60 black hat MIDDLE EAST AND AFRICA MINUTES

black hat MIDDLE EAST AND AFRICA
tahawultech.com

Show dates: 2-4 December 2025, Riyadh Exhibition & Convention Center, Malham, Saudi Arabia
Exhibition hours: 11AM - 8PM

DAY 3

Seclore strengthens commitment to Saudi Arabia's digital transformation agenda

FROM SOVEREIGN CLOUD TO AI ADOPTION, JUSTIN ENDRES DETAILS HOW SECLORE'S PLATFORM SUPPORTS VISION 2030 PRIORITIES AND ELEVATES REGIONAL DATA RESILIENCE.

Digital acceleration across the Middle East and Africa is redefining how governments and enterprises safeguard their most valuable asset: data. With AI adoption rising, cloud ecosystems expanding, and national digital strategies advancing at unprecedented scale, organisations are demanding smarter, more predictive, and more unified approaches to data security. The shift toward data-centric defence is no longer optional — it is foundational to building resilient, future-ready digital economies.

Within this landscape, Seclore is emerging as a key enabler of intelligent data protection, offering enterprises and public-sector entities the ability to understand, govern, and secure data across complex, fast-moving environments. Speaking to Daniel Sheperd, Online Editor, Tahawultech.com, at Black Hat MEA 2025, Justin Endres, Chief Revenue Officer, shared insights into the company's vision for the MEA region, the evolution of its security framework, and how Seclore's strategy aligns with Saudi Arabia's national priorities. Endres also highlighted the strategic importance of Black Hat MEA as a platform for customer engagement, collaboration, and innovation.

What is Seclore's vision for the Middle East and Africa region, and which additional geographies are you targeting for expansion?

Our vision is simple yet ambitious: to become the global data-centric security backbone for enterprises and governments worldwide. In the Middle East and Africa, organisations are accelerating digital transformation, cloud adoption, and AI integration. This creates an urgent need for stronger, intelligence-driven data protection. We see MEA not just as a growth region, but as a strategic landscape where governments and enterprises are moving fast toward AI-enabled economies. Beyond the region, we are expanding across global markets where data sovereignty, cloud proliferation, and regulatory expectations demand a more advanced model of data security. Seclore aims to be the platform that protects this next generation of digital ecosystems — wherever the data travels.

Could you elaborate on your new security framework and the core problems it aims to address?

We're introducing a powerful evolution of our data-centric security platform by adding an intelligence and predictive analytics layer on top of our existing controls.

The new framework addresses three core challenges:

CONTINUED ON PAGE 3

Black Hat MEA surges through day two as Capture the Flag competition takes centre stage

RIYADH DRIVES THE GLOBAL CYBERSECURITY CONVERSATION WITH BREAKTHROUGH EXPLOITS, HANDS-ON SIMULATIONS AND HIGH-PRESSURE INTELLIGENCE AT BLACK HAT MEA.

Black Hat MEA lit up Riyadh again for day two, pulling the global cybersecurity community deeper into the core questions shaping 2026. Thousands of specialists, founders, CISOs and researchers were in attendance to discuss the next trends in cybersecurity. Across the Executive Summit, Briefings and Deep Dive stages, the conversations cut straight into the realities of the current threat horizon: attack surfaces that shift by the minute, AI systems that influence the decision cycle, supply chains that create hidden dependencies and identity layers constantly pushed to breaking point.

Anne Marie Zettlemoyer of the National Security Institute delivered one of the morning's most urgent sessions. "The systems we defend and the speed at which we defend them have changed more in the past couple of years than in the previous twenty" she said, stressing that AI has shifted from emerging idea to "our next critical infrastructure." She closed with a clear challenge. "Black Hat is not just a conference, it is a gathering of the most capable strategic and powerful minds anywhere in the world. If anyone can define responsible AI security, it is this community."

Charles Forte, Director General and CIO at the UK Ministry of Defence, used a 'Surfing the Digital Tsunami' analogy to break down what effective leadership looks like when attack surfaces expand faster than defenders can map them. He told attendees that "being good at digital defines winning and losing" and outlined three priorities for any organised response: discipline in process, new investment in AI era defence and equal scrutiny on the supply chain as in internal systems.

The focus then moved to career impact with a session named Mastering the CISO Maturity Model, led by Derek Cheng, CISO at Deliveroo. Cheng mapped out the real benchmarks for modern security leadership. He explored how CISOs measure influence, scale governance, and evolve from technical operators into high-impact decision-makers who shape risk agendas at board level.

The Ship Spoofing simulation quickly became one of day two's biggest draws. Before stepping into the live environment, participants were briefed on the fundamentals: how navigation systems on modern vessels can be manipulated by corrupted data streams and how

CONTINUED ON PAGE 4

SECLORE™

Data Security Intelligence Framework

CONTINUED FROM PAGE 1

Seclore...

1. Visibility Gaps
Organisations struggle to see how data is being used across apps, clouds, endpoints, and AI models. Our updated framework gives clear, real-time insight into data usage and behaviour.

2. Misuse and Insider Risk
Misconfiguration, unauthorised access, and misuse — whether accidental or malicious — remain persistent threats. We now offer predictive indicators that identify abnormal patterns before they escalate.

3. AI + Data Governance
As organisations adopt AI, data becomes both fuel and risk.

Our goal is not just to protect data, but to help organisations understand, govern, and optimise that data so they can innovate responsibly.

This is the level of maturity the market has been demanding, and we're excited to pioneer it.

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

Saudi Arabia is undergoing one of the world's most ambitious national digital transformations. Investments in sovereign cloud, AI, smart cities, and data governance frameworks perfectly align with Seclore's focus on secure, intelligent data management.

Government support, strong regulatory direction, and a rapidly expanding talent ecosystem make the Kingdom a strategic environment for data-centric innovation.

Our platform directly supports national objectives by enabling:

- compliance with cybersecurity and data-protection frameworks
- secure cloud and AI adoption
- continuous visibility and control over data movement
- strengthening of digital resilience across critical sectors

Saudi Arabia's momentum positions it as a global benchmark — and Seclore is committed to being part of that future.

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 has become one of the most influential cybersecurity events globally.

For us, the value is clear:

- Direct customer engagement with enterprises and government entities
- Insight into emerging regional challenges
- Collaboration opportunities with partners and innovators
- A platform to showcase our newest capabilities
- A space to learn — not just exhibit

We've invested significantly in this event because the return on innovation and customer connection is undeniable. Black Hat MEA enables us to stay closely aligned with the region's security priorities.

CONTINUED FROM PAGE 1

Black Hat MEA...

a single injected signal can redirect or blind critical systems. Inside the simulation, attendees watched ships veer off course in real time as spoofed coordinates rewrote their route logic. The experience exposed why maritime transport is now a high-value target and how much work remains to reinforce this sector against increasingly precise attacks.

But the centerpiece for day two was the world's largest Capture the Flag (CTF) competition. Thousands of specialists are locked into a three-day jeopardy-style tournament designed to test and sharpen ethical hacking skills across categories, including web, PWN, forensics, reverse engineering, and cryptography. With the finale set for tomorrow, every remaining challenge becomes a potential match-winner, where one decisive exploit could rewrite the entire table before the countdown hits zero.

Running alongside CTF is the Bug Bounty Cup. Here, elite hunters spent the day drilling into live targets on the Bug Bounty platform, surfacing critical vulnerabilities and pushing each other to stay ahead by minutes, not hours. The competition has built steadily across two days, and tomorrow's final hits will determine who walks out with top discoveries and the bragging rights that matter in this community.

Steve Durning, Portfolio Director of Black Hat MEA at Tahaluf, said: "Day two showed how powerful the activity-led experiences have become at Black Hat MEA. The simulations, competitions and hands-on environments are where theory gets pressure-tested and where teams discover what actually holds up against real attacks. Riyadh is proving that when you put this level of capability in one place, progress accelerates fast."

Annabelle Mander, Executive Vice President of Tahaluf, added: "Day two showed how quickly this community moves when the pressure is real. The conversations here are not theory. They are decisions that shape national resilience and global security. Riyadh has become a place where IT leaders compare notes, challenge assumptions, and build capability with clarity and intent."

Black Hat MEA moves into its final day, and the focus turns to advanced research, high-impact strategy discussions and the closing rounds of the CTF and Bug Bounty Cup. Tomorrow brings new disclosures, fresh intelligence, and the final battles that will decide the champions of both competitions. Day three will deliver clarity on the risks, capabilities and decisions that will define the next year of global cybersecurity.

Cisco AI Readiness Index 2025 reveals KSA's proactive approach to AI security amid rapid adoption

- *60% of KSA organisations are highly aware of AI-specific security threats, with over half (51%) already deploying AI to enhance cybersecurity defenses.*
- *KSA organisations are rapidly scaling AI adoption, with 91% planning to deploy AI agents and 68% reporting tangible gains in profitability, productivity, and innovation from their AI investments.*
- *Over a third (39%) of organisations in the Kingdom are integrating AI directly into their security and identity systems, demonstrating growing confidence in controlling and securing AI agents.*

Ahead of Black Hat MEA in Riyadh from 2-4 December 2025, Cisco, the worldwide leader in networking and security, released the KSA findings from the third annual Cisco AI Readiness Index, highlighting how organisations in the Kingdom are leveraging AI to strengthen cybersecurity and respond to emerging AI-driven threats.

The Cisco AI Readiness Index 2025 is a global study, now in its third year, based on a double-blind survey of 8,000 senior IT and business leaders responsible for AI strategy at organisations with over 500 employees across 26 industries.

As AI becomes more prevalent, KSA organisations are prioritising security. According to the Index, a significant 60% of respondents are highly aware of AI-specific threats, with 51% actively deploying AI to enhance cybersecurity capabilities, including faster threat detection, response, and recovery.

More organisations are embedding AI directly into their security architecture. In KSA, 39% of organisations are integrating AI into their security and identity systems, and a further 39% say they are fully equipped to control and secure AI agents across their environments. Together, these figures show that many KSA organisations are moving beyond experimentation and now embedding and governing AI as part of their core security approach.

The Index also reveals that AI adoption in the Kingdom is scaling at pace. In KSA, 91% of organisations plan to deploy AI agents, and 40% expect these agents to work alongside employees within the next year. At the same time, 68% already report gains across profitability, productivity and innovation because of AI investments, underscoring AI's growing impact on business outcomes.

"Saudi Arabia is making strong progress in embedding AI across its economy in line with Vision 2030," said Fady Younes, Managing Director for Cybersecurity at Cisco Middle East, Africa, Türkiye, Romania and CIS.

"Our latest AI Readiness Index reveals KSA organisations are not just rapidly scaling AI but are critically adopting a proactive stance on protecting AI, data, and identities. Cisco is powering this secure evolution with our AI-ready infrastructure and next-generation security solutions. At Black Hat MEA, we look forward to engaging directly with our customers and partners to explore practical strategies for strengthening cyber resilience in the AI era."

At this year's premier cybersecurity event, Cisco spotlighted its latest innovations where security meets the network, with solutions powered by the combined strengths of Cisco Security and Splunk. The company will engage customers, partners, and security practitioners on strategies to build secure, AI-ready infrastructure and modern security operations to defend against AI-driven threats.

Attendees will see how organisations can protect identities, secure AI agents, and gain end-to-end visibility across hybrid environments as they adopt and scale AI. Cisco will showcase solutions for the AI era, including AI Defense, Hybrid Mesh Firewall and Universal Zero Trust Network Access (ZTNA) that simplify policy management, enhance visibility, and help enterprises scale securely. Additionally, Cisco will highlight advancements in Splunk integrations that unify data across platforms and empower security teams to automate tasks and respond faster to threats.

CPI Corporate Publishing International Ltd. tahawultech.com
cnme computer news middle east · Security Advisor Middle East · Reseller Middle East · 60 MINS LIVE عربية · GovTech

Founder, CPIMEDIA GROUP **Dominic De Sousa** (1959-2015), Group Publishing Director **Kausar Syed,** Sales Director **Sabita Miranda**,
Editors **Mark Forker, Sandhya D'Mello, Daniel Shepherd**, Designer **Prajith Payyapilly**, Web Developer **Adarsh Snehajan**

Saudi Arabia's cybersecurity evolution accelerates with Kaspersky's new academy and expanding MoUs

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 Sheperd, 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.

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 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?

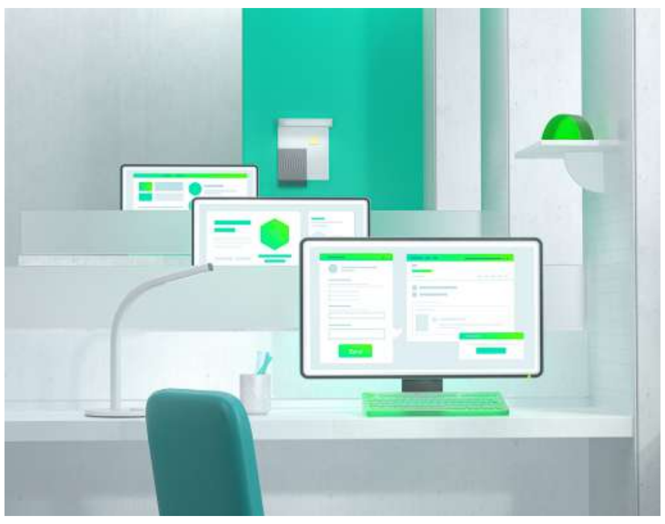
AI systems themselves can be manipulated; attackers can tamper with datasets or libraries to influence outputs. Before adopting AI at scale, organisations must ensure their infrastructure is properly secured. I strongly advise investing in strong cybersecurity solutions and conducting compromise assessments and penetration testing to uncover hidden vulnerabilities before deploying AI-driven tools.

Human error fuels breaches as only half of professionals receive cybersecurity training

A recent Kaspersky survey in the Middle East, Turkiye and Africa (META) region entitled "Cybersecurity in the workplace: Employee knowledge and behavior", found that just 48% of professionals in the United Arab Emirates received a training on digital threats. This knowledge gap is significant, especially given that the majority of cybersecurity breaches are attributed to human error. The findings underscore a need for IT departments to provide clear guidance and for organizations to implement structured, practical cybersecurity training that reaches employees at every level.

Many cyberattacks today are deliberately designed to bypass digital defenses by exploiting human psychology. "Social engineering" schemes, like phishing emails, manipulate trust and urgency to trick employees into sharing sensitive information or initiating fraudulent transactions. Nearly half of surveyed professionals (45.5%) encountered scams disguised as messages from their organization, colleagues or suppliers within the past year, while 13% suffered negative consequences after such deceptive communication. Other cybersecurity issues closely linked to the human factor include compromised passwords, the leakage of sensitive data, unpatched IT systems and applications, unlocked and unencrypted devices.

Human-related cyberattacks can be prevented through appropriate education and awareness. 13,5% of respondents acknowledged they made IT-related mistakes due to a lack of cybersecurity knowledge. At the same time, training was named as the most effective means of raising cybersecurity awareness among non-IT employees: 59% of professionals chose it over other options such treat stories (27%) and references to legal responsibility (37.5%). These findings show that cybersecurity training is an essential layer of organizational defense.



When given the opportunity to choose specific training topics, respondents said they would choose ones dedicated to websites and internet security (47%); security of accounts and passwords (43%); protecting confidential work data (41%), e-mails (35%), mobile devices (33%), safe use of social networks and messengers (28%), secure remote work (26,5%) and safe use of neural network-based services such as chatbots (24%), while 23% would prefer to undergo all the above trainings, which highlights the broad demand for comprehensive cybersecurity education.

The data shows that employees are open to improving their cybersecurity skills. However, for this knowledge to become an integral part of their daily IT routines, training needs to be well-structured, tailored to the role and existing IT skills of each employee, regularly updated, as well as gamified and practical. This approach enhances engagement and knowledge retention. When organizations invest in such education, they are not just meeting a requirement, but also fostering a "security-first" mindset among workforce. This turns employees from a potential point of weakness into a distributed network of vigilant guards, capable of making smart security decisions instinctively.

"Cybersecurity can't live solely within the IT department. Everyone—from executives to new hires—needs a clear grasp of digital risks. A truly resilient organization is built by equipping every employee with the skills to recognize scams, prevent costly errors, and safeguard company data," comments Rashed Al Momani, General Manager for the Middle East at Kaspersky.

To strengthen their defences organizations should consider the following:

- Implement robust monitoring and cybersecurity solutions, for example from the Kaspersky Next product line.
- Introduce employee education and cybersecurity trainings, such as Kaspersky Automated Security Awareness Platform, developed to help IT and HR departments with delivering practical cybersecurity skills to employees.
- Implement security policies for employees, from password and software installation to network segmentation.
- Foster a culture of security: encourage employees to report suspicious activity, reward proactive security behaviors to reinforce good habits.

*The survey was conducted by Toluna research agency at the request of Kaspersky in 2025. The study sample included 2800 online interviews with employees and business owners using computers for work in seven countries: Türkiye, South Africa, Kenya, Pakistan, Egypt, Saudi Arabia, and the UAE.

black hat
MIDDLE EAST AND AFRICA

2 - 4 DECEMBER 2025
MALHAM, SAUDI ARABIA

CYBERSECURITY'S GLOBAL STAGE

REGISTER FOR YOUR **FREE** PASS TODAY

GCC enterprises accelerate security readiness for post-quantum future

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 Sheperd, 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.

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-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.

The threat landscape is moving fast—and CISOs must ensure their organisations can adapt just as quickly.

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:

1. **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.

2. **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.

3. **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.

4. **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.

5. **Secure VMI – Virtual Mobile Infrastructure**

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.

Anne Marie Zettlemoyer of the National Security Institute delivered a powerful warning at Black Hat MEA 2025, noting that the systems we defend have changed more in two years than in the previous twenty.

Zscaler highlights advanced security solutions

Zscaler, Inc., showcased its Zero Trust Exchange platform at Black Hat MEA 2025, demonstrating how Zero Trust Everywhere helps organisations modernise their security architectures and defend against advanced cyber threats.

As digital transformation accelerates, organisations require security approaches that protect distributed users, applications, and devices. Zscaler's AI-powered platform delivers secure and reliable connectivity while reducing operational complexity and cost. Visitors attending Black Hat MEA can explore these solutions at Hall 1 Stand N31, where Zscaler experts will conduct live demonstrations throughout the event.

Supporting Saudi Arabia's Digital Future

Saudi Arabia's Vision 2030 continues to advance national goals for cybersecurity, digital transformation, and technology-driven growth. Zscaler's participation reflects its commitment to supporting organisations across the Kingdom as they build secure and scalable digital foundations that enable cloud adoption, smart services, and AI-led innovation.

The company will also present its AI-powered data security offering, which safeguards sensitive information across cloud, endpoint, and mobile environments. The service combines AI-based discovery, TLS/SSL inspection, and unified policy controls to secure data wherever it travels, addressing new risks that accompany the rapid adoption of AI tools and autonomous systems.

These capabilities align with national initiatives led by the Saudi Data and Artificial Intelligence Authority (SDAIA). By enabling organisations to protect and manage data responsibly, Sscaler supports SDAIA's vision of positioning Saudi Arabia as a global leader in data-driven innovation and artificial intelligence.

Advancing Connectivity and Data Protection

Zscaler will also highlight Zscaler Cellular, a key advancement that integrates Zero Trust principles directly into a cellular SIM card. The solution removes the need for traditional agents or VPNs, allowing devices to connect securely to any network while operating in isolated environments to prevent lateral movement. This solution is especially valuable for sectors such as manufacturing, logistics, and energy, where secure and resilient connectivity is essential.

"Zscaler has led the evolution of Zero Trust by securing users and applications, and we're now extending that protection to IoT and OT environments," said Ahmed Al Qadri, Regional Sales Director at Zscaler. "With Zscaler Cellular, organizations can strengthen device security, streamline connectivity, and maintain full visibility and control."

Zscaler experts will further demonstrate how the Zero Trust Exchange Platform enhances the security of hybrid workforces and modern workloads. By replacing traditional VPNs and firewalls with direct, secure access to applications, organizations can improve performance, enhance user experience, and elevate their overall security standards.

By continuing to expand Zero Trust across users, devices, workloads, and now cellular-connected environments, Zscaler is helping organisations strengthen cyber resilience and simplify security operations. The company's presence at Black Hat MEA 2025 demonstrates the company's ongoing commitment to supporting secure digital transformation across Saudi Arabia and the wider region as enterprises embrace cloud, AI, and next-generation connectivity.

Inside the Industrialisation of Cybercrime: What to Expect in 2026

Automation, AI, and Scale Will Define the Next Phase of the Global Cyberthreat Landscape.

Each year, FortiGuard Labs analyses how technology, economics, and human behavior shape global cyber risk. The 2026 Cyberthreat Predictions Report outlines a turning point in that evolution. Cybercrime will continue to evolve into an organised industry, built on automation, specialisation, and artificial intelligence (AI). But in 2026, success in both offense and defense will be determined less by innovation than by throughput: how quickly intelligence can be turned into action.

From Innovation to Throughput

Because AI, automation, and a mature cybercrime supply chain will make intrusion faster and easier than ever, attackers will spend less time inventing new tools and more time refining and automating techniques that already work. AI systems will manage reconnaissance, accelerate intrusion, parse stolen data, and generate ransom negotiations. At the same time, autonomous cybercrime agents on the dark web will begin executing entire attack stages with minimal human oversight.

These shifts will exponentially expand attacker capacity. A ransomware affiliate that once managed a handful of campaigns will soon be able to launch dozens in parallel. And the time between intrusion and impact will shrink from days to minutes, making speed the defining risk factor for organisations in 2026.

The Next Generation of Offense

FortiGuard Labs expects to see the emergence of specialised AI agents designed to assist cybercriminal operations. Although these agents will not yet operate independently, they will begin to automate and enhance critical stages of the attack chain, including credential theft, lateral movement, and data monetisation.

At the same time, AI will accelerate the monetisation of data. Once attackers gain access to stolen databases, AI tools will instantly analyse and prioritise them, determine which victims offer the highest return, and generate personalised extortion messages. As a result, data will become currency faster than ever before.

The underground economy will also become more structured. Botnet and credential-rental services will become increasingly tailored in 2026. Data enrichment and automation will enable sellers to offer more specific access packages based on industry, geography, and system profile, replacing the generic bundles that dominate today's underground markets. Black markets will adopt customer service, reputation scoring, and automated escrow. Due to these innovations, cybercrime will accelerate its evolution toward full industrialisation.

The Evolution of Defense

Defenders will need to respond with the same efficiency and coordination. In 2026, security operations will move closer to what FortiGuard Labs describes as machine-speed defense—a continuous process of intelligence, validation, and containment that compresses detection and response from hours to minutes.

Frameworks such as continuous threat exposure management (CTEM) and MITRE ATT&CK will need to be leveraged so defenders can quickly map active threats, identify exposures, and prioritise remediation based on live data. Identity will also need to become the foundation of security operations, as organisations will need to not only authenticate people but also automated agents, AI processes, and machine-to-machine interactions.

Managing these non-human identities will become critical to preventing large-scale privilege escalation and data exposure.

Collaboration and Deterrence

Industrialised cybercrime will also demand a more coordinated global response. Initiatives such as INTERPOL's Operation Serengeti 2.0, supported by Fortinet and other private-sector partners, demonstrate how joint intelligence sharing and targeted disruption can dismantle criminal infrastructure. New initiatives, such as the Fortinet-Crime Stoppers International Cybercrime Bounty program, will enable global communities to safely report cyberthreats, helping to scale deterrence and accountability.

FortiGuard Labs also expects to see continued investment in education and deterrence programs that target young or at-risk populations who are being drawn into online crime. Preventing the next generation of cybercriminals will depend on redirecting them before they enter the ecosystem.

Looking Ahead

By 2027, cybercrime is expected to function at a scale comparable to legitimate global industries. FortiGuard Labs predicts further automation of offensive operations through agentic AI models, where swarm-based agents will begin coordinating tasks semi-autonomously and adapting to defender behavior, alongside increasingly sophisticated supply-chain attacks targeting AI and embedded systems.

Defenders will need to evolve as well, leveraging predictive intelligence, automation, and exposure management to contain incidents faster and anticipate adversary behavior. The next stage of cybersecurity will depend on how effectively humans and machines can operate together as adaptive systems.

Velocity and scale will define the decade ahead. Organisations that unify intelligence, automation, and human expertise into a single, responsive system will be the ones best able to withstand what comes next.

StarLink sharpens AI-first cybersecurity vision to power Saudi Arabia's next decade of digital 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.

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 Sheperd, 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.

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 is 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?

Becaus**e** we have direct, constant engagement with Saudi customers, 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.

black hat MIDDLE EAST AND AFRICA
THE WALL STREET JOURNAL.
What Musk, Altman and Others Say About AI-Funded 'Universal Basic Income'
'There's Just No Reason to Deal With Young Employees'
AI is taking entry-level jobs. What happens when Gen-Z-ers can't start their careers?
The Future of Work – Cutting Through the Sci-Fi
Dr. Rumman Chowdhury
Founder & CEO
Humane Intelligence
#BHMEA25

CYBER READINESS BECOMES REALITY
WITH
COMMVAULT® CLOUD CLEANROOM™ RECOVERY
Commvault®
Visit commvault.com to Learn More

Hybrid visibility, AI observability, and post-quantum readiness will define 2026, says Gigamon official

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.

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. According to this year Gigamon Hybrid Cloud Survey 91% of global Security and IT leaders say they are "recalibrating" how they assess hybrid cloud risk in light of growing AI-driven threats and increased complexity.

The conversations are surely shifting 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 and as an example 89% of Security and IT leaders now cite deep observability as fundamental to securing hybrid cloud 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?

As quantum computing advances, current public key encryption methods will soon be at risk. Leading analysts forecast traditional cryptography will be unsafe as early as 2030. Many organisations already have post-quantum strategies because threat 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.

رقميات
Raqmiyat

Secure Your Digital Future

Simple. Secure. Resilient.

Secure Your Enterprise IT Footprint For A Safer Digital Journey

www.raqmiyat.com
UAE | KSA | INDIA

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**

FORTINET