCE ARE SHAPING THE KINGDOM’S NEXT PHASE OF CRITICAL INFRASTRUCTURE PROTECTION AT BLACK HAT MEA 2025.

Forescout’s presence at Black Hat MEA 2025 reflects a pivotal moment for cybersecurity in the Middle East, where OT-IT convergence, smart infrastructure, and giga-project expansion are redefining national risk landscapes. Mohammad Tahmaz, Country Sales Manager – KSA, spoke to Daniel Shepherd, Online Editor, Tahawultech on how real-time visibility, automated control, and threat intelligence are becoming essential foundations for securing industrial environments. Tahmaz’s insights highlight the region’s growing urgency to safeguard critical infrastructure against increasingly sophisticated adversaries.

Interview excerpts:

What are Forescout’s key priorities and focus areas at Black Hat MEA 2025, and how does your presence this year reflect the region’s growing urgency around OT security?

Our focus at Black Hat MEA 2025 is centred on raising awareness around OT security and demonstrating how organisations can build resilient, real-time defence





capabilities across complex hybrid environments. The region is undergoing rapid digital transformation, and with that comes an urgent need to secure operational environments that were never originally designed for connectivity. We are showcasing how Forescout delivers continuous visibility, automated control, and risk-based response across OT, IT, and IoT ecosystems—capabilities that are now essential as Saudi Arabia accelerates industrial digitalisation.

With OT-IT convergence accelerating across energy, utilities, transport and manufacturing, what new vulnerabilities are you seeing, and how does Forescout help organisations secure these blended environments?

OT-IT convergence is expanding the attack surface dramatically. Many organisations are transitioning from legacy, isolated systems to highly connected environments with an increasing number of IoT and smart devices. This shift introduces vulnerabilities related to outdated platforms, misconfigurations, and devices that were never intended to be exposed. Forescout supports organisations by identifying every device—managed or unmanaged—profiling its behaviour, and applying automated policy-based controls. This helps maintain security as industrial

networks evolve and adopt modern technologies.

Gaining real-time visibility into OT assets remains a major challenge in the Middle East. How does Forescout's platform address unmanaged devices, legacy systems and segmentation gaps across industrial networks?

Unmanaged and legacy devices continue to be one of the biggest risks in OT environments. Forescout provides deep, continuous visibility into all assets the moment they appear on the network, without requiring agents. We detect devices across previously siloed segments, highlight gaps in network segmentation, and allow operators to enforce micro-segmentation with precision. This enables organisations to secure legacy infrastructure while progressively modernising their industrial architecture.

As Saudi Arabia scales giga-projects and smart city deployments, how is Forescout supporting critical infrastructure operators in building secure-by-design OT ecosystems?

Saudi Arabia's giga-projects and smart city initiatives depend on highly interconnected OT-IT environments. Forescout helps operators design networks where security is embedded from the start, not added

later. Modern smart facilities no longer rely on a single, flat network; they have multiple specialised systems that must be isolated, monitored, and managed intelligently. Our platform provides the orchestration layer that enforces segmentation, monitors device interactions, and ensures that every asset maintains compliant behaviour across expanding digital infrastructures.

Ransomware groups and nation-state actors are increasingly targeting OT environments. What does Forescout's threat intelligence indicate about evolving attacker behaviour in the region, and what defensive actions should organisations prioritise?

Threat actors are becoming more sophisticated, and they are actively exploiting the complexity of modern industrial environments. Ransomware groups and nation-state adversaries are leveraging unmanaged devices, legacy assets, and segmentation blind spots to move laterally and disrupt operations. Forescout's threat intelligence provides continuous visibility into these behaviours, allowing organisations to detect anomalies early and respond before attackers can achieve impact. The priority now is to adopt automated detection, enforce segmentation, and maintain continuous monitoring across every device and protocol used in OT ecosystems. 🔒

GROUP-IB CHARTS NEXT FRONTIER OF CYBER DEFENCE IN SAUDI ARABIA

IDMITRY VOLKOV HIGHLIGHTS HOW AI-DRIVEN THREATS, PREDICTIVE SECURITY, AND REAL-TIME FRAUD INTELLIGENCE SHARING ARE RESHAPING THE KINGDOM'S CYBERSECURITY ECOSYSTEM.

Saudi Arabia's cybersecurity landscape is entering a defining phase, shaped by rapid digital growth, AI-enabled threats, and a nationwide push for stronger cyber resilience. Against this backdrop, Group-IB is deepening its presence in the Kingdom, bringing adversary-centric intelligence, predictive defence capabilities, and new ecosystem-wide fraud prevention technologies to the market.

Dmitry Volkov, CEO of Group-IB, spoke to Daniel Shepherd, Online Editor, Tahawultech.com about how AI-driven cybercrime is reshaping risk, why collaborative defence models are becoming essential, and how the company's newly launched Central Fraud Intelligence Platform (CFIP) is set to transform real-time fraud intelligence sharing across Saudi organisations.

Interview excerpts:

You've been expanding quickly in Saudi Arabia this year. What's driving demand for Group-IB's solutions across Saudi enterprises?

Saudi Arabia is a highly mature market, and organisations here know exactly what they want. They are looking for best-in-class technical capabilities that allow them not only to close gaps but to build advanced, service-driven security programmes. Demand for Group-IB stems from our adversary-centric approach and our ability to help enterprises focus on threat factors

rather than just raw attacks. Because we conduct deep research on cybercriminal activity across global regions, our technologies allow customers to predict what may happen next and build stronger, more proactive cyber defences.

Looking at 2025 and beyond, what advanced Tactics, Techniques, and Procedures (TTPs) or threat groups are most actively targeting the Kingdom?

It varies by industry, but the overarching trend is clear: AI-enabled cybercrime is becoming the dominant threat. Fraud-focused criminal groups are adopting AI faster than any other segment—particularly video and voice deepfakes, which dramatically increase the success rate of scams. We also see sophisticated cyber attackers using AI to automate reconnaissance, vulnerability identification, and exploitation workflows. These AI-driven attacks operate at very high speed, so defenders need equally advanced technologies that can match or ideally anticipate the next step in the kill chain.

If you had to distil it into five points, what actionable threat insights should Saudi CISOs take away from Black Hat MEA 2025?

1. Shift away from legacy mindsets. Traditional security approaches no longer match the pace and sophistication of modern threats.
2. Adopt collective defence. Saudi enterprises need to collaborate more closely—sharing real-time cyber

intelligence, fraud patterns, and threat telemetry.

3. Unify cyber and fraud operations. Criminals do not distinguish between these domains; defenders should not either.
4. Prioritise real-time intelligence. Rapid visibility into attacker behaviour is essential for resilience.
5. Move towards predictive security. AI-driven, behaviour-based modelling is the next frontier for advanced cybersecurity.

Tell us more about the CFIP launch. What technology sits behind it, and how does it solve gaps existing fraud systems cannot?

Every fraud system—behavioural, transactional, or rule-based—inevitably leaves gaps. Organisations increasingly want to share real-time fraud intelligence with banks, fintechs, telcos, regulators, and major e-commerce platforms.

The Central Fraud Intelligence Platform (CFIP) solves this by enabling live information exchange while ensuring zero sensitive data ever leaves the organisation.

Group-IB uses a patented tokenisation mechanism that allows entities to compare and correlate fraud signals without exposing personal or regulated data. This achieves two goals simultaneously:

- real-time collaboration across the ecosystem
- full compliance with privacy and data-protection requirements



Dmitry Volkov, CEO, Group-IB

This is a breakthrough because it bridges a long-standing gap between the need to share intelligence and the need to protect customer information.

How is Group-IB collaborating with Saudi companies and global vendors to build a more unified cybersecurity ecosystem?

We work closely with Saudi regulators, public-sector bodies, and major enterprises, helping strengthen national cyber resilience. Group-IB has built a full technical infrastructure and a local expert team within the Kingdom, ensuring our customers receive in-country expertise and support.

Our full-stack platform integrates

across the technologies that organisations have already invested in—whether on-premises or cloud-based—so that existing tools are enhanced rather than replaced. This integrated approach helps automate routine actions, improve operational efficiency, and unify cyber and fraud defence across the ecosystem. [i](#)

HYBRID VISIBILITY, AI OBSERVABILITY, AND POST-QUANTUM READINESS WILL DEFINE 2026, SAYS GIGAMON OFFICIAL

I DANIELLE KINSELLA, SENIOR DIRECTOR – SALES ENGINEERING, GIGAMON, EXPLAINS HOW SAUDI ENTERPRISES ARE LEAPFROGGING GLOBAL MARKETS THROUGH GROUND-UP ARCHITECTURES, MULTI-CLOUD RESILIENCE AND TRAFFIC INTELLIGENCE.

Black Hat MEA 2025 has emerged as a real-time proving ground for Saudi Arabia's rapidly advancing technology landscape.

Enterprises across Saudi Arabia are shifting from traditional on-premise models to highly distributed, multi-cloud architectures, creating new demands for visibility, encrypted traffic insights and performance-centric observability.

Danielle Kinsella, Senior Director for Sales Engineering at Gigamon, spoke to Daniel Sheperd, Online Editor, on how regional organisations are designing resilient platforms from the ground up, preparing for post-quantum security, and using traffic intelligence to accelerate digital transformation.

Interview excerpts:

Black Hat MEA has evolved into a proving ground for the region's fast-moving tech landscape. What conversations are emerging today with Saudi enterprises that weren't happening two or three years ago?

Enterprises in Saudi Arabia today are asking for real-time visibility across hybrid environments. Previously, the focus was mostly on on-premise data centre visibility. Now, as organisations transition into virtualised and cloud

environments—and increasingly into multiple cloud vendors—they need consistent and unified visibility across all these platforms. The conversations have shifted from isolated monitoring to comprehensive hybrid cloud visibility.

The region has moved rapidly from adopting cloud to managing several clouds at once. Which architecture patterns or design approaches are you seeing here that other markets are still evaluating?

We're seeing organisations in the region build far more resilient platforms. A key difference is that many Middle Eastern enterprises are designing their architectures from the ground up. In other markets, companies often rely heavily on legacy workloads and then try to shift them to the cloud, which introduces delays and complexity. The ability to start fresh is giving the region a significant advantage.

Looking ahead to 2026, how do you see observability evolving inside organisations? Is it still viewed mainly as part of security, or is it becoming essential for performance, AI workloads, and digital experience?

Visibility is becoming the backbone of organisational infrastructure. It was traditionally used for troubleshooting performance issues and addressing

security threats. Now, enterprises are using visibility to understand and secure AI workloads, both in terms of what users are doing with AI and whether those AI workloads are themselves secure. Observability is expanding well beyond security into performance optimisation and digital experience assurance.

Many organisations here are building platforms from scratch rather than upgrading legacy systems. Does this give Middle Eastern enterprises an advantage in building secure, encrypted, future-focused environments?

Beginning with clean, modern architecture is a huge advantage. In many global markets, enterprises are trying to maintain legacy environments while moving to the cloud, which slows them down. Organisations in the Middle East can design secure, encrypted, future-ready platforms from day one, and that really sets them apart.

Post-quantum computing is becoming a major topic. How can Gigamon help organisations maintain visibility in encrypted environments today and prepare for new post-quantum standards?

Many organisations already have post-quantum strategies because threat



Danielle Kinsella
Senior Director – Sales Engineering,
Gigamon

actors are harvesting data now to decrypt later. Visibility plays a key role in identifying outdated TLS versions—like TLS 1.0, 1.1 or 1.2—across workloads. If attackers obtain that data today, they may be able to decrypt it easily once post-quantum capabilities mature. Knowing exactly where those outdated encryption versions reside allows organisations to remediate and upgrade proactively.

As we move into 2026, more leaders are saying that security should support momentum rather than limit it. How are customers using traffic intelligence to speed up transformation and innovation?

Traffic intelligence is helping organisations transform faster by enabling smooth shifts from data centres to cloud environments. With

AI workloads, network traffic is increasing dramatically, and visibility allows enterprises to extract the exact data they need without overwhelming their tools. By enriching packets and outputting metadata, organisations can optimise tool performance, improve efficiency, and accelerate innovation without compromising security. 📌

SAUDI ARABIA'S CYBERSECURITY EVOLUTION ACCELERATES WITH KASPERSKY'S NEW ACADEMY AND EXPANDING MOUS

I GENERAL MANAGER MOHAMAD HASHEM OUTLINES HOW VISION 2030, DIGITAL MATURITY, AND AI ADOPTION ARE RESHAPING SECURITY PRIORITIES FOR ORGANISATIONS NATIONWIDE.

Saudi Arabia's cybersecurity landscape is advancing at an unprecedented pace, powered by Vision 2030, rapid digital transformation, and a market increasingly aware of modern cyber risks. Against this backdrop, Kaspersky continues to strengthen its footprint in the Kingdom, reporting double-digit growth and expanding its collaborations with government entities, academic institutions, and national digital upskilling programmes. With AI-driven threats becoming more sophisticated and cybercriminals leveraging the same technologies as defenders, the company is doubling down on innovation, talent development, and intelligence-led security.

Mohamad Hashem, General Manager – KSA & Bahrain at Kaspersky, spoke to Daniel Shepherd, Online Editor, about the company's 2025 performance, the evolving threat landscape, AI-powered cyber defence, and the critical steps organisations must take to stay resilient in an increasingly complex digital environment.

Interview excerpts:

How much growth has Kaspersky achieved in Saudi Arabia this year, and what factors are driving this performance?

We have recorded steady year-on-year growth, and for the first three quarters of 2025 alone, we have already achieved 12% YoY growth, with this number

expected to rise by the end of December. This momentum is driven by the strength of our products and services, as well as the maturity of the Saudi market, where organisations can clearly differentiate between cybersecurity offerings.

What are the most significant cyberthreats Kaspersky has blocked in the Kingdom and the wider GCC region in 2025?

Kaspersky detects over 15 million cyberthreats every day, including around 500,000 newly identified malicious files. Among the most common threats we see are backdoors, password stealers, and ransomware. Ransomware attacks, in particular, have grown more sophisticated, often executed by highly prepared and well-funded groups. Thankfully, our technologies enable us to detect and block millions of threats daily, keeping customers across the Kingdom and the GCC protected.

Are you planning to sign any new MoUs or strategic partnerships in Saudi Arabia, particularly with government entities or educational institutions?

We have recently signed an MoU with Monsha'at, the government body supporting SMEs, making our solutions more accessible to smaller organisations. We have also partnered with several respected Saudi universities to train students in cybersecurity. In addition, I am pleased to announce our collaboration with Tuwaiq Academy to establish the Kaspersky Academy

in Saudi Arabia, helping advance Vision 2030's goals for secure digital transformation and building a strong cybersecurity talent pipeline.

How is Kaspersky leveraging artificial intelligence to detect and respond to increasingly sophisticated cyberattacks?

AI has been part of Kaspersky's technology stack since 2008, well before today's AI evolution. With more than 15 million threats detected daily, AI is essential in our detection engine. Cybercriminals are also using AI to enhance their attacks and make them more realistic. To counter this, we continuously evolve our AI capabilities to defend against AI-driven threats effectively.

Given the surge in AI-powered cyberattacks predicted by IT specialists, how is Kaspersky preparing the Kingdom's workforce and businesses for the next generation of threats?

AI is an indispensable tool across industries today, but it is also used by cybercriminals. For example, AI can replicate legitimate websites within minutes to carry out highly convincing phishing attacks. Kaspersky helps organisations by distinguishing between legitimate and fake sites through our threat intelligence and extensive global database. Our academic partnerships and the newly announced Kaspersky Academy will equip Saudi students and



Mohamad Hashem
General Manager – KSA & Bahrain,
Kaspersky.

professionals with the skills needed to combat next-generation threats.

If you were to give one piece of advice to Saudi organisations looking to strengthen their cybersecurity posture

in 2025, what would it be?

AI systems themselves can be manipulated, attackers can tamper with datasets or libraries to influence outputs. Before adopting AI at scale, organisations must ensure their infrastructure is

properly secured. I strongly advise investing in strong cybersecurity solutions and conducting compromise assessments and penetration testing to uncover hidden vulnerabilities before deploying AI-driven tools. 🛡️

GCC ENTERPRISES BOOST SECURITY READINESS FOR POST-QUANTUM FUTURE, SAYS QUANTUMGATE

QUANTUMGATE'S EIBRAHYM SULTAN OUTLINES HOW QUANTUM THREATS, AI-DRIVEN ATTACKS, AND RISING REGULATORY PRESSURE ARE TRANSFORMING CYBERSECURITY STRATEGIES ACROSS THE UAE AND SAUDI ARABIA.

Enterprises in the UAE and Saudi Arabia are now confronting a dual challenge: preparing for future quantum decryption threats while also keeping pace with AI-powered attacks that are reshaping adversarial behaviour at unprecedented speed. This shift is compelling organisations to re-evaluate how they protect long-lived data, secure their cryptographic foundations, and strengthen their resilience strategies.

Eibrahym Sultan, Director of Growth at QuantumGate, spoke to Daniel Shepherd, Online Editor, about why the region must accelerate its post-quantum cryptography (PQC) migration, the impact of "harvest-now, decrypt-later" threats, and the growing expectation for identity-first and crypto-agile security models. Sultan highlights the critical interplay between visibility, readiness, and innovation at a time when both quantum and AI-driven adversaries are advancing rapidly.

Interview excerpts:

With BlackHat MEA 2025 becoming a key platform for security innovation, what key insights or announcements will QuantumGate be highlighting during the event?

A core focus for us this year is education—helping the market understand the urgency and practical steps of the post-quantum cryptography (PQC) migration journey. Around the world, and increasingly across the GCC, governments are issuing directives that require organisations in government, semi-government and critical private-



Eibrahym Sultan
Director of Growth at
QuantumGate.

sector industries to begin transitioning their cryptographic systems. At Black Hat, we are highlighting why this migration is essential, how organisations should structure it, and how QuantumGate's tools support each stage of the transition. Our aim is to demystify PQC for the region and give enterprises clarity on enabling a secure, compliant, future-ready cryptographic environment.

What emerging cybersecurity trends do you see shaping enterprise security strategies across Saudi Arabia and the wider GCC?

One of the strongest trends we're seeing is the rising recognition of quantum-enabled threats. The global acceleration in quantum computing, driven by large players and major research groups, means organisations are now seriously considering the real-world consequences. There is consensus that once practical quantum computers emerge, they will be capable of breaking today's widely used public-key cryptography. Enterprises in Saudi Arabia and the GCC are therefore reassessing their long-term data protection strategies. This is exactly where QuantumGate's portfolio becomes relevant: we provide the tools that allow organisations to understand and map their cryptographic assets, identify risks, and start preparing for a quantum-resilient future today.

The shift toward post-quantum security is gaining urgency globally. Why do you believe Middle East enterprises must begin their migration now, and what risks do they face if they delay?

Two forces make early migration non-negotiable: first, the rapid rise in sensitive data and second, the emergence of "harvest-now, decrypt-later" attacks. Over the past decade, organisations have accumulated unprecedented amounts of data with long confidentiality requirements—

medical records, banking information, citizen data and other critical assets. This data must remain secure not only today, but decades into the future. Threat actors are already harvesting encrypted data now, with the intention of decrypting it once quantum computers mature. Even if the data cannot be exploited today, a future breach could have enormous consequences. That is why waiting five or ten years is not an option. Enterprises must act now to ensure their data cannot be retroactively compromised.

AI-powered attacks are evolving rapidly. How is this transformation redefining threat landscapes and influencing how CISOs prioritise investments in resilience?

AI is fundamentally reshaping adversarial behaviour. Attacks have become more dynamic, automated and sophisticated. As a result, CISOs are being forced to rethink both their budgets and strategy.

Several priorities are emerging:

- Identity-first security frameworks are becoming essential.
- Strong authentication and zero-trust models are now baseline requirements.
- Crypto resilience and crypto agility are gaining urgency because the underlying cryptographic primitives must adapt as threats evolve.
- Continuous validation and discovery across the security estate is increasingly critical.
- Long-term data security is becoming top-of-mind, especially as AI accelerates attacks on identity, data and critical infrastructure.

What role does QuantumGate play in helping organisations future-proof their cybersecurity architectures—particularly as quantum threats and AI-driven adversaries converge?

QuantumGate delivers a comprehensive suite

of products designed to help enterprises future-proof their entire cryptographic environment and security foundations. We cover both post-quantum protection and broader enterprise security needs.

Our portfolio spans five major areas:

- **Cryptographic asset discovery and inventory**

Most enterprises only understand 20–30% of their cryptographic footprint. Our discovery tool generates a full cryptographic bill of materials, highlighting vulnerabilities, deprecated algorithms, weak keys, and expired certificates. This is the foundation for any PQC migration strategy.

- **QSphere -Quantum-resistant VPN**

A next-generation VPN that integrates quantum-safe encryption to protect data in transit today while preparing for future quantum decryption risks.

- **QSphere- Quantum-resistant data encryption**

A cryptography platform that encrypts, signs, and verifies data to ensure confidentiality, integrity, and authenticity across files, email, and messaging. It protects data at rest and in transit using both classical and post-quantum encryption.

- **Salina- Passwordless, password-free access**

Salina delivers passwordless access for users while integrating with legacy systems. It removes passwords from the login experience and automates password management, reducing phishing and credential-related risks.

- **Secure VMI – Virtual MobileInfrastructure**

A secure, isolated mobile workspace that runs alongside the user's personal environment. It keeps corporate data and applications fully separated and protected with enterprise-grade controls. If a device is lost or compromised, the work instance can be locked, wiped or redeployed immediately.

Together, these solutions allow organisations to build a security architecture capable of resisting both quantum and AI-driven adversaries—protecting their data, identities, and infrastructure well into the future. 🚀

→ **THE THREAT LANDSCAPE IS MOVING FAST—AND CISOs MUST ENSURE THEIR ORGANISATIONS CAN ADAPT JUST AS QUICKLY.**

STARLINK SHARPENS AI-FIRST CYBERSECURITY VISION TO POWER KSA'S NEXT DECADE OF GROWTH

COO AHMED DIAB OUTLINES HOW DEEPER LOCAL INVESTMENT, AGENTIC AUTOMATION, AND VERTICAL-READY SOLUTIONS ARE POSITIONING STARLINK AT THE FOREFRONT OF THE KINGDOM'S CYBER RESILIENCE JOURNEY.



ALL OUR SOLUTIONS NOW MAP TO THESE PRACTICES, ENSURING WE STAY IN SYNC WITH SAUDI ARABIA'S FAST-MOVING TECHNOLOGY LANDSCAPE AND ACROSS MEA AS WELL.

Saudi Arabia's cybersecurity landscape is entering a defining phase, driven by rapid AI adoption, expanding digital infrastructure, and evolving regulatory frameworks across critical industries. Organisations are accelerating cloud transformation, building secure-by-design platforms, and preparing for AI-driven threats, which is creating unprecedented demand for integrated and adaptive security strategies.

Ahmed Diab, Chief Operating Officer at StarLink, spoke to Daniel Shepherd, Online Editor, about how the company is deepening its investment in the Kingdom, reshaping its operating model, and supporting enterprises with AI-enabled resilience, vertical-tailored solutions, and close alignment with national priorities.

Interview excerpts:

How is StarLink adapting its regional strategy to support Saudi enterprises as AI adoption accelerates and new cyber risks emerge?

We continuously evolve our go-to-market approach to align with each country's needs, and Saudi Arabia is our number one focus and the largest market in the region. This year, we introduced a five-year vision under the name StarLink 5.0 that is fully aligned with Saudi Arabia's national digital and cybersecurity directions. To support this, we have restructured our offerings into five core practices that reflect the Kingdom's priorities:

1. Cyber Resilience
2. Cloud Transformation
3. Agentic Automation
4. Enterprise AI
5. Digital Infrastructure

"All our solutions now map to these practices, ensuring we stay in sync with Saudi Arabia's fast-moving technology landscape and across MEA as well."

What key operational priorities are

driving StarLink's growth in 2025, especially in high-demand markets like Saudi Arabia?

Our top priority is local investment. At Black Hat MEA 2025, we marked the grand opening of our new Saudi office, where we now have more than 110 employees. We aim to double our investment and workforce in the next three to five years. Operationally, we are transforming our entire ecosystem through platformisation—bringing all communication channels and service touchpoints onto one automated, intelligent platform. Our customers, partners and vendors will be assisted by a unified, automated digital platform supported by intelligent workflows and AI agents. This shift enables us to operate 24/7/365, scale efficiently, and deliver seamless, consistent service across the region.

How is StarLink helping organisations move toward predictive, AI-enabled cyber resilience, and what differentiates your approach from traditional integrators?

We act as client zero for the technologies we promote. Before offering AI-driven or agentic cybersecurity capabilities to partners and customers, we implement them internally across our sales operations and service workflows. Today, agentic AI is embedded across StarLink's internal operations, powering automation, decision-making, and service delivery. This real-world use allows us to build practical use cases for our partners and guide them on how to adopt and operationalise advanced AI technologies. What differentiates us is this practical-first approach—we use it, refine it, and then help our partners apply it to their customers, ensuring the transition to predictive cyber resilience grounded in proven operational experience.

How are you working with global

technology partners to keep their solutions aligned with Saudi regulations such as NCA ECC, PDPL, and the requirements of mega-projects?

We have direct, constant engagement with Saudi customers, and we understand the regulatory environment and industry needs very deeply. We have built six vertical-focused solution frameworks, including Public Sector, BFSI, Energy & Oil and Gas, Telco, Healthcare, and Education. Each vertical has its own compliance requirements, regulatory expectations, and market-specific needs. We ensure that every solution we design or bring to market adheres to those requirements so that our global partners can directly benefit from a framework already aligned with the necessary regulations. This verticalisation ensures partners enter the market with solutions that are pre-aligned with NCA ECC, PDPL, and mega-project mandates.

What outcomes is StarLink aiming for at Black Hat MEA 2025, and how does the event strengthen your engagement with customers and government stakeholders in the Kingdom?

Black Hat MEA is one of the most important events for us, and we have participated every year since it began. Our goals here are twofold:

1. Showcase our solutions and services to partners and customers
 2. Listen closely to the market
- Beyond presenting our capabilities, we use the event to understand customer challenges, partner expectations, and vendor priorities. Saudi Arabia is developing at an extraordinary speed, and Black Hat helps us stay deeply connected to the market's pulse.

The event gives us the opportunity to engage directly with customers, partners, and government entities, ensuring we evolve with the Kingdom's momentum and support its ambition to be a global cybersecurity leader. 🔑

VEEAM POSITIONS TRUSTED DATA AS FOUNDATION FOR SCALING SAFE AI, SAYS

I CEO ANAND ESWARAN EXPLAINS HOW THE ACQUISITION OF SECURITI AI UNIFIES DATA RESILIENCE, SECURITY, GOVERNANCE, AND AI TRUST TO HELP ENTERPRISES MOVE AI FROM EXPERIMENTATION TO PRODUCTION WITH CONFIDENCE

Enterprises accelerating AI adoption are discovering that the biggest barrier to success is no longer models or infrastructure, but whether data can be trusted, governed, secured, and recovered at machine speed.

Anand Eswaran, CEO of Veeam, spoke to Sandhya D'Mello, Technology Editor, Security Advisor Middle East, about the strategic rationale behind the company's landmark acquisition of Securiti AI.

The interview explores how unifying data resilience with security, privacy, governance, and AI trust creates a foundational platform for scaling safe AI, why fragmented data tools are no longer viable in an AI-driven world, and how the combined Veeam–Securiti AI platform is reshaping global data resilience strategies.

Eswaran also highlights why the UAE's digital-first vision and strong regulatory focus make the region a strategic priority

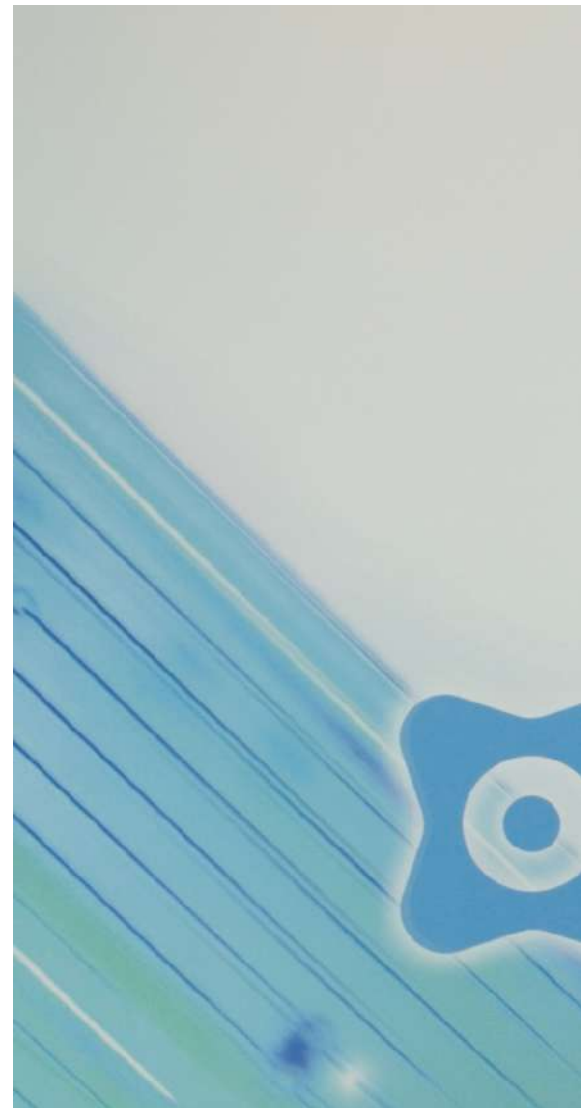
for Veeam's next phase of growth, as organisations seek to innovate confidently while meeting evolving requirements around data sovereignty, compliance, and AI ethics.

Interview excerpts:

Why was this the right moment for Veeam to acquire Securiti AI?

AI has fundamentally changed how organisations consume, move, and monetise data. Customers today operate multiple disconnected tools—one set for analytics and intelligence, another for security, privacy, compliance, and governance, and a separate layer for data protection and resilience. This fragmentation no longer works in an AI-driven world.

The speed at which AI operates means humans cannot manually orchestrate these layers safely. The industry needed to step back and rethink how data is managed end-to-end. This acquisition allows Veeam to bring together data



understanding, security, privacy, governance, and resilience into a single unified platform. The timing is critical because enterprises are scaling AI now—and without this foundation, most AI projects fail before reaching production.

How will the combined platform accelerate safe and trusted AI adoption?

Today, most AI projects fail not because of models or infrastructure, but because data is not secured, governed, or exposed correctly. With the combined platform, AI initiatives can move from idea to pilot to production in weeks rather than months. When we say “safe AI,” we mean two things coming together: data security and data resilience. There is no

The Veeam logo is displayed in white lowercase letters on a green rectangular background.

**THERE IS NO AI
WITHOUT DATA
SECURITY, AND
THERE IS NO TRUST
IN AI WITHOUT DATA
RESILIENCE.**



AI without data security, and there is no trust in AI without data resilience. The platform provides deep visibility across primary and backup data, structured and unstructured data, enabling organisations to understand lineage, risk, and exposure. This ensures the right data feeds AI pipelines—preventing hallucinations, data leakage, and compliance violations—while allowing rapid, confident innovation.

How will this acquisition reshape Veeam’s global data resilience strategy in the coming years?

Veeam has long been the global leader in data resilience. This acquisition elevates our role from protecting data to enabling

trusted AI outcomes. We are evolving into a data and AI trust company. Our strategy now spans the entire data lifecycle—from creation and classification to protection, recovery, and AI consumption. By unifying resilience with security, privacy, compliance, and governance, we are redefining what resilience means in the AI era. It is no longer just about recovery after an incident, but about ensuring data is always trusted, compliant, and ready to fuel AI-driven transformation at scale.

With the UAE shaping itself as a “digital-first” nation, how is Veeam aligning its vision to expand its regional presence?

The Middle East, and particularly the UAE, is one of Veeam’s most strategic

regions. What stands out is the region’s ability to balance innovation with strong regulatory frameworks. Initiatives around data protection, AI ethics, governance, and sovereignty are progressing in parallel with aggressive digital transformation agendas. Veeam’s unified platform aligns directly with this vision. We abstract the complexity of compliance and data sovereignty across jurisdictions, allowing organisations to innovate without worrying about regulatory risk. This enables enterprises, governments, and cities to focus on leveraging AI safely and responsibly. We are investing heavily in the region and are excited to partner with public and private sector organisations to support the UAE’s digital-first ambitions. 📍

AI AGENTS, MACHINE IDENTITIES TO RESHAPE BOARDROOM CYBERSECURITY PRIORITIES

KEVIN BOCEK, SENIOR VICE PRESIDENT OF INNOVATION AT CYBERARK, EXPLAINS WHY IDENTITY SECURITY WILL DEFINE GOVERNANCE, RESILIENCE AND DIGITAL TRUST IN 2026 AS AI AGENTS AND AUTOMATION RESHAPE CORPORATE DECISION-MAKING IN THE GULF AND BEYOND.

Organisations across the Gulf are accelerating AI adoption and automation, making identity security the defining control plane for digital trust. Kevin Bocek, Senior Vice-President of Innovation at CyberArk, spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, on how AI agents, machine identities, and board-level governance could reshape cybersecurity priorities by 2026.

From the potential role of AI agents in corporate decision-making to the growing risk of runaway automation, Bocek explains why identity — both human and non-human — now sits at the core of resilience, accountability, and fiduciary responsibility.

Bocek also outlines the priorities CISOs and boards must address today to secure machine identities at scale, as cloud, AI and autonomous systems transform the Gulf's digital ecosystems.

Interview excerpts:

You've predicted that shareholders may soon appoint AI agents to corporate boards — what signals make this shift realistic for 2026, and what governance risks does it introduce?

The prospect of AI agents joining corporate boards by 2026 is becoming realistic due to two factors: the rise of autonomous AI agents capable of reasoning and acting independently, and

their deep integration into corporate data streams. These agents can already analyse complex financial and legal information, producing auditable insights faster than human teams. This creates opportunities for shareholders to use AI to drive more data-driven, transparent governance. However, AI board agents also introduce significant risks, particularly around legal accountability, fiduciary duty and data security. Questions remain over liability when AI-driven decisions cause losses, while granting agents access to highly sensitive board data increases insider risk and makes strong machine identity management and access controls essential.

What cybersecurity trends or threat patterns do you expect will define 2026 as AI-driven automation accelerates?

Machine identity threats will accelerate as automation expands, driven by the explosive growth of non-human credentials such as certificates and API keys. Organisations now manage 82 machine identities for every human, yet many remain poorly governed, with privileged access often overlooked. The issue will peak in 2026 when Microsoft, Google, and Apple shorten TLS certificate lifespans, triggering widespread outages as mismanaged certificates expire and critical systems go offline. At the same time, AI will

further expand the attack surface, particularly through the rise of "runaway" AI agents. Poorly secured agents, misconfigured identities, or leaked API keys could enable a single rogue agent to spread rapidly across systems. The defining security challenge will be ensuring every AI agent has a unique, revocable identity, making identity governance the only true kill switch in an automated world.

How will board expectations of CISOs evolve next year as identity-centric attacks and machine-led decision-making increase?

Boards will increasingly see the CISO as a strategic risk advisor, not just a compliance leader, responsible for safeguarding digital trust. As identity-centric attacks grow, security focus is shifting from the perimeter to protecting every human and machine identity. CISOs are already warning boards about unavoidable third-party risks, such as the TLS certificate mandates from Google, Apple, and Microsoft, where a single failure can disrupt operations and damage brand value. The rise of AI agents further elevates governance expectations. CISOs will be held accountable for proving that machine and AI identities are properly governed under a zero-trust model, with secure access to all corporate secrets becoming a core board-level

Kevin Bocek
Senior Vice President of
Innovation, CyberArk.

→ **THE MOST SIGNIFICANT SECURITY THREAT IS A 'RUNAWAY AGENT' EXECUTING UNAUTHORISED WORK ACROSS INTERCOMMUNICATING WORKFLOWS.**

responsibility.

What must Gulf organisations prioritise today to secure machine identities at scale as they expand AI, cloud, and automation initiatives?

Gulf organisations must prioritise securing machine identities, which underpin AI, cloud and automation growth. This starts with strong secrets management to eliminate static credentials and automate the rotation of short-lived keys and tokens across multi-cloud and on-premise environments. A zero-trust approach is essential, assuming

breach by default and granting access based on verified machine identity, context and least privilege, with no standing access to critical systems. Centralised visibility and governance over all machine identities are also critical to maintain compliance, resilience and security at the speed of modern automation.

How can the Gulf enable aggressive AI innovation while ensuring identity security remains uncompromised across digital ecosystems?

To accelerate AI innovation securely, Gulf organisations must embrace a machine identity-first strategy. Since AI models and automated systems are driven entirely by non-human credentials, security must be built into the CI/CD pipeline. This involves implementing automated secrets management for all service accounts used by AI and ML workloads. This security automation will help ensure that aggressive digital expansion does not compromise identity security across AI, multi-cloud and hybrid environments. **1**

PHISHING EVOLVES INTO SCALABLE CYBERCRIME BUSINESS, SAYS RO'YA HATAMLEH

RO'YA HATAMLEH OF MICROSOFT EXPLAINS HOW PHISHING-AS-A-SERVICE OPERATIONS LIKE RACCOON0365 ARE SCALING GLOBALLY, WHY CLOUD-FIRST REGIONS SUCH AS THE MIDDLE EAST FACE HEIGHTENED RISK, AND HOW ORGANISATIONS CAN COUNTER AI-DRIVEN ATTACKS THROUGH IDENTITY SECURITY AND ZERO TRUST.



Ro'ya Hatamleh
Security Cloud Commercial
Solutions, EMEA HQ - Middle
East and Africa - Microsoft

Phishing has evolved from opportunistic scams into a highly industrialised cybercrime model, driven by automation, artificial intelligence, and subscription-based criminal services. One of the most prominent examples is Raccoon0365, a phishing-as-a-service (PhaaS) operation that enabled large-scale credential theft across nearly 100 countries by lowering the technical barriers for cybercriminals. Microsoft recently led a coordinated global takedown of Raccoon0365, seizing hundreds of domains and disrupting its infrastructure. The operation highlights both the growing sophistication of phishing campaigns and the importance of intelligence-led, collaborative defence in combating cybercrime at scale.

Ro'ya Hatamleh, Security Cloud Commercial Solutions, EMEA HQ – Middle East and Africa at Microsoft, spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, about how the PhaaS model works, why cloud-first regions such as the Middle East face heightened risk, and how organisations

can defend themselves against AI-driven phishing through strong identity security, Zero Trust principles, and continuous awareness.

Interview excerpts:

How does the phishing-as-a-service model like Raccoon0365 work, and why is it so powerful?

Raccoon0365 is a prime example of phishing-as-a-service (PhaaS), essentially a criminal subscription model. Even attackers with minimal technical skills can run large-scale phishing campaigns simply by paying a subscription fee. Once subscribed, they gain access to ready-made tools, templates, and email kits that mimic Microsoft 365 login pages, complete with convincing branding.

What makes it powerful are three key points:

- Scalability & Automation: Our investigation showed that Raccoon0365 could target up to 9,000 email addresses per day. Since July 2024, it was used to steal over 5,000 user credentials across 94 countries.
- Low Barrier to Entry: Cybercrime-in-a-box, anyone can use it without maintaining infrastructure.
- Continuous Evolution: Like a legitimate SaaS business, it offers updates and new features. For example, it recently introduced "AI Mail Chick", an AI-powered tool that generates more convincing phishing emails.

While many organisations were able to mitigate the impact through multi-factor authentication and other safeguards, the

sheer scale of credential theft highlights how far automation has transformed phishing. This industrialised approach has made phishing campaigns faster, broader, and more efficient, turning what used to be manual, small-scale attacks into operations that resemble high-volume marketing campaigns.

What truly sets Raccoon0365 apart, however, is its commercialisation and profit motive. It was operated as a full-fledged business within criminal ecosystems, marketed openly across Telegram channels and underground forums to attract a paying customer base of other cybercriminals. By the time of its takedown, the group had over 850 members on Telegram and had received at least US \$100,000 in cryptocurrency payments from subscriptions. Microsoft's Digital Crimes Unit (DCU) seized 338 domains, took down Raccoon0365's infrastructure, and identified its Nigeria-based operator for law enforcement. The action shows that while PhaaS fuels cybercrime-as-a-business, Microsoft's intelligence and legal reach are reshaping the fight against it.

How vulnerable are enterprises and healthcare organisations in the Middle East?

The Middle East has embraced cloud services as a central element of digital transformation. According to a PWC Research, 68% of organisations in the region plan to migrate the majority of their operations to the cloud within the next two years, and many are evolving beyond basic lift-and-shift to modernise into cloud-native or hybrid architectures.

This rapid shift makes the region more

attractive to cyber attackers, especially in high-stakes sectors like healthcare, finance, and government, which are often targeted for credential theft.

For example, if a hospital employee's credentials are phished, attackers could gain access to confidential patient records or disrupt vital systems, potentially leading to serious operational and data breaches. While vulnerability is inevitable, it does not imply defenseless. Microsoft continues to invest in advanced security capabilities, and regional organisations show signs of being proactive. For instance, the 2025 PwC Digital Trust Insights report states that only 24% of respondents in the Middle East felt they were least prepared to address cloud-related threats over the next year, compared to 34% globally. Still, no region or industry is entirely immune to phishing. The human element remains the weakest link, even skilled professionals can be deceived by a convincing email, whether they're in Dubai or London. The real threat lies not in the cloud itself, but in attackers exploiting weak credentials through phishing and social engineering. As digital transformation accelerates, identity has become the new security perimeter. Without consistent enforcement of multi-factor authentication (MFA), stolen credentials can enable attackers to impersonate legitimate users and bypass traditional defenses.

How can organisations defend against AI-driven phishing?

The simple rule is that you can't fight AI-powered attacks without AI-powered defense. At Microsoft, AI is embedded across the entire security stack. Microsoft Threat Intelligence now processes 84 trillion signals per day, revealing the exponential growth in cyberattacks, including 7,000 password attacks per second, enabling Defender, Sentinel, and Security Copilot to detect and block phishing attempts at scale. This intelligence is shared globally, so

DEFENDING AGAINST AI-DRIVEN PHISHING REQUIRES A HOLISTIC APPROACH, COMBINING INTELLIGENT TECHNOLOGY, STRONG IDENTITY PROTECTION, AND ONGOING HUMAN AWARENESS TO STAY AHEAD OF INCREASINGLY SOPHISTICATED ATTACKS.

if a suspicious IP address is flagged in one part of the world, protections are cascaded across products to safeguard customers everywhere.

However, technology alone is not enough. Strengthening identity and access protections is equally vital. Even the most convincing AI-generated phishing email can be neutralized with robust identity security, enforcing Multi-Factor Authentication (MFA) for all users and adopting phishing-resistant MFA (PRMFA). Conditional Access policies and risk-based sign-in detection add further layers of AI-driven defense, automatically flagging or blocking anomalous logins, such as impossible travel, unfamiliar devices, or unusual access patterns.

Across the Middle East, many organisations are also adopting a Zero Trust approach, a security model built on the principle of “never trust, always verify.” By assuming every user, device, or link could be malicious until verified, and continuously validating signals and identities, companies significantly reduce the chances of an AI-augmented phishing attack succeeding.

The human element remains critical, Microsoft helps organisations strengthen this layer through phishing education and simulation tools. We actively partner with government agencies and enterprises across the region to run awareness workshops, webinars, and public campaigns, including the annual Cybersecurity Awareness Month toolkit that provides internal resources like posters, slide decks, and short videos.

Ultimately, defending against AI-driven phishing requires a holistic approach, combining intelligent technology, strong identity protection, and ongoing human awareness to stay ahead of increasingly sophisticated attacks.

What are the biggest misconceptions about phishing risks?

A common misconception is that only naive individuals fall for phishing attempts. In reality, even seasoned professionals, including security experts, can be deceived



by today's AI-powered spear phishing. Another misconception is that phishing is an outdated or low-level threat. This is far from true, phishing remains the number one entry point for attackers worldwide, providing direct access to sensitive credentials and, ultimately, the “crown jewels” of an organisation. It is also often assumed that basic protections such as multi-factor authentication are sufficient. While MFA is critical, it is not foolproof, and continuous innovation is required, such as anomaly detection that can flag suspicious logins from unusual locations. Phishing continues to evolve rapidly, and Microsoft adapts in parallel by integrating AI-driven identity protections to ensure defenses remain ahead of attackers.

What long-term strategies is Microsoft pursuing globally?

Microsoft views the fight against phishing as part of a wider battle against cybercrime. One of its key strategies is Continuous Technical and Legal Disruption: in the recent Raccoon0365 case, Microsoft's Digital Crimes Unit seized 338 domains, disabling the phishing network, and coordinated with Cloudflare to suspend infrastructure and ban domains. The takedown also involved tracing cryptocurrency flows via

Chainalysis to help link operators to the attacks.

For lasting impact, Microsoft continues to invest in next-generation investigative capabilities, including blockchain analytics, AI-driven threat intelligence, and cloud-scale forensics, to stay ahead of evolving criminal tactics and strengthen the global fight against cyber-enabled crime.

The principle of collective defense is also central: Microsoft engages with partners, governments, and trusted third parties. In the Raccoon0365 operation, it worked directly with Cloudflare. More broadly, Microsoft operates the Government Security Program (GSP), which grants governments access to threat intelligence, code transparency, and coordinated security exchange.

Microsoft also emphasises security by design and continuous innovation. Its approach is to embed intelligence and protection capabilities into its core security products, including integrating threat signals across Defender, Sentinel, and other tools. Finally, Microsoft promotes cybersecurity awareness as a foundational element. Through resources like the Be Cyber Smart Kit, the company helps organisations educate personnel on phishing risks, identity protection, and good security habits worldwide. 📌

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT



SCAN HERE



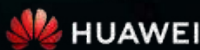
ENQUIRE FOR
 2026!

#giseccglobal
 gisec@dwtc.com

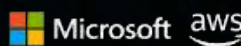
OFFICIAL DISTRIBUTION PARTNER



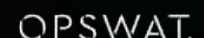
LEAD STRATEGIC PARTNER



STRATEGIC PARTNER



DIAMOND SPONSOR



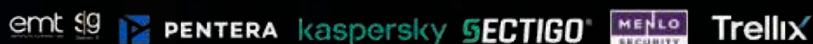
PLATINUM SPONSOR



GOLD SPONSOR



GOLD SPONSOR



PHYSICAL SECURITY EMERGES AS STRATEGIC ENTERPRISE FUNCTION, SAYS GENETEC 2026 REPORT

Genetec Inc. (Genetec), the global leader in enterprise physical security software, today released its sixth annual State of Physical Security report. Based on insights from over 7,300 physical security leaders worldwide (including end users, channel partners, systems integrators, and consultants), the report shows that physical security is playing a broader strategic role within organisations. The findings highlight closer collaboration across departments and greater interest in technologies that support better operational awareness and decision-making.

Physical security is evolving from protection to empowering business outcomes

The report shows a shift in how physical security systems are deployed and valued. They are no longer viewed only as a protection layer, and instead, are becoming an enterprise function that contributes to broader organisational goals.

“As it becomes more tightly woven into the broader fabric of the enterprise, security is emerging as a genuine enabler of business outcomes—helping organisations work more cohesively, respond more effectively, and stay focused on long-term goals,” said Christian Morin, Vice President of Product Engineering at Genetec Inc.

- Physical security has evolved into a strategic business function, strengthening IT collaboration and decision-making
- Interest in adopting AI more than doubled among end users since last year
- Organisations want flexibility to deploy workloads on premises, in the cloud, or in a hybrid model

Modernisation is accelerating as demand for unified systems grows

Survey findings indicate that organisations are prioritising modernisation of their physical security systems to support this shift toward stronger collaboration and business decision-making. More than 70% of respondents are using unified or integrated systems, and 60% say their main motivation for replacing legacy technology is to integrate new capabilities. Fifty-one percent cite access to new features as another key driver. These trends reflect a growing interest in cross-functional systems that deliver operational insight and help teams achieve more with their existing investments.

Long-term vendor stability is becoming a key selection factor

Survey findings show that organisations place strong importance on choosing manufacturers they consider stable and

trustworthy. Seventy-three percent of end users say the long-term viability and stability of the vendor is a key factor when evaluating solutions, while product performance and price indicators followed behind, ranked at 45% and 43%, respectively. This points to a clear preference for partners who can provide continuity, support multi-year modernisation efforts, and deliver reliable product development as systems evolve.

Interest in AI is rising but teams want practical benefits

AI is an area of growing focus. For the first time, AI ranked alongside access control and video surveillance as a top project priority for 2026. Interest in adopting AI has more than doubled among end users since last year's report. They see value in technology that helps navigate alarms, support investigations, and reduce noise in busy environments. At the same time, 70% express concerns about how AI systems are designed and implemented, specifically around data use and understanding how AI works, reinforcing the need for clear guidance from vendors.

Hybrid cloud is preferred, and defines the future of security infrastructure

Cloud is playing a stronger role in how security infrastructure is designed and maintained. End users identify automatic updates, ease of deployment, and

Modernization is accelerating as demand for unified systems grows



More than
70%

of respondents
are using unified or
integrated systems



60%

say their main motivation
for replacing legacy
technology is to integrate
new capabilities



51%

cite access to
new features as
another motivation

GenetecTM

[genetec.com/soti26](https://www.genetec.com/soti26)

simpler maintenance as key benefits. Respondents expect continued cloud adoption in 2026, supported by the flexibility to choose which workloads remain on premises and which move to the cloud.

2026 Forecast

The report also provides insights into priorities for 2026, including access control modernisation, cybersecurity initiatives, and the growing use of analytics. It also offers regional findings

and additional forecasts to help organisations plan their next steps. For more information and to download the 2026 State of Physical Security report, please go to <https://www.genetec.com/a/physical-security-report>.

AS IT BECOMES MORE TIGHTLY WOVEN INTO THE BROADER FABRIC OF THE ENTERPRISE, SECURITY IS EMERGING AS A GENUINE ENABLER OF BUSINESS OUTCOMES—HELPING ORGANISATIONS WORK MORE COHESIVELY, RESPOND MORE EFFECTIVELY, AND STAY FOCUSED ON LONG-TERM GOALS, SAID CHRISTIAN MORIN, VICE PRESIDENT OF PRODUCT ENGINEERING AT GENETEC INC.

Survey methodology

The report is based on survey responses from 7,368 physical security professionals across six global regions (USA and Canada; Latin America and the Caribbean; Europe; Asia-Pacific; Middle East and Africa; and Australia and New Zealand). Participants included end users, channel partners, consultants, and manufacturers from organisations of all sizes and industries. The survey was conducted between August 18 and September 15, 2025, and only fully completed responses were included in the analysis. 📌



Jay Reddy
Head of Growth,
ManageEngine

REDEFINING TRUST: WHY CREDENTIALS, NOT PASSWORDS, WILL SECURE ENTERPRISE

CRYPTOGRAPHIC, SYSTEM-GOVERNED CREDENTIALS ARE BECOMING THE ONLY SCALABLE FOUNDATION FOR ZERO TRUST SECURITY BEYOND PASSWORDS.

A survey found that 87% of IT professionals believe moving to passwordless authentication is essential for improving security. Yet 56% of organisations still rely on SMS-based one-time passcodes (OTPs) for logins, a method that still depends on passwords and is vulnerable to SIM-swapping and phishing attacks. This contradiction isn't just ironic; it's risky—and it exists in the gap between intent and implementation. Most IT teams understand the need for stronger authentication, but many remain tied to legacy systems that keep them exposed. Modern infrastructures are evolving faster than the authentication models that protect them, and attackers have long mastered exploiting user-managed secrets.

For years, the IT industry has agreed that passwords are obsolete, yet only a

few organisations have taken decisive action to move beyond them. Enterprises have upgraded interfaces and layered in new controls, but the foundation—static, human-managed authentication—has largely remained untouched.

The UAE's decision to phase out OTPs by 2026 will accelerate the change to passwordless methods. By mandating the adoption of advanced authentication methods such as Emirates Face Recognition, biometric verification, and mobile-based soft tokens, the Central Bank of the UAE (CBUAE) is accelerating a transformation that much of the world has been too cautious to take on.

The UAE is forcing a long-overdue conversation: trust cannot depend on something users remember or receive, it must be something systems can prove.

This shift will expose just how much password dependence truly costs enterprises today, not only in terms

of security risk but also in everyday operations and user behaviour.

Hidden operational and behavioural costs

Password dependence is not merely inefficient, it's corrosive. IT teams are bogged down by constant reset requests. Users are forced to juggle multiple credentials, leading to reuse, insecure storage, and informal sharing. These aren't edge cases, they're symptoms of a flawed model.

Employees, overwhelmed by the number of credentials they must manage, begin using unsafe work-arounds such as reusing passwords, storing them in insecure locations, or delegating access informally. Every work-around reflects a breakdown in the authentication model. Worse, fallback flows like email or SMS resets are rarely monitored or logged, quietly introduce compliance gaps. In highly regulated environments, these blind spots translate to audit failures and avoidable exposure. And this isn't limited to one industry:

- In financial services, password friction increases fraud risks and impacts the customer experience.
- In healthcare, shared workstations

ENTERPRISES HAVE UPGRADED INTERFACES AND LAYERED IN NEW CONTROLS, BUT THE FOUNDATION—STATIC, HUMAN-MANAGED AUTHENTICATION—HAS LARGELY REMAINED UNTOUCHED.

in critical care environments create security gaps.

- In manufacturing, password hygiene suffers under shift-based identity management and operational technology system access.

According to the FIDO Alliance's 2025 passkey adoption study, 35% of global users reported account compromises in the last year due to password vulnerabilities.

Passwordless programs stall after the pilot phase

Security leaders generally agree: Passwords are a liability. The real problem is in the rollout. IAM teams may be ready for passwordless methods, but endpoint, compliance, and application teams often aren't aligned.

Even when organisations aim to go fully passwordless, they often face resistance from practical realities like emergency access needs, legacy systems, or lack of alignment across IT and compliance teams. In industries like retail and logistics, shared terminals make device-bound credentials difficult to enforce. In education, student and staff accounts often rely on basic login infrastructure that doesn't support advanced credentialing.

This isn't just a technical limitation, it's an organisational one. Without coordinated support across teams, passwordless authentication becomes a cosmetic change rather than a structural one.

Cryptographic proofs

Moving beyond passwords isn't about removing friction, it's about changing the trust model. In a mature Zero Trust system, identity is not something a user asserts; it's something a system proves.

Modern credentials are based on asymmetric cryptography: A device generates a public-private key pair during registration. The private key is stored in secure hardware, such as a Trusted Platform Module or Secure Enclave, and never leaves the device. The public key is shared with the service.

During authentication, the service issues a random challenge. The device uses the private key to sign the challenge. The server verifies the signature using the public key. Since the private key never travels over the network and is never reused, phishing, credential replay, and credential stuffing attacks become functionally impossible.

Importantly, this model is device-bound, not human-managed. It removes the need for users to create, remember, or rotate secrets. Authentication becomes context-aware and continuous, relying not only on credentials but also on device health, user behaviour, and environmental risk.

Passwordless authentication

Too often, organisations treat passwordless authentication as a login screen upgrade. They enable biometrics or push notifications but retain passwords underneath as a fallback. That's not a real change.

A true passwordless model is built into the control plane. It shifts identity from a one-time event to an ongoing evaluation of signals like device health, behavior, and access context. SSO, MFA, and risk engines aren't just features anymore, they work together as part of a continuous trust decision.

In this model, users don't manage credentials, systems do. And every access decision is logged, explainable, and adaptable. Credential management, in this model, is largely invisible to the user but fully transparent to security teams.

Every key has provenance. Every session is verifiable. And access decisions can be made in real time without disrupting user flow.

Credential-based identity

Transitioning to this model isn't an overnight overhaul. It requires a phased approach focused on high-risk users and access points such as administrative users, accounts with remote access, and external contractors. These users are the most frequently targeted, and their

compromise has the highest blast radius.

Replace passwords for these roles with cryptographic credentials backed by strong device-binding policies. Remove the ability to fall back on shared secrets. Track what changes like reduced help desk tickets, faster response times, and better audit results, and use that to build the business case for broader adoption.

Use life cycle events such as onboarding, role changes, and offboarding, as anchors for change. Make sure new users never get passwords in the first place. The fewer legacy credentials you issue, the less technical debt you'll need to reverse later.

Make credential hygiene a governance goal, not just a deployment metric. Let each industry lead with its own highest-risk entry points:

- Banking: Customer service agents and high-value transaction workflows
- Healthcare: Clinician workstations and prescription access
- Education: Faculty access to academic records and payroll systems

Transition is not optional

Credential compromise continues to dominate breach reports, not because users are careless, but because the architecture still makes it possible. Phishing, credential stuffing, and session hijacking all thrive on the same weakness: a transferable, human-managed secret that was never designed for the complexity of modern systems.

The real solution isn't to build taller walls around passwords but to remove them entirely. By moving toward cryptographic, system-governed credentials, organisations gain more than a security upgrade, they elevate digital trust itself. By adopting Zero Trust enterprises are enabling an identity layer that is verifiable, tamper resistant, and resilient by design.

This is an enterprise imperative. It's no longer about reminding users to create stronger passwords, it's about helping organisations design and deploy systems that eliminate passwords altogether. 🔒



CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD
CLEANROOM™ RECOVERY



Visit [commvault.com](https://www.commvault.com) to Learn More

BUILDING CYBER RESILIENCE THROUGH COLLABORATION: WHY IT MATTERS MORE THAN EVER IN MIDEAST

CYBERWISE STRENGTHENS ITS DECADE-LONG REGIONAL COMMITMENT AS COLLECTIVE DEFENCE BECOMES ESSENTIAL FOR THE GCC'S DIGITAL FUTURE.

For over ten years, Cyberwise has been deeply embedded in the Middle East's cybersecurity landscape—supporting banks, payment providers, government entities and critical infrastructure organisations through an era of unprecedented digital change. Far from being a newcomer, the company has grown alongside the region's digital transformation and now sees its mission evolving from expansion to sustained, long-term investment in regional cyber resilience.

Today, as GCC governments accelerate national strategies, financial institutions scale digital services, and enterprises adopt cloud, AI, and next-generation platforms at record speed, the stakes have never been higher. Cyberwise is doubling down on its presence, talent and collaborative initiatives to help build a more resilient, interconnected cybersecurity ecosystem across the Middle East. As part of this commitment, the company will establish its local entity in Saudi Arabia in early 2026—strengthening its ability to support national priorities and remain close to the day-to-day operational realities of its clients.

Traditional cybersecurity to resilience

For many organisations, security has long been synonymous with technology stacks—firewalls, endpoint tools, and dashboards. While these remain essential, Cyberwise emphasises that tools alone create a false sense of security if organisations lack the ability to respond, adapt and recover when incidents inevitably occur.

Cyber resilience reframes the conversation around a more practical question: How quickly can the business continue operating with minimal disruption when something goes wrong?

This shift integrates cybersecurity with business continuity, governance, crisis management, and culture. And in markets like the UAE and Saudi Arabia—where fintech, digital services, and AI adoption are accelerating rapidly—resilience is no longer optional. It becomes the measure of whether an organisation can detect early, contain effectively, communicate clearly and recover confidently.

Collaboration region's strongest defence

With threats moving across borders, industries, and shared technologies,

cybersecurity is no longer an isolated function. Cyberwise stresses that collective defence—uniting financial institutions, regulators, service providers and cybersecurity companies—creates a powerful regional early-warning system.

Faster information sharing

Earlier visibility into shared risks

Coordinated response actions

Less duplication of mistakes

GCC regulators have taken significant steps in this direction by encouraging reporting, strengthening frameworks, and promoting knowledge exchange. Cyberwise's role is to bridge global insights with local realities—translating threat intelligence, identifying sector-wide patterns, and helping institutions adopt global best practices tailored to the region. In an economy as interconnected as the GCC, this level of collaboration is not just beneficial; it is essential.

Hidden challenges of operationalising resilience

Despite growing awareness, many organisations still struggle to make resilience truly operational. CYBERWISE identifies four recurring challenges:

1. Consistency:

Strong strategies often fail in execution

Kadir Yüceer
Regional Director(EMEA),
Cyberwise.



when preparedness varies across teams or locations.

2. Visibility:

Hybrid environments, legacy systems, and evolving architectures create blind spots that complicate detection and decision-making.

3. Culture:

Resilience demands cross-functional coordination—IT, security, risk, operations, and leadership. Silos slow response and fragment decision-making.

4. Continuous Testing:

Annual drills are not enough. Real resilience requires regular, realistic simulations that expose gaps before attackers do.

Organisations that overcome these challenges treat resilience not as a project, but as an operational discipline embedded across the entire business.

Resilience by design

Cyberwise helps clients build resilience deliberately—integrating cyber readiness into the architecture, processes, and decision-making of the organisation from the very beginning.

Technical Resilience

- Continuous monitoring
- Threat-led validation
- Red teaming
- Proactive detection logic
- Incident readiness exercises that mimic real attacker behavior

These capabilities reduce blind spots and ensure controls hold up under real pressure.

Organisational resilience

- Clear governance and role definition
- Crisis simulations and tabletop exercises
- Communication planning
- Cross-team coordination
- A culture where security is part of daily operations, not isolated within IT

What sets Cyberwise apart is how it connects all these layers. Strong policies mean little without real-world validation; detection capability is ineffective without a rehearsed response. By aligning

CYBER RESILIENCE REFRAMES THE CONVERSATION AROUND A MORE PRACTICAL QUESTION: HOW QUICKLY CAN THE BUSINESS CONTINUE OPERATING WITH MINIMAL DISRUPTION WHEN SOMETHING GOES WRONG?

people, processes, and technology, the company helps clients maintain operations even during disruption. The ultimate outcome is confidence—knowing that teams are prepared and decisions are informed when the unexpected occurs.

Global lessons applied to GCC realities

From Türkiye to Europe to Africa, CYBERWISE has witnessed a consistent pattern: resilience becomes truly durable only when cybersecurity becomes part of the organisational identity.

Three lessons stand out:

1. Security must transcend compliance and become embedded in how teams collaborate and make decisions.
2. Threat-led, continuous testing—not annual checklists—gives leadership a realistic view of readiness.
3. Clear, rehearsed communication channels significantly reduce confusion during high-pressure incidents.

The GCC is uniquely well-positioned to adopt these global best practices thanks to strong regulatory frameworks, ambitious digital agendas, and sector-level collaboration. Modernisation is accelerating, and with it, the opportunity to build resilience into the region’s digital fabric.

CISOs across the region are navigating one of the most demanding operating environments in the world—balancing rapid transformation, complex threats, regulatory expectations and cross-border operations while safeguarding continuity.

Cyberwise sees several key trends:

- A shift toward realism, with CISOs prioritising continuous validation through red teaming and simulations.
- Growing focus on identity, cloud, and third-party ecosystems, recognising that resilience requires alignment far beyond the organisation’s perimeter.
- A critical challenge: bandwidth. With responsibilities expanding, no CISO can shoulder the load alone.

This is where ecosystem collaboration becomes indispensable. Cyberwise supports CISOs by extending capacity, translating strategy into operational reality, and ensuring security teams are connected—not isolated. The company’s goal is not simply to fill gaps, but to enable a stronger, more unified cybersecurity community across the region.

Shared vision for resilient digital future

As the GCC builds the foundations of tomorrow’s digital economy, cyber resilience will define the region’s long-term stability and competitiveness. Cyberwise’s commitment—strengthened by local investment, regional collaboration and global expertise—aligns perfectly with this vision. The message is clear: resilience is not built through tools alone. It is built through partnership, preparedness, and collective defence. And after more than a decade in the Middle East, Cyberwise is more committed than ever to supporting organisations as they navigate the challenges and opportunities ahead. 📍



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 46:1¹, 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.

¹Delinea, Cybersecurity and the AI Threat Landscape, 2025



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