ISSUE 100 | NOVEMBER 2025

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

QUANTUM THREAT ARRIVES EARLY: RACE TO PROTECT DATA STARTS NOW

QUANTUMGATE'S CTO JANNE HIRVIMIES WARNS THAT ATTACKERS ARE ALREADY HARVESTING ENCRYPTED DATA — AND THE WINDOW FOR POST-QUANTUM READINESS IS RAPIDLY CLOSING.

tahawultech.com

cnme computer news middle east SUPPLEMENT

Delinea

Unlock AI's potential, not your defenses.

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

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

Secure AI with Delinea so you can:

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

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

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

delinea.com

CONTENTS


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

EDITOR'S NOTE

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

Sandhya DMello
Editor

AI AND QUANTUM FORCES REDEFINE CYBERSECURITY

The cybersecurity landscape is entering a decisive new phase as organisations confront rapid shifts in threats, innovation, and digital transformation across the Middle East. This November issue captures that momentum, spotlighting the technologies and leadership shaping the region's next decade of cyber resilience.

Our cover story examines the rising urgency of quantum disruption. QuantumGate CTO Janne Hirvimies outlines why the quantum threat is already unfolding, with adversaries harvesting encrypted data today to decrypt in the future. Post-quantum readiness now demands long-term planning across cloud platforms, hardware ecosystems, critical infrastructure, and national strategies. The UAE's early steps toward quantum resilience offer an important regional benchmark.

BUILDING QUANTUM-SAFE FOUNDATIONS

Urgency also defines our Black Hat MEA feature, where Tenable Co-CEO Mark Thurmond explains how exposure management is shifting cybersecurity from reactive to pre-emptive. Unified visibility, AI-driven prioritisation, and rapid action are emerging as the new foundation for modern defence strategies. This edition also includes a Special Report on LinkShadow's participation at Black Hat MEA 2025, chronicling the debut of CyberMeshX and its vision for unified, AI-driven security architecture.

GITEX Global 2025's energy runs through the magazine, highlighting next-generation solutions from Delinea, Sophos, Seclore, Forescout, SentinelOne, Fortinet, Zscaler, and StarLink. Identity, automation, sovereignty, and AI-powered resilience continue to dominate enterprise security priorities.

Our news section tracks major advancements in agentic AI, sovereign cloud, and autonomous cybersecurity. Innovations such as CrowdStrike and NVIDIA's AI agents, Palo Alto Networks' AIRS 2.0, Cisco's Silicon One P200-based AI networking, Commvault's secure Data Rooms, and Genetec's unified cloud-native security illustrate how infrastructure is becoming more intelligent and responsive.

Across all sections, one message stands out: the Middle East is rapidly emerging as a global hub for cyber-secure, AI-driven innovation — and resilience is now a continuous discipline built on intelligence, speed, and collaboration.

EVENTS

tahawultech.com FUTURE SECURITY AWARDS

tahawultech.com CISO50 AWARDS & FORUM

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

GENETEC ENHANCES SECURITY CENTER SAAS WITH INTEGRATED AUDIO COMMUNICATIONS

The cloud-native upgrade brings intercom and SIP-based audio capabilities into Genetec's unified security platform, improving incident response and operational efficiency.

Genetec's latest Security Center SaaS update introduces real-time voice communications to its unified cloud-based security platform.

Genetec Inc., a global leader in enterprise physical security software, has announced a major expansion of its Security Center SaaS platform with the introduction of cloud-native audio communications capabilities. The new feature integrates intercom support and SIP-based audio into the same unified interface that already combines video surveillance, access control, and intrusion monitoring.

The enhancement marks another step in Genetec's drive to deliver fully unified, cloud-based security operations. By adding real-time voice functionality, the company aims to help security teams across sectors such as education, retail, and healthcare respond more quickly and make better-informed decisions.

With communications now built directly into Security Center SaaS, operators can interact with individuals at entry points, verify identities using live video, and take immediate action — all without switching between multiple tools or interfaces.

"Organisations can choose the intercom devices that best fit their needs and manage them through a single cloud-native platform without being tied into a proprietary ecosystem," said Christian Morin, Vice President of Product Engineering at Genetec Inc.

The new communications capability is designed to scale from a few intercoms to thousands across large enterprises. Built on an open, cloud-native architecture, the platform allows organisations to start small and expand rapidly, using their preferred intercom devices. At launch, the system will support intercoms from Axis, with additional vendor integrations planned for future releases.

Fredrik Nilsson, Vice President, Americas, at Axis Communications, added: "The native integration of Axis intercoms into Security Center SaaS — built with Axis Cloud Connect — enables customers to achieve enterprise-grade communications without the complexity of standalone systems. Security teams can manage Axis intercoms in the same platform they already use for video surveillance, access control, data analysis, and more."

As with all Genetec solutions, strong cybersecurity and privacy protections are built into the design. Audio data is treated as confidential information, secured through encrypted communications, and supported by audit trails for accountability. Automated updates and regular security patches ensure continued protection against emerging threats.

The new audio communications feature for Security Center SaaS is now available through the Genetec network of accredited channel partners.

CROWDSTRIKE AND NVIDIA REDEFINE CYBERSECURITY WITH ALWAYS-ON AI AGENTS

Always-on agents built with CrowdStrike Charlotte AI AgentWorks and integrated with NVIDIA Nemotron and NVIDIA NIM microservices will enable real-time threat detection and response across cloud, data center, and edge environments.

CrowdStrike is collaborating with NVIDIA to bring always-on, continuously learning AI agents for cybersecurity to the edge through Charlotte AI AgentWorks, NVIDIA Nemotron open models, NVIDIA NeMo Data Designer synthetic data, NVIDIA Nemo Agent Toolkit, and NVIDIA NIM microservices.

Expanding CrowdStrike and NVIDIA's work to build, power, and secure the agentic ecosystem, the latest collaboration will deliver autonomous, real-time AI agents that learn continuously and defend critical infrastructure across cloud, data-center, and edge environments.

"AI is transforming cybersecurity, and defenders need speed and edge intelligence to outpace the adversary," said George Kurtz, CEO and founder of CrowdStrike. "Addressing AI-driven cyber threats requires AI to protect systems from the speed and volume of attacks, and we're working with NVIDIA to deliver autonomous, AI agents that learn continuously to defend the critical infrastructure powering the global economy."

"Cybersecurity in the era of AI demands intelligence that thinks at the speed of machines," said Jensen Huang, founder and CEO of NVIDIA. "Together with CrowdStrike, we're building real-time, AI-driven security agents that defend cloud, data center, and edge infrastructure – protecting the systems that power our economy and national security."

George Kurtz, CEO and founder of CrowdStrike.

Advancing Continuous Learning and Edge Intelligence

Bringing agents built with Charlotte AI AgentWorks and NVIDIA to the edge will enable organizations to deploy autonomous, continuously learning AI agents closer to where data is created – extending protection to data centers and controlled environments. By training NVIDIA Nemotron open models with data from CrowdStrike experts using NVIDIA NeMo Data Designer, customers will be able to fine-tune and optimize models for their own AI agents, built on CrowdStrike's Agentic Security Platform. This joint innovation will enable enterprises to scale and accelerate security operations with local inference, continuously improving detection accuracy and real-time response to threats – helping to maintain control of sensitive data and align with regional sovereignty requirements.

Unifying Data, Compute, and Governance

By integrating the Agentic Security Platform – including Falcon® LogScale, Onum, and Pangea – with NVIDIA accelerated computing and CUDA-X libraries, CrowdStrike is creating a unified telemetry pipeline for high-fidelity, real-time security data. This architecture enables defenders to feed enriched telemetry directly into locally hosted AI models and agents built and optimized with the NVIDIA NeMo Agent Toolkit, now operating at the edge, allowing systems to learn safely, reason accurately, and act within enterprise guardrails.

CrowdStrike also supports the latest NVIDIA AI Factory for Government reference design, which provides guidance for security teams to build and deploy AI agents in federal and high-assurance organizations. This enables enterprises to manage multiple AI workloads on-premises and in the hybrid cloud while meeting the highest security requirements of regulated industries.

Together, CrowdStrike and NVIDIA are redefining cybersecurity for the AI era – uniting continuous learning, real-time intelligence, and machine-speed defense to protect the digital infrastructure powering the global economy and national security.

COMMVAULT UNVEILS CONVERSATIONAL AI, DATA ROOMS TO ADVANCE CYBER RESILIENCE IN REGION

Commvault, a leading provider of cyber resilience and data protection solutions for the hybrid cloud, today announced two major innovations that redefine how enterprises activate and protect their data in the age of artificial intelligence (AI). The introduction of Data Rooms and Commvault's Model Context Protocol (MCP) server represents a significant step forward in enabling organisations to securely connect backup data with AI platforms and manage resilience tasks through natural language.

Pranay Ahlawat, Chief Technology and AI Officer at Commvault.

The announcement reflects growing momentum across the Middle East, where governments and enterprises are rapidly advancing AI and data strategies in line with national vision such as the UAE's National AI Strategy 2031.

Data Rooms is a secure environment that enables enterprises to safely connect trusted backup data to the AI platforms they rely on, or to their own AI initiatives, such as internal data lakes. It combines governed, self-service access with built-in classification and compliance controls, bridging the gap between data protection and data activation and helping organisations transform backup data into AI-ready assets without adding new risk or complexity.

With the new Data Rooms offering, authorised users can locate and prepare data directly from backup repositories across on-premises and cloud environments. Built-in governance helps maintain control so that approved, access policy-compliant datasets can be safely shared and exported, with classification, sensitivity tagging, and audit trails automatically applied. Additionally, Data Rooms operate within Commvault Cloud's zero-trust architecture, leveraging role-based access controls (RBAC) and encryption at rest and in transit. These safety measures can give organisations confidence that their data remains protected, governed, and traceable from backup to activation.

"Organisations are beginning to realise that their historical data is more than just insurance, it's a powerful, untapped strategic asset," said Pranay Ahlawat, Chief Technology and AI Officer at Commvault. "With Commvault Data Rooms, enterprises can confidently export their secondary data and harness it with the AI platform of their choice to unlock new opportunities for intelligence, innovation, and business growth."

Commvault also introduced the Model Context Protocol (MCP) server, a policy-based bridge connecting enterprise systems with popular GenAI assistants such as OpenAI's ChatGPT Enterprise and Anthropic's Claude. With MCP, users can interact with Commvault Cloud in natural language to configure, manage, and execute resilience tasks. For example, a user could ask, "Is my DocuSign instance backed up?" and receive a compliant, actionable response such as, "You don't have a Docusign backup set up yet. Would you like me to create that up so that you have the necessary configuration in place?" MCP then carries out authorised actions to configure and run backup and resilience tasks, all within enterprise policies. This advancement brings human-level simplicity to cyber resilience, allowing users to communicate with Commvault Cloud just as they would to a colleague – naturally, safely, and within enterprise policy guardrails.

Every conversational interaction with Commvault Cloud takes place through Commvault's policy-based MCP server, which governs authentication, access, and encryption. In addition, Commvault does not use or train external AI models with customer data or inputs. Customer data remains protected under Commvault's privacy and security policies, and external GenAI platforms operate under their own customer-managed controls. These built-in safeguards help maintain traceability, auditability, and compliance with enterprise-grade data protection standards, so simplicity never comes at the cost of security.

"Commvault is moving beyond conversational interfaces to enable agentic resilience where AI can act on behalf of teams, safely and transparently," Ahlawat added. "By adopting the Model Context Protocol, we're giving enterprises the foundation to automate recovery and protection workflows within the guardrails of the NIST Risk Management Framework – auditable, policy-driven, and role-based access controlled. This is how we bring simplicity and trust

together in the age of AI operations."

Commvault's MCP server will enter private early access in November at Commvault SHIFT 2025, with public early access targeted for early 2026 and general availability in spring 2026. Conversational Resilience capabilities will align with the availability of supported enterprise GenAI platforms, including ChatGPT Enterprise and Claude. Additional integrations with other enterprise GenAI assistants are under evaluation.

GRAND THEFT TELEMATICS: KASPERSKY FINDS SECURITY FLAWS THREATENING VEHICLE SAFETY

Cybersecurity firm Kaspersky unveiled the results of a comprehensive security audit at the Security Analyst Summit 2025, revealing a critical vulnerability that could allow remote attackers to take control of connected vehicles belonging to a major automotive manufacturer.

By exploiting a zero-day vulnerability in a contractor's publicly accessible application, it was possible to gain control over the vehicle telematics system, compromising the physical safety of drivers and passengers. For instance, attackers could force gear shifts or turn off the engine when the vehicle is driving. The findings highlight potential cybersecurity weaknesses in the automotive industry, prompting calls for enhanced security measures.

Car manufacturer's side

The security audit was conducted remotely and targeted the manufacturer's publicly accessible services and the contractor's infrastructure. Kaspersky identified several exposed web services. First, through a zero-day SQL injection vulnerability in the wiki application (a web-based platform that allows users to collaboratively create, edit, and manage content), the researchers were able to extract a list of users on the contractor's side with password hashes, some of which were guessed due to a weak password policy. This breach provided access to the contractor's issue tracking system (a software tool used to manage and track tasks, bugs, or issues within a project), which contained sensitive configuration details about the manufacturer's telematics infrastructure, including a file with hashed passwords of users of one of the manufacturer's vehicle telematics servers. In a modern car, telematics enables the collection, transmission, analysis, and utilisation of various data (e.g., speed, geolocation, etc.) from connected vehicles.

Connected vehicle side

On the connected vehicle side, Kaspersky discovered a misconfigured firewall exposing internal servers. Using a previously acquired service account password, the researchers accessed the server's file system and uncovered credentials for another contractor, granting full control over the telematics infrastructure. Most alarmingly, the researchers discovered a firmware update command that allowed them to upload modified firmware to the Telematics Control Unit (TCU). This provided access to the vehicle's CAN (Controller Area Network) bus – a system that connects different parts of the vehicle, like the engine and sensors. Afterwards, various other systems were accessed, including the engine, transmission, etc. This enabled potential manipulation of a range of critical vehicle functions, which could endanger driver and passenger safety.

"The security flaws stem from issues that are quite common in the automotive industry: publicly accessible web services, weak passwords, lack of two-factor authentication (2FA), and unencrypted sensitive data storage. This breach demonstrates how a single weak link in a contractor's infrastructure can cascade into a full compromise of all of the connected vehicles. The automotive industry must prioritise robust cybersecurity practices, especially for third-party systems, to protect drivers and maintain trust in connected vehicle technologies," said Artem Zinenko, Head of Kaspersky ICS CERT Vulnerability Research and Assessment.

Kaspersky recommends that contractors restrict internet access to web services via VPN, isolate services from corporate networks, enforce strict password policies, implement 2FA, encrypt sensitive data, and integrate logging with a SIEM system for real-time monitoring.

For the automotive manufacturer, Kaspersky advises restricting telematics platform access from the vehicle network segment, using allowlists for network interactions, disabling SSH password authentication, running services with minimal privileges, and ensuring command authenticity in TCUs, alongside SIEM integration.

PALO ALTO NETWORKS STRENGTHENS ENTERPRISE AI SECURITY WITH PRISMA AIRS 2.0

Palo Alto Networks has introduced Prisma AIRS 2.0, a major enhancement to its AI security portfolio aimed at protecting enterprises across the entire artificial intelligence lifecycle. The upgraded platform represents the full integration of Protect AI, which the company recently acquired, and extends its leadership in securing AI-driven business transformation.

With artificial intelligence becoming central to enterprise operations, the security implications have become more pressing. Palo Alto Networks notes that while 78 percent of organisations are actively adopting AI, only six percent have the necessary guardrails in place to ensure safe deployment. Prisma AIRS 2.0 is designed to bridge this gap, delivering what the company describes as the industry's most comprehensive end-to-end AI security coverage.

"AI is transforming every enterprise, creating extraordinary opportunities and new risks," said Anand Oswal, Executive Vice President of Network Security at Palo Alto Networks. "Prisma AIRS 2.0 bridges that gap, uniting deep model inspection, real-time agent defence, and continuous red teaming in a single platform."

Prisma AIRS 2.0 connects AI agent and model inspection during development with real-time defence in production, ensuring that all interactions between AI models, data, and users remain protected. The platform employs autonomous red teaming to continuously validate and strengthen enterprise AI defences, enabling organisations to innovate securely at scale.

The new release features three advanced modules designed to deliver visibility, control, and protection across complex AI environments:

- **AI Agent Security:** Provides real-time, in-line defence against prompt injections, tool misuse, and malicious agent behaviour. It also discovers and inventories both sanctioned and "shadow" AI agents to improve governance.
- **AI Red Teaming:** Uses an autonomous, continuous, and context-aware approach to simulate more than 500 types of attacks, helping enterprises detect vulnerabilities before they can be exploited.
- **AI Model Security:** Conducts deep architectural analysis to uncover AI-native threats such as data poisoning and hidden backdoors, while providing a full "bill of materials" for models to support compliance and risk management.

Harshul Joshi, Principal for Cyber, Data & Tech Risk at PwC US, highlighted the urgency of securing generative AI deployments: "The rapid adoption of generative AI is creating a new, complex threat surface for every enterprise. Our strategic alliance with Palo Alto Networks helps clients secure AI through a unified, full-lifecycle approach that's truly secure by design."

Looking ahead, Palo Alto Networks plans to extend its AI innovation strategy to new security domains. The company is developing technologies such as Cortex AgentiX for securing autonomous workforces, enhanced browser security at the endpoint, and defences against emerging computational risks including quantum threats.

By combining advanced AI inspection, automation, and integrated protection, Palo Alto Networks is positioning Prisma AIRS 2.0 as the benchmark for securing enterprise AI. The platform underscores the company's commitment to enabling customers to innovate with confidence in an increasingly AI-driven world.

Anand Oswal, Executive Vice President of Network Security at Palo Alto Networks.

KEYSTRIKE AND BULWARK TECHNOLOGIES PARTNER TO BRING ADVANCED CYBERSECURITY TO THE MIDDLE EAST

Keystrike, an Iceland-headquartered cybersecurity innovator that prevents lateral movement and user impersonation through continuous human-and-device attestation, recently announced a regional distribution partnership with Bulwark Technologies LLC, a leading value-added distributor (VAD) of IT and cybersecurity solutions across the Middle East and India.

Under the agreement, Bulwark will distribute and support Keystrike Core Protector and Keystrike Cloud Protector, two complementary solutions that defend organisations against one of the fastest-growing attack vectors: user impersonation and post-breach lateral movement.

Two products, one unified attestation layer

- Keystrike Core Protector stops lateral movement and user impersonation inside server environments by continuously verifying that every keystroke and command received over SSH or RDP originates physically from an authenticated user and device and not from an adversary.
- Keystrike Cloud Protector extends the same zero-trust attestation to web interfaces and SaaS dashboards, ensuring that web-based administrative and operational portals cannot be hijacked or manipulated by compromised endpoints or through compromised credentials.

Together, these technologies close the gap left by credentials, MFA, and endpoint tools – guaranteeing that every command accepted by a system is genuinely human, verified, and trusted, and all of that without any friction for the users or administrators.

"Bulwark's reputation for introducing high-impact cybersecurity innovations to the region makes them an ideal partner", said Leifur Saemundsson, Regional General Manager, Keystrike MEA. "With Core Protector and Cloud Protector, customers can finally ensure that every command—whether to a server or a browser-based console—comes only from verified, uncompromised users".

"We are delighted to add Keystrike to our next-generation security portfolio", said Jose Menacherry, Managing Director, Bulwark Technologies. "The Keystrike platform brings a completely new defensive layer to organisations striving for zero-trust maturity. It prevents the invisible insider and remote-session risks that conventional tools often miss. The Core Protector detects any attempt of lateral movement to a protected server without any attention from the admin team and protects the servers at the same time, and the Cloud Protector safeguards the user access, even in case the credentials are compromised".

Regional impact

The collaboration enables Bulwark's extensive channel network—spanning the UAE, Saudi Arabia, Qatar, Oman, and India—to offer Keystrike solutions as part of comprehensive managed-security and compliance frameworks. Customers benefit from local implementation expertise, rapid support, and integration with existing SIEM/SOAR systems for high-fidelity incident detection.

NETSCOUT EXTENDS VISIBILITY INTO KUBERNETES CONTAINERS WITH OBSERVABILITY INNOVATION

Helps organisations understand the why behind issues across private and public cloud environments.

NETSCOUT Systems Inc., a leading provider in observability, AIOps, cybersecurity, and DDoS attack protection solutions, has announced an innovation aimed at meeting organisations' increasing needs for comprehensive observability within complex cloud environments. With the ever-growing demands of large, multi-cluster Kubernetes deployments, organisations often face significant challenges related to visibility and blind spots in their environments.

Omnis KlearSight Sensor for Kubernetes (KlearSight) delivers deep, actionable, and real-time insights into system performance, health, and cost drivers. This solution is specifically designed to support dynamic and distributed architectures, environments that are challenging to monitor due to their encrypted nature. KlearSight captures Kubernetes packets and SSL messages directly from the Linux kernel's networking stack after decryption has occurred. It then converts this data into standard IT traffic, enabling visibility into application-layer communications without requiring access to encryption keys. By providing robust visibility into these cloud environments, KlearSight empowers organisations to better manage and optimise their infrastructure, ensuring more reliable and efficient operations.

"Microservices running on a Kubernetes cluster generate multiple metrics, events, logs, and traces to provide some visibility across complex multi-cloud environments," stated Jim Frey, principal analyst, Omdia. "However, searching through telemetry data streams to determine the root cause of an incident can be like searching for multiple needles across multiple haystacks. The ultimate source of truth lies in packets, and organisations can only benefit by establishing this level of visibility enterprise-wide, including the cloud and Kubernetes environments. Time and again, this has proven to be crucial for rapid recognition and diagnosis of performance incidents and issues while also enhancing AI-driven observability."

Phil Gray, AVP, product management, NETSCOUT

Developed from NETSCOUT's expertise in network traffic analysis, deep packet inspection (DPI), and real-time traffic intelligence, KlearSight uses extended Berkeley Packet Filter (eBPF) technology to extract packets from within the Linux kernel's networking stack. It extends and enhances observability to understand system behavior and accelerate troubleshooting and incident response with unprecedented, low-overhead access to granular system and application data. The result is moving beyond monitoring what is happening in the environment towards understanding the why of any issue, including unusual patterns and anomalies, that often go unnoticed.

"NETSCOUT has been delivering innovative observability and visibility solutions that address end-through-end performance challenges for decades," said Phil Gray, AVP, product management, NETSCOUT. "Our solutions are mission-critical to large enterprises across all industries, especially as AI and cloud complexity continue to accelerate."

NETSCOUT's mission is to keep the connected world running by helping customers make smarter, better decisions – faster – to keep them resilient against disruptions of any kind. Our enterprise, service provider, and government agency customers have some of the most complex digital infrastructures in the world, and we partner with leading technology companies to drive customer success. Recently, NETSCOUT was recognised for network observability leadership in the QKS Group's SPARK Matrix: Network Observability, Q3 2025, and was also honored as the recipient of the CRN Tech Innovators award in the Application Performance / Observability category for overcoming remote office observability challenges with cost-effective nGenius Edge Sensors.

MADE IN TAIWAN

4G LTE N300 Wi-Fi Router

G403C

Uninterrupted Connectivity With Peace of Mind

Seamless Connectivity Anywhere: Ideal for Residential, Pop-up Stores, and Events

Easy setup, Cable-free

Anyone can do it.

Insert the SIM card for immediate Internet access with an easy setup.

The G403C is an ideal solution for areas with or without wired Internet, including homes, businesses, events, cottages, and RVs. It offers reliable 4G LTE/3G connectivity with speeds up to 150 Mbps downlink and 50 Mbps uplink.

N300

Wi-Fi Speed up to 300 Mbps

Provide enough bandwidth with Wi-Fi speeds up to 300 Mbps for smooth Internet browsing, email, and social media use.

5dBi

Boosted by 5dBi Antennas

Equipped with 5dBi external antennas to enhance cellular LTE and Wi-Fi signals, ensuring better coverage and performance.

Enhanced Security

Keep your network secure with guest Wi-Fi, WPA3 encryption, and security certifications including EN18031 and IEC 1-4-62443.

D-Link®

Connect to more...

OPSWAT EMPOWERING WOMEN LEADERS TO SHAPE SAUDI ARABIA'S CYBERSECURITY FUTURE

Industry experts explore cybersecurity leadership and resilience and celebrate women's growing impact on the Kingdom's digital future at CyberSHEsec summit.

OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, hosted the inaugural CyberSHEsec: Shaping Cybersecurity with SHE Vision summit, organised by CyberForge Global. The event brought together leading voices to spotlight the crucial role of women in advancing cybersecurity across Saudi Arabia and the wider GCC region. Supported by Women in Cybersecurity Middle East and the Ministry of Health Saudi Arabia, the high-profile event was a celebration of Cybersecurity Awareness Month, dedicated to empowering women and promoting diverse, innovative leadership within the digital security landscape.

Thought leaders, rising professionals, and industry experts from both the public and private sectors exchanged insights on the evolving cybersecurity landscape. Discussions explored the impact of artificial intelligence (AI) on cyber defense, strategies for strengthening national cyber resilience, and approaches to building the cybersecurity workforce of the future. The event also celebrated the growing influence of women in cybersecurity and reaffirmed Saudi Arabia's Vision 2030 and commitment to empowering women, fostering innovation, and shaping a secure, digitally resilient economy.

According to the Saudi Federation for Cybersecurity, Programming and Drones (SAFCSP), women now hold 45% of cybersecurity roles in Saudi Arabia, compared to a global average of approximately 25%. This highlights the Kingdom's leadership in advancing gender diversity in technology and innovation.

Delivering the keynote speech, Raneem Alsalem, Women Empowerment General

Director at the Ministry of Health, underscored the alignment between women's empowerment in cybersecurity and the Kingdom's broader national transformation. "Empowering women in cybersecurity is not only about inclusion, but also about innovation. Under Vision 2030, Saudi Arabia is witnessing a new era when women are not just participants but leaders in building a secure digital future. Platforms such as CyberSHEsec inspire more women to step forward, lead with confidence, and contribute to the Kingdom's growing digital resilience."

As part of OPSWAT's commitment to strengthening critical infrastructure protection (CIP) and nurturing cyber talent in the Kingdom, attendees were also offered complimentary CIP certifications through the OPSWAT Academy, the region's leading training platform for cybersecurity professionals. The program reinforces OPSWAT's mission to advance national cybersecurity capabilities and support Saudi Arabia's strategy to safeguard critical digital assets.

"At OPSWAT, we see innovation and security excellence as inseparable from diversity and empowerment," said Rana Alghrassi, Field & Channel Marketing Manager GCC, OPSWAT. "By hosting CyberSHEsec, we aim to offer a platform for women in cybersecurity to share their experiences, insights, and drive conversations toward a more inclusive and resilient digital future. We continue to champion women's contributions in cybersecurity and provide learning opportunities that equip professionals with the skills needed to protect the Kingdom's critical infrastructure. Our collaboration with CyberForge Global and support from the Ministry of Health emphasise our shared vision for a secure and inclusive digital future."

"Events like CyberSHEsec are crucial in driving dialogue, mentorship, and innovation," said Norah Aldeghaim, Regional Representative at Women in Cyber Security Middle East. "They help us reimagine what leadership in cybersecurity looks like – one that values diversity, collaboration, and continuous learning. By creating spaces where ideas are shared and voices are amplified, CyberSHEsec empowers women to bring fresh perspectives to complex security challenges and contribute meaningfully to national digital transformation efforts."

By connecting industry expertise with national priorities, CyberSHEsec demonstrated the power of collaboration, mentorship, and innovation in shaping the future of cybersecurity in the Kingdom.

black hat
MIDDLE EAST AND AFRICA

2 - 4 DECEMBER 2025
MALHAM, SAUDI ARABIA

CYBERSECURITY'S GLOBAL STAGE

REGISTER FOR YOUR **FREE** PASS TODAY

QUANTUM REALITY CHECK: RACE TO SECURE DATA HAS ALREADY BEGUN

QUANTUMGATE'S JANNE HIRVIMIES WARNS THAT HARVESTED DATA IS ALREADY AT RISK — AND ORGANISATIONS MUST ACCELERATE THEIR POST-QUANTUM READINESS NOW.

Quantum computing is rapidly reshaping the security assumptions that have guided digital infrastructure for decades. The shift to post-quantum cryptography is no longer a distant milestone on global roadmaps; it has become an urgent, multi-year undertaking that many organisations still underestimate.

QuantumGate CTO Janne Hirvimies spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, about the industry's readiness and emphasised that the threat has already started, driven by "Harvest Now, Decrypt Later" tactics where adversaries quietly intercept encrypted data today with the intention of unlocking it once quantum capabilities mature.

Hirvimies highlights the UAE's early national stance on quantum resilience, while underscoring the sheer complexity of replacing cryptographic foundations embedded across applications, devices, protocols, and critical infrastructure. For leaders, he argues, the challenge is not only technical but cultural — requiring crypto agility, long-term planning, and collaboration across hardware ecosystems, cloud platforms, regulators, and service operators.

You've often spoken about the illusion of time in cybersecurity transformation. Why do you believe the timelines many organisations set for quantum migration are dangerously optimistic?

Many organisations take comfort in dates like 2030 or 2035 that appear in global post-quantum roadmaps. The set timelines often create the impression that there is still room to wait and that the risk is far away. The threat, however, does not begin when quantum computers become fully capable. It begins the moment attackers start harvesting

Janne Hirvimies
CTO
QuantumGate

encrypted data with the intention of decrypting it in the future. That is already happening today, which means time is not on our side.

Another misconception is how long migration actually takes. Moving to post-quantum cryptography is a multi-year transformation that affects applications, devices, protocols, and long-lived data. Even the first step, which is identifying where cryptography is used across an environment, can take six to eight months in a large organisation. During crypto discovery, we often uncover what teams describe as "shadow cryptography" — keys, certificates, and embedded mechanisms organisations did not know existed. This hidden complexity is what turns long timelines into urgent ones.

The UAE recognised this early and through the UAE Cybersecurity Council (CSC) the country set a clear path for quantum readiness and highlighted the importance of sovereign, in-country cryptographic capabilities. Protecting long-lasting national data depends on keeping algorithms, libraries, and key management under national oversight and aligned with the country's cybersecurity strategy. The real illusion of time is not only the calendar date. It is the assumption that change can happen quickly.

Many organisations still treat post-quantum readiness as a future concern. How would you convince leaders that the "Harvest Now, Decrypt Later" threat is already real and needs immediate attention?

The most effective way to show leaders that this threat is real is to focus on the data itself. Encrypted information that needs long-term protection is already exposed. Government records, healthcare files, financial histories, intellectual property and research data often require confidentiality that lasts for many years. Once any of this information is intercepted and stored by an adversary, it remains vulnerable until quantum computers can break the public key algorithms that protect it, such as RSA and ECC.

Data stays vulnerable for as long as it relies on today's public key encryption standards. If confidential information is being shared or transmitted, there is a real risk it can be harvested. Once this happens, control over that data is lost, and an adversary can simply wait until quantum computers allow them to decrypt it.

This is the reality behind Harvest Now Decrypt Later. Attackers do not need quantum computers today; they only need access to the data, for instance, while it is moving across networks or through compromised infrastructure. The moment it is collected, the exposure begins.

MOVING TO POST-QUANTUM CRYPTOGRAPHY IS A MULTI-YEAR TRANSFORMATION THAT AFFECTS APPLICATIONS, DEVICES, PROTOCOLS, AND LONG-LIVED DATA.

From your two decades in hardware-based mobile security, how do you see the evolution of cryptographic systems that are now deeply embedded across devices — and why does that make migration so complex?

For nearly fifty years, the cryptography we rely on has remained stable. The same public key foundations became the basis for authentication, secure access, and digital transactions. Updates happened over time, such as increasing key lengths or retiring from individual algorithms, but they were gradual. The overall trust model remained unchanged.

Because of this long period of stability, public key cryptography is built into every layer of modern infrastructure and into the mechanisms that secure how systems operate. It underpins how devices exchange data, how certificates function, and how digital trust is established across mobile, cloud, IoT and industrial environments. This model has served as the bedrock of security for decades.

The challenge now is that the entire foundation of public key cryptography needs to change. Post-quantum algorithms introduce new ways of establishing keys and creating signatures, and this affects every system that relies on the existing PKI model. Since the same approach has been adopted everywhere for forty years, the migration is complex. We are updating the base layer that everything else depends on.

What are the biggest misconceptions enterprises hold about the speed at which they can transition to quantum-safe systems?

One major misconception is the idea that moving to quantum-safe systems is similar to a routine software update. The change goes much deeper. It affects software libraries, communication protocols, embedded code, and often the hard-coded algorithms inside legacy

ATTACKERS DO NOT NEED QUANTUM COMPUTERS TODAY, THEY ONLY NEED ACCESS TO THE DATA, FOR INSTANCE WHILE IT IS MOVING ACROSS NETWORKS OR THROUGH COMPROMISED INFRASTRUCTURE.

hardware. Many of these components were never designed for rapid replacement.

Another misconception is the belief that organisations can wait for mandates or off-the-shelf solutions before taking action. When everyone begins at the same time, pressure builds across the entire ecosystem. Suppliers become overwhelmed, costs rise, and there is little space for careful testing or phased rollout. Starting early is what prevents that bottleneck.

There is also the assumption that migration fits into a short project window. In practice, this work spans years. Before any upgrade can happen, organisations need a full picture of where cryptography sits across their environment, which can take many months. Only then can they prioritise, test, integrate, and gradually cut over to new quantum safe mechanisms. Fault-tolerant quantum computers are still in development, but progress is accelerating, and the timelines are tightening.

QuantumGate positions itself at the frontier of secure communication and applied cryptography. What role do secure hardware platforms and key-management innovation play in accelerating quantum migration?

Secure hardware and key management are both important in quantum safe migration, but neither is a one-size-fits-all approach. Each addresses different parts of the problem. Hardware anchored keys provide strong assurance for high value assets, yet they also come with cost, operational complexity and long replacement cycles. If a migration depends only on hardware, these factors can slow progress across the wider environment.

This is where key-management innovation becomes essential. Post-quantum migration increases the number and types of keys organisations must handle, and in many cases quantum-safe keys can be deployed directly to devices like mobile phones, providing strong

security without the expense of dedicated hardware.

Sovereign capability also matters for leaders responsible for national or critical infrastructure. In the UAE, the Technology Innovation Institute's (TII) cryptographic libraries provide an in-country, certified foundation that integrates with both secure hardware platforms and large-scale key management systems. This gives organisations a clear path that matches national requirements.

In practice, secure hardware and modern key management work best together. The right combination supports quantum safe adoption in a way that is practical, secure, and aligned with the realities of each environment.

You've led security architecture development across global chipset and mobile ecosystems. How can industry-wide collaboration shorten the pilot-to-production cycle for quantum-resistant solutions?

Industry-wide collaboration is not just helpful for quantum migration, but essential. Cryptographic systems only work when they are interoperable, meaning devices, platforms, certificate authorities, and communication protocols must support the new algorithms in a consistent way. If one layer lags, the entire chain slows.

Standards bodies such as NIST and ETSI define the algorithms, but real progress happens when hardware makers, cloud providers, software developers, regulators and service operators test and validate these changes together. Shared pilots reveal performance characteristics, integration issues, and interoperability gaps early, which prevents costly rework later. Collaboration does more than shorten timelines. It makes the transition possible.

ORGANISATIONS THAT ACT NOW WILL STRENGTHEN THEIR FOUNDATIONS, PROTECT LONG-LIVED DATA, REPLACE DEPRECATED CRYPTOGRAPHY, AND BUILD THE CRYPTO AGILITY TO ADOPT FUTURE ALGORITHMS.

Beyond technology, what cultural or organisational inertia prevents decision-makers from acting faster on quantum resilience — and how can this mindset be shifted?

Many decision-makers still assume they have time or believe the threat is too distant to compete with more immediate priorities. This creates a kind of scope blindness. When leaders underestimate how deeply cryptography is woven into their infrastructure, they plan a small fix instead of recognising the scale of the modernisation required.

Another challenge is the perception that cryptography is stable and slow-moving. That was true for decades, but the field is evolving quickly. Algorithms, standards, and best practices are shifting faster than before, which means organisations need crypto agility, the ability to adopt new algorithms and key-management approaches as they emerge. Post-quantum migration should be viewed not only as a security requirement but also as an opportunity to replace deprecated cryptographic assets.

Shifting this mindset is largely an educational effort. This is why we place so much emphasis on awareness and guided planning. Once leaders understand that their cryptographic foundations and key-management systems are long-term assets that must remain adaptable, the conversation changes. It moves from "Do we need to do this now?" to "How do we build the agility to stay ahead as the standards evolve?"

Looking ahead to 2030, do you think we'll view this decade as the period when industry leaders responded wisely to the quantum threat, or as the time we lost to the comfort of the calendar?

It is still a choice. We already have enough clarity to act. The leading post-quantum algorithms have been selected, migration guidance is maturing, and hybrid paths allow organisations to move safely as the ecosystem evolves. Many countries are beginning to set expectations, and the UAE has been among the first to place post-quantum resilience on the national agenda through the Cyber Security Council. That direction signals where the world is heading, and those who begin early will navigate the transition more smoothly. The organisations that use this decade well will treat PQC as a chance to strengthen their foundations. They will protect long-lived data, replace deprecated cryptography, modernise key-management, and build the crypto agility needed to adopt new algorithms as standards continue to develop. Those who start discovery now, pilot next, and move into hybrid deployments after that will look back on the 2020s as the period they prepared with intention rather than urgency. Those who wait will still do the same work, but under pressure.

FAULT-TOLERANT QUANTUM COMPUTERS ARE STILL IN DEVELOPMENT, BUT PROGRESS IS ACCELERATING, AND THE TIMELINES ARE TIGHTENING.

LINKSHADOW®

CYBERMESHX PLATFORM

UNIFY YOUR ENTIRE SECURITY UNIVERSE

ONE PLATFORM, TOTAL CONTROL

black hat
MIDDLE EAST AND AFRICA
2 - 4 DEC 2025
Exhibition Centre, Malham - KSA

HALL 1,
STAND #H1-H20

E: info@linkshadow.com
T: +1 877 267 7313
W: linkshadow.com

Security ADVISOR MIDDLE EAST

SPECIAL REPORT

LINKSHADOW

FADI SHARAF EL-DEAN, CHIEF REVENUE OFFICER, LINKSHADOW

CyberMeshX: Unifying Security Architecture for AI-First Era

The relentless march of digital transformation has simultaneously expanded the attack surface and fragmented the tools used to defend it. Today, organisations face increasingly complex and decentralised environments, and the need for a unified security foundation has never been more urgent.

LinkShadow's CyberMeshX Platform is built to simplify modern defence by bringing identity, data, and network visibility together into a single, connected security layer. The unified platform provides clearer insights, faster detection, and stronger, adaptive protection. The platform aims to remove complexity, connect every part of the security ecosystem, and deliver a more intelligent, coordinated response to today's threats.

Fadi Sharaf, Chief Revenue Officer, LinkShadow, said: "AI is no longer an enhancement; it is the core of modern cyber resilience. With CyberMeshX, we have created a unified security foundation that is simple, intelligent, and built to help organisations stay ahead of increasingly sophisticated threats."

LINKSHADOW®

black hat
MIDDLE EAST AND AFRICA

Architecting Resilience with CSMA

Inside CyberMeshX: A Future-Proof Security Architecture Approach

Modern enterprises are navigating an environment where threats evolve faster than traditional security layers can respond. Fragmented tools create blind spots, slow down investigations, and increase operational overhead. A unified architecture is now essential — not optional — for businesses seeking clarity, speed, and resilience across their digital ecosystems.

Welcome to Black Hat MEA 2025. This year marks a turning point where organisations must shift from isolated defence components to a cohesive, integrated security model.

LinkShadow's CyberMeshX Platform is built on our AI-driven Cyber Mesh Architecture, unifying identity, data, and network defence into one intelligent layer. The result is complete visibility, stronger contextual intelligenc,e and predictive defence capabilities that scale with modern business demands.

We believe true security comes from connecting every component clearly, intelligently, and instantly. This is why we are proud to introduce MeshConnectX, the breakthrough that enables immediate, zero-code integration across the enterprise.

TRUE SECURITY COMES FROM CONNECTING EVERY COMPONENT CLEARLY, INTELLIGENTLY, AND INSTANTLY.

The LinkShadow Journey

The Journey to CyberMeshX

Founded in 2015, LinkShadow began with a vision centred on proactive threat intelligence and Network Detection and Response (NDR). Recognising the limitations of reactive security models, the company invested heavily in AI analytics and modular cybersecurity. By 2023, the brand expanded beyond NDR to incorporate Identity Threat Detection and Response (ITDR) and Data Security Posture Management (DSPM), paving the way for the CyberMeshX Platform.

Today, through CyberMeshX and the transformative MeshConnectX module, LinkShadow maintains a global presence across the Middle East, Europe, and North America—delivering the future of unified defence.

Milestones That Matter

2015: Founding vision with a focus on real-time Network Detection
2023: Strategic expansion with DSPM
2024: Major milestone with the introduction of ITDR
2025: Launch of CyberMeshX — the unified, AI-driven security platform
2025 (Black Hat MEA 2025): Introduction of MeshConnectX — pioneering zero-code integration

Product Deep Dive

Inside CyberMeshX: A Future-Proof Security Architecture Approach

The battle against sophisticated threats and disjointed security systems ends here. CyberMeshX is more than a SIEM or XDR platform — it is a holistic security ecosystem transforming raw signals into a coherent security narrative.

"Security teams spend long hours managing complex integrations requiring heavy coding. MeshConnectX removes that burden and allows teams to connect any tool or technology within CyberMeshX instantly", said Fadi Sharaf.

Built on Gartner's Cybersecurity Mesh Architecture (CSMA):
CyberMeshX ensures security policies are consistently distributed and enforced across cloud, endpoints, and identity layers.

Unified Visibility and Action:
Identity, Data, and Network signals converge into a single investigation plane, enabling analysts to view the entire attack storyline—from credential compromise to data exfiltration.

CYBERMESHX TURNS FRAGMENTATION INTO COHESION, EMPOWERING ENTERPRISES TO EVOLVE AT THE SPEED OF THREATS. WITH MESHCONNECTX, THE END OF SECURITY SILOS IS TRULY HERE.

MeshConnectX for Seamless Integration:
MeshConnectX makes complex integrations effortless. It is the zero-code gateway to immediate, enterprise-wide resilience.

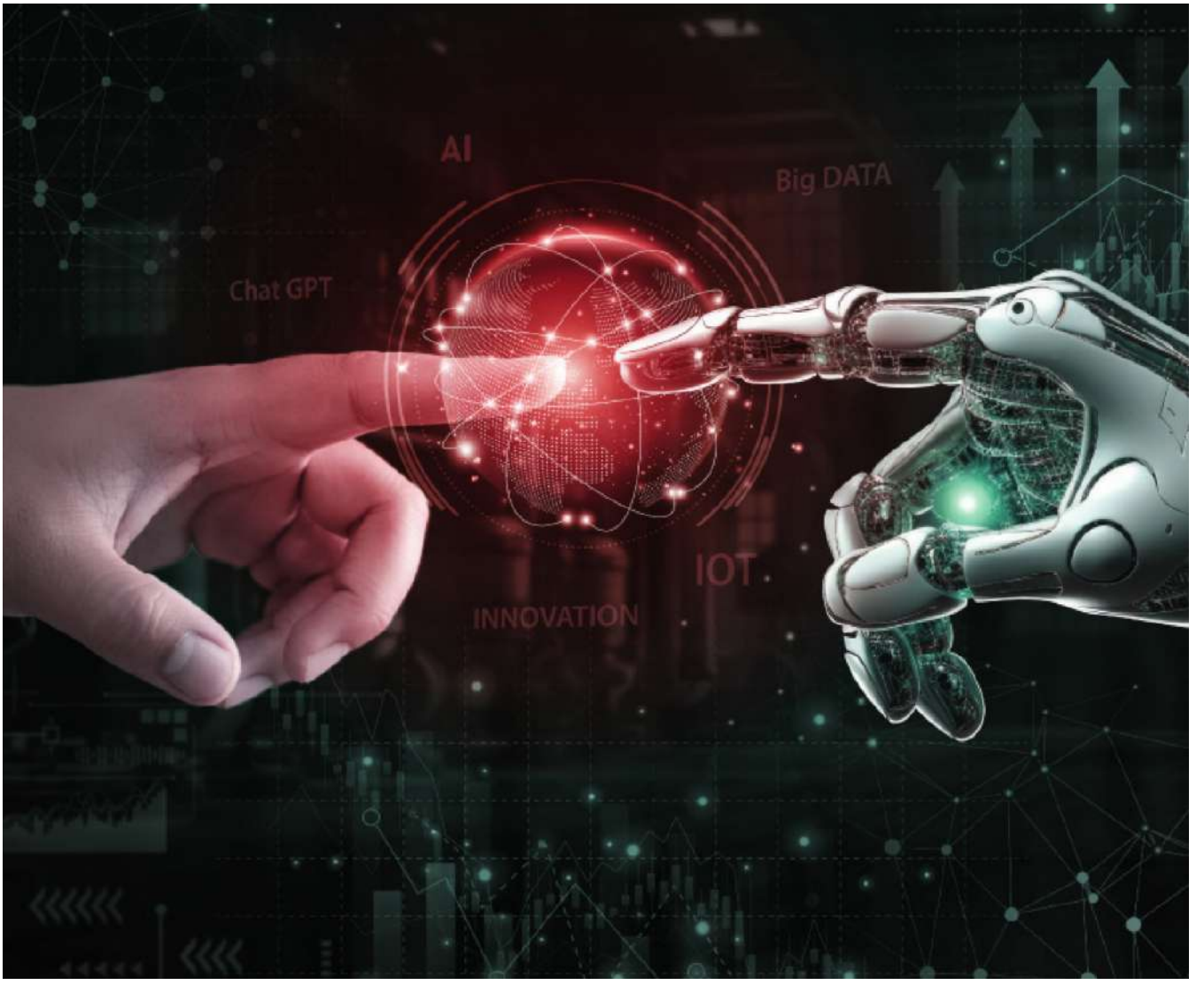
AI-Driven Contextual Intelligence:
Every detection is backed by Explainable AI, presenting clear rationale, mapped evidence and MITRE-aligned context. False positives fall dramatically, restoring confidence across security teams.

AI Shapes into New Cyber Command Centre

Artificial intelligence is no longer a peripheral feature; it is the central nervous system of modern security operations. Defenders must rely on AI to automate detection, prediction, and adaptive response as adversaries weaponise AI to automate attacks.

Within CyberMeshX, AI progresses far beyond anomaly detection as it acts like an autonomous orchestration layer, continuously learning and adapting. By correlating Identity, Data and Network signals, LinkShadow's AI reduces bias, minimises noise, and drastically cuts investigation time. Analysts are freed from tactical firefighting and empowered to focus on strategic defence.

This is LinkShadow's leadership in AI-native cybersecurity.



KSA Vision Feature

Empowering Digital Future: LinkShadow Catalyses Cyber Resilience

Saudi Arabia's Vision 2030 sets ambitious goals for digital transformation, making cybersecurity a national priority. LinkShadow is fully committed to supporting this vision.

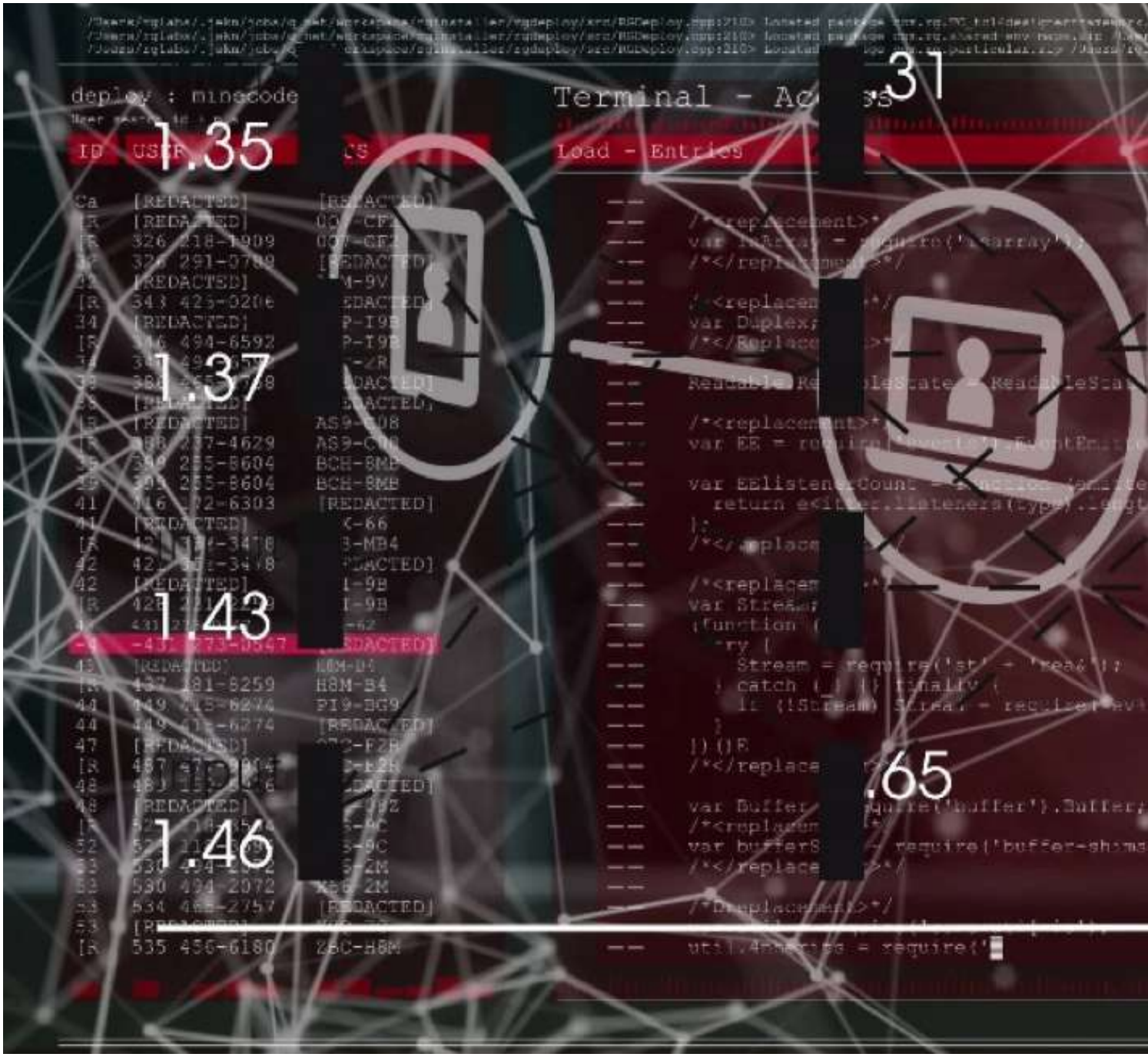
CyberMeshX is engineered to align with the stringent requirements of the National Cybersecurity Authority (NCA) and ensure data sovereignty across critical sectors. LinkShadow is developing local partnerships, R&D collaborations, and talent-development initiatives tailored to the Kingdom's needs.

By offering unified visibility and explainable AI across hybrid and multi-cloud environments, LinkShadow serves as a key enabler of KSA's cybersecurity growth and digital resilience.

WE SEE SAUDI ARABIA AS A GLOBAL CYBERSECURITY POWERHOUSE, AND LINKSHADOW INTENDS TO BE PART OF THAT JOURNEY, PROVIDING THE FOUNDATIONAL TECHNOLOGY FOR DIGITAL SOVEREIGNTY.

Case Studies / Customer Success

Unified Defence in Action: Real-World Success with CyberMeshX



Case 1: Telecom — 60% Faster Threat Detection
A major telecom provider transformed its operations by leveraging multi-tool Security Signals, advanced Incident Prioritisation, and AI/ML threat detection models. By unifying data streams, the organisation achieved 60% faster threat detection, reduced noise, and strengthened its resilience.

Case 2: BFSI — 40% Reduction in Alert Fatigue
A leading BFSI enterprise consolidated alerts and correlated Data and Network Security events to achieve a 40% reduction in alert fatigue. Analysts shifted their focus to high-risk threats, vastly improving response effectiveness.

Case 3: Government — Unified Visibility Across Hybrid Clouds
A government agency deployed CyberMeshX across on-premise and multi-cloud environments. By unifying Identity, Data, and Network layers, the agency achieved comprehensive visibility, streamlined investigations, and significantly enhanced governance.

Partner & Ecosystem Story

Building the Cyber Mesh Ecosystem: Partners in Progress

LinkShadow recognises that a connected ecosystem forms the strongest line of defence. Our API-first design—simplified by MeshConnectX—enables seamless integration with SIEM, SOAR, CASB, firewall solutions, and beyond.

Our partner-enablement strategy empowers Managed Security Service Providers and value-added distributors to deliver CyberMeshX's unified capabilities. This approach helps organisations maximise their existing investments while avoiding restrictive vendor lock-ins.

A CONNECTED ECOSYSTEM IS THE STRONGEST FORM OF DEFENCE. OUR PARTNERS ARE ESSENTIAL IN DELIVERING THE UNIFIED INTELLIGENCE OUR CUSTOMERS DEMAND.

The State of Cybersecurity in the Middle East 2025

The Middle East is undergoing a transformational shift. Rapid cloud migration, 5G deployment, and national digital programmes have heightened exposure to nation-state-level threats. Key trends include:

- Identity emerging as the primary perimeter
- Convergence of OT and IT security
- Increasing demands for data residency and sovereignty (UAE PDPL, KSA compliance regimes)

CISOs now require platforms that support continuous compliance and deep visibility. The Cyber Mesh framework is fast becoming the regional standard—transforming cybersecurity from periodic assessment to a continuous state of operational assurance.

Top 5 Trends Shaping GCC Cybersecurity

- Identity-Centric Attacks
- Data Sovereignty & Residency Mandates
- IT/OT Security Convergence
- Adoption of AI-Native Defence Platforms
- Zero Trust Architecture Deployment

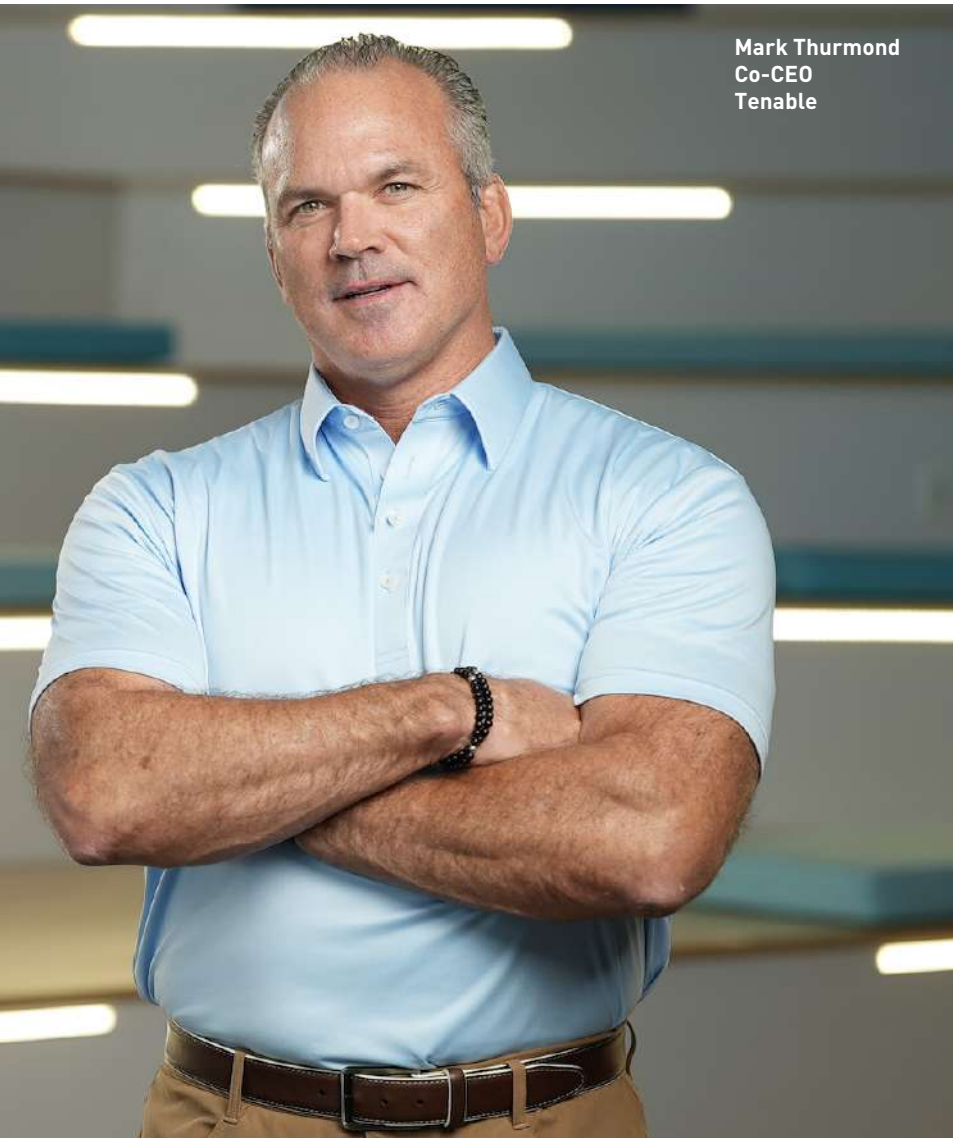
Step Into the Next Era of Cyber Resilience

Join the Mesh: Experience the Future of Adaptive Security

Resilience is not achieved overnight; it emerges through vision, collaboration and AI at the centre of every security decision. LinkShadow is aligned with the region's mandate to stay ahead of AI-powered adversaries. CyberMeshX—supercharged with the zero-code integration power of MeshConnectX—is ready to become the decision-intelligence layer of your SOC.

CYBER RESILIENCE IS NOT BUILT OVERNIGHT; IT IS BUILT WITH VISION, COLLABORATION, AND AI AT THE CORE. WE INVITE YOU TO EXPERIENCE THE MESH.

Visit the LinkShadow booth at Black Hat MEA 2025
Scan the QR code for a personalised product demonstration.
Follow us on all social platforms or contact our regional team.



Mark Thurmond
Co-CEO
Tenable

REDEFINING CYBER RESILIENCE: EXPOSURE MANAGEMENT POWERS PRE-EMPTIVE SECURITY ERA

TENABLE'S CO-CEO, **MARK THURMOND**, EXPLAINS HOW EXPOSURE MANAGEMENT IS HELPING ENTERPRISES – FROM SAUDI GIGA-PROJECTS TO GLOBAL CORPORATIONS – MOVE FROM REACTIVE DEFENCES TO PROACTIVE, AI-DRIVEN CYBERSECURITY.

Cyberattacks are evolving at machine speed, fuelled by advances in artificial intelligence and automation, leaving traditional defence models struggling to keep up. Mark Thurmond, Co-CEO of Tenable, spoke to Sandhya D'Mello, Technology Editor of CPI Media Group, on how organisations must move beyond reactive measures toward a pre-emptive approach rooted in exposure management — a framework that unifies visibility, prioritises critical risks, and empowers leadership to act decisively.

Thurmond explores how this new discipline is transforming cybersecurity strategy across global enterprises and enabling the Middle East's digital vision, from Saudi Arabia's giga-projects to the UAE's rapidly advancing innovation economy.

How is exposure management transforming the way global and regional enterprises think about cybersecurity at a business level, especially in the age of AI and automation?

Exposure management is driving a fundamental shift from the outdated, reactive cybersecurity playbook of the past two decades to a pre-emptive, business-aligned approach. In the age of AI, where attack timelines are reduced from weeks to minutes, the process of manually analysing and responding to threats is a "simple math problem" that human teams cannot win.

An exposure management program provides a "master blueprint" to identify, assess, and reduce cyber risk across an exploding digital attack surface. By unifying siloed teams, tools, and data, it allows leadership to move from collecting spreadsheets to confidently answering the question, "Are we exposed?" with a data-backed answer. At a business level, this provides laser focus, allowing teams to prioritise the few critical exposures, typically just 3% of known vulnerabilities, that attackers are using AI to target so actually expose an organisation to risk. This approach effectively fireproofs the organisation rather than leaving them firefighting.

Traditional defense models are proving insufficient in today's interconnected digital world. From your perspective, what new mindset or operating model should CISOs and CEOs adopt to stay ahead of modern threats?

The traditional defense model is fragmented, with organisations deploying an average of 83 different cybersecurity tools from up to 29 different vendors. This fragmented approach creates "disconnected silos" that give attackers a major advantage.

The new exposure management operating model shifts mindset to a proactive, pre-emptive security posture, built for unified visibility and action. Exposure management acts like an elite football manager, commanding the sideline and seeing the entire field to ensure all specialised teams are positioned to work as a unified front. It moves security from a system of record to a system of action, leveraging AI to see risk the same way attackers do by connecting the dots to show how a breach could occur and forecasting the likelihood of an attack. This enables teams to reduce risk proactively and eliminate it before it emerges.

Saudi Arabia's giga-projects, such as NEOM and The Line, are setting new global benchmarks for smart, connected infrastructure. How does Tenable see its role in helping build the cybersecurity foundations that will sustain these ambitious digital ecosystems?

Saudi Arabia's giga-projects, like NEOM, will involve billions of connected physical devices and sprawling IoT networks, creating a highly complex digital ecosystem. For projects of this scale, Tenable views its role as providing the essential cybersecurity foundations for survival.

The goal is to provide a "master blueprint" for this digital complexity, ensuring the infrastructure doesn't run blind. The unique challenges include not only security but also complying with visionary frameworks like PDPL and the NCA's Essential Cybersecurity Controls, which rightfully demand to know exactly where data is and how it is governed.

Tenable's Exposure Management platform offers unified visibility of every asset and exposure, transforming the complex digital landscape into an understandable, manageable security posture. This unified, pre-emptive approach ensures that ambition on this scale is protected against the inevitable new opportunities for cyber criminals.

AI is now both a powerful defense tool and a source of new attack surfaces. How is Tenable leveraging AI to help organisations anticipate, prioritise and mitigate emerging risks?

AI is a critical third force that exploits weaknesses at "super speed and scale." With AI-driven attacks hitting 87% of organisations last year, Tenable's core strategy is to fight AI with AI. Tenable's exposure management platform is fundamentally AI-powered, which is key to anticipating, prioritising, and mitigating emerging risks.

AI enables the platform to prioritise by seeing risk the same way attackers do, connecting the dots to show how an organisation could be breached, and forecasting that an attack might come in a specific timeframe. For mitigation, AI evolves the platform into a self-driving system that automatically handles routine tasks. It can check if a patch is available for a critical vulnerability, open a remediation ticket, and schedule a follow-up scan in minutes or seconds, freeing human teams from the manual process that AI adversaries would overwhelm.

Given the substantial investments in digital transformation across the Middle East under Vision 2030, what additional measures can be implemented by both the private sector and governmental bodies to cultivate enhanced cyber resilience and robust local talent pipelines?

Saudi Arabia's Vision 2030 is a bold declaration about the future, underpinned by a rich ecosystem of technology collaborations. To build stronger cyber resilience, both industry and government must move beyond an outdated security playbook that no longer works.

The imperative is to show up as a unified front and adopt the pre-emptive discipline of Exposure Management. This starts with building cybersecurity foundations that focus on unified visibility and reducing risk proactively, rather than simply reacting to alerts. For local talent, it's essential to recognise that human teams cannot manually keep pace with threats executed by AI at machine speed. Therefore, industry and government must invest in AI-powered tools that automate routine tasks, like finding patches and opening tickets to level the playing field, empowering cybersecurity professionals to focus on the strategic reduction of the most critical risks.

How do you see Saudi Arabia's and the UAE's approach to digital innovation influencing cybersecurity priorities across the wider region?

Saudi Arabia's ambitious, forward-thinking leadership and national transformation under Vision 2030 have made it a global symbol of ambition and innovation. This level of digital transformation, including groundbreaking ventures like the AI Zone built by HUMAIN and AWS, introduces a massive digital attack surface that requires a new level of protection.

This bold approach directly influences regional cybersecurity priorities by demonstrating that innovation on a grand scale brings new challenges that cannot be solved with old methods. Frameworks like Saudi's PDPL and the NCA's Essential Cybersecurity Controls rightfully raise the global standard by demanding clear data sovereignty and governance. The required response, the adoption of a pre-emptive, AI-powered discipline like exposure management to see risk clearly and act on it, becomes the necessary blueprint for any nation or enterprise in the region seeking to secure its bold, prosperous future.

SENTINELONE TO SHOWCASE AI SECURITY LEADERSHIP AT BLACK HAT MEA 2025

THE COMPANY WILL PRESENT AI-NATIVE CYBERSECURITY CAPABILITIES TO POWER AUTONOMOUS SECURITY OPERATIONS, THE MORTAL VS MACHINE COMPETITION, AND SHARE INSIGHTS ON ACCELERATING AND DERISKING AI ADOPTION.

SentinelOne, the leader in AI-native cybersecurity, has announced its participation at Black Hat Middle East and Africa 2025, which will be held from December 2 to 4 in Riyadh. The company will highlight how its Singularity Platform enables secure and swift innovation in the AI era. This is made possible by bringing together endpoint, identity, cloud and data security into a single autonomous ecosystem. The company's presence aims to support regional enterprises by strengthening their security posture as they accelerate digital transformation and adopt advanced technologies.

A key attraction this year will be Mortal vs Machine, a live threat-hunting competition that places human analysts against SentinelOne's agentic AI in real-time incident response scenarios. The activation will demonstrate the way speed, precision, and automation can transform security outcomes and will take place daily from 12:30 PM to 12:50 PM at the event.

SentinelOne will present interactive demonstrations, platform showcases and expert-led engagements to support organisations in enhancing visibility and reducing risk. It will also help them adopt AI-driven cyber defense confidently. Throughout the exhibition, SentinelOne's leaders will host focused sessions on the future of enterprise security in the age of AI. On December 2nd, Abdulkareem Abuihlayel, Senior Solutions Engineer, will speak on "Beyond the Endpoint: AI-Driven Endpoint and Identity Security". On December 3rd, Ibrahim Karam, Senior Solutions Engineer, will present "The Rise of AI SIEM: Hyperautomation for Cyber Defense". On December 4th, Abdulkareem Abuihlayel will return with a session titled "The Power of One: Unifying Endpoint, Identity, Cloud and Data with AI". The sessions will offer practical insights into strengthening cyber resilience through unified intelligence, deep visibility and autonomous response.

"The Middle East is entering a new era of digital acceleration, and AI is at the heart of every major transformation initiative," says Meriam ElOuazzani, Regional Senior Director, Middle East, Turkey, and Africa, at SentinelOne. "SentinelOne's mission is to help organisations embrace this shift without compromising security. Our Singularity Platform gives enterprises a unified and autonomous foundation that protects every layer of the environment and enables teams to stay ahead of emerging threats. Black Hat MEA is a platform for us to empower regional businesses with the tools and insights they require to enhance resilience in a rapidly changing digital environment."

As organisations across the Middle East increase their adoption of Generative AI, cloud-first strategies and modern identity architectures, there has been a significant demand for unified and autonomous security. SentinelOne's Singularity Platform addresses this need by delivering integrated protection across the entire enterprise environment. The platform helps security teams by preventing, detecting and responding to threats quickly and with clarity while bringing down operational complexity.

Visitors can find the SentinelOne booth at Hall 1, Stand U121, to experience the company's AI-native solutions, meet regional experts, and participate in the Mortal vs Machine competition.

THE MIDDLE EAST IS ENTERING A NEW ERA OF DIGITAL ACCELERATION, AND AI IS AT THE HEART OF EVERY MAJOR TRANSFORMATION INITIATIVE

Meriam ElOuazzani
Regional Senior Director, Middle East, Turkey, and Africa
SentinelOne.

DELINEA STRENGTHENS IDENTITY SECURITY WITH AI-POWERED INNOVATION AND REGIONAL COMMITMENT

ART GILLILAND, CEO OF DELINEA, DISCUSSES AT GITEX GLOBAL 2025 HOW THE COMPANY'S AI-INFUSED PLATFORM AND INTUITIVE DESIGN ARE REDEFINING IDENTITY SECURITY, ENHANCING AUTOMATION, AND EMPOWERING ORGANISATIONS ACROSS THE MIDDLE EAST.

Delinea, a global leader in privileged access management and identity security, is helping organisations simplify and secure access across complex hybrid environments. The global brand's cloud-native platform enables administrators to centralise control over human and machine credentials, ensuring consistent policies and visibility across on-premises, SaaS, and cloud systems. In an exclusive conversation with Mark Forker, Editor – Technology Division, Art Gilliland, CEO of Delinea, discussed how the company is integrating AI-driven innovation through its Iris AI capability to enhance automation, authorisation, and user experience. Gilliland also highlighted Delinea's commitment to the Middle East, where digital transformation and AI adoption are accelerating the need for intuitive, scalable identity security solutions.

How does the Delinea platform help organisations centralise and secure identity and access management across hybrid environments?

Delinea was formed about four years ago through the merger of a few different businesses, each bringing unique products. Our focus is on identity security—specifically, how companies decide which privileges or rights to give their users, whether those users are human or machine identities. The Delinea platform provides security administrators with a centralised way to manage and control these credentials across different environments—on-premises, in the cloud, or within SaaS platforms. Essentially, it gives them visibility and consistent policy enforcement, ensuring secure access management across the organisation.

How does Delinea enable administrators to gain full visibility and control over both human and machine credentials across the organisation?

The first challenge most companies face is understanding how many credentials are in use and where they are. With AI and automation tools, users often create new agents or applications and feed in their credentials without full oversight. Our platform helps administrators identify all those credentials—both human and non-human—showing where and how they're used. Once that visibility is achieved, administrators can centralise control and apply consistent security policies to reduce risks and prevent unauthorised access.

The Iris AI capability has generated a lot of attention. Can you explain what it does and how it adds intelligence to the Delinea platform?

Iris AI brings together a set of AI-driven features under one umbrella. Broadly, it operates in two key areas. The first is embedding AI directly into the platform to enhance user experience and automation. For example, our "Delinea Expert" tool works like a ChatGPT-style assistant, trained exclusively on Delinea's product documentation and support articles. Customers can ask questions, upload log files, or request scripts for integrations. Since its launch, we've seen support requests drop by 60%—a huge win for both customers and our support teams. The second area involves intelligent authorisation. Using contextual data such as support tickets, timing, and risk factors, Iris AI helps determine whether to grant or deny access requests. It automates much


Art Gilliland
CEO
Delinea.
Delinea
Securing identities at every interaction
We futureproof identity security
Enterprise-grade, cloud-native architecture
30 minutes code to production
Quantum-safe encryption
Hundreds of integrations

of this process, saving administrators from decision fatigue and helping ensure more accurate, consistent authorisation decisions.

How do you ensure the platform remains intuitive for users who may not be highly technical?
Ease of use has always been central to our philosophy. We started by serving smaller companies with limited IT resources, so our products had to be powerful yet simple and intuitive. Over time, as our platform evolved, larger enterprises began adopting it because they also value usability. Even in big organisations, staff turnover and skill gaps make intuitive design essential. By keeping our interface user-friendly, we lower the cost of ownership and reduce the time needed for training and onboarding—benefiting customers of all sizes.

Cyber threats are constantly evolving, especially with AI accelerating the pace of attacks. What trends or challenges are you seeing now in identity security?
AI is absolutely reshaping the threat landscape. Adversaries can move faster, automate attacks, and exploit vulnerabilities more efficiently. There's an inherent imbalance—attackers operate for profit and can reinvest quickly, while defenders have limited budgets and must get it right every time. One of the most striking trends we're seeing is that around 13% of zero-day vulnerabilities are now linked to identity. Attackers find it cheaper and easier to log in than to break in. Once inside with valid credentials, they become invisible to many detection systems. That's why identity has become the new front line in cybersecurity, and why we're doubling down on securing it.

How do these challenges manifest differently in the Middle East compared to other regions?
The Middle East is investing heavily in digital infrastructure and AI-driven transformation. However, access to local AI tooling and data centres can be more limited compared to markets like the US. Many organisations here are focused on ensuring data sovereignty, which sometimes restricts their use of global AI services. This makes local modernisation efforts—such as building regional AI capabilities—especially critical. The governments in the region are making strong strides in that direction, which is helping organisations strengthen their overall cybersecurity posture.

IDENTITY HAS BECOME THE NEW FRONT LINE IN CYBERSECURITY, AND WE'RE DOUBLING DOWN ON SECURING IT.

Finally, what was Delinea's focus at GITEX Global 2025 this year?
GITEX Global was massive, inspiring to see how much innovation is happening here. For us, the event served two main purposes. Firstly, it's about reaffirming our commitment to the region through ongoing investment and engagement. Secondly, it's an invaluable opportunity to meet with existing customers and partners, understand their evolving challenges, and explore how we can support them further. We also connected with potential new customers who want to learn more about our platform. It's a great environment to deepen relationships and strengthen our footprint in the Middle East.

معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC GLOBAL

05 - 07 MAY 2026

DUBAI EXHIBITION CENTRE (DEC), EXPO CITY

HOSTED BY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY

وزارة الداخلية
MINISTRY OF INTERIOR

شرطة دبي
DUBAI POLICE

MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE

ENQUIRE FOR 2026!

#gisecglobal

gisec@dwtc.com

OFFICIAL DISTRIBUTION PARTNER

SPIRE

LEAD STRATEGIC PARTNER

HUAWEI

STRATEGIC PARTNER

Microsoft aws

DIAMOND SPONSOR

CHECK POINT OPSWAT.

PLATINUM SPONSOR

cisco DREAM

GOLD SPONSOR

1Password CPX CLOUDFLARE CROWDSTRIKE Google Cloud Security

GOLD SPONSOR

emt sig PENTERA kaspersky SECTIGO MENLO SECURITY Trellix

SOPHOS HIGHLIGHTS AI-ERA THREATS AND HUMAN RESILIENCE IN CYBERSECURITY

AT GITEX GLOBAL 2025, SOPHOS UNDERSCORED ITS COMMITMENT TO REGIONAL DATA SOVEREIGNTY WITH THE LAUNCH OF A UAE DATA CENTRE, WHILE ADDRESSING EVOLVING ADVERSARY TACTICS, AI-POWERED THREATS, AND THE NEED FOR ORGANISATIONS TO BUILD PEOPLE-CENTRIC RESILIENCE FOR LONG-TERM CYBERSECURITY SUSTAINABILITY.

Cybersecurity leader Sophos reinforced its focus on the Middle East market with the launch of a new UAE Data Centre at GITEX Global 2025. Hosted through AWS, the facility is designed to deliver improved latency, enhanced access to Sophos' portfolio, and crucially, regional data sovereignty — a growing priority for regulated sectors such as healthcare, finance, and critical infrastructure.

"We established the UAE Data Centre to ensure customers can securely store and manage their data within the local region, aligning with tightening compliance frameworks," explained John Shier, Field CTO at Sophos. "It's about giving organisations control and confidence as regulatory landscapes mature."

Evolving adversary tradecraft

Drawing on findings from the Sophos Active Adversary Report 2025, Shier noted a 126% increase in "living off the land" attacks — a technique in which adversaries exploit legitimate Microsoft tools already installed in systems to conceal their movements.

"Defenders must understand their baseline environment — which tools are used, when, and how," he said. "You can't simply disable PowerShell, but you can monitor for unusual behaviours, like obfuscated scripts, which are rarely legitimate. New tactics evolve constantly, but old weaknesses such as stolen credentials and unpatched vulnerabilities remain persistent. The key is to understand your normal, manage the new, and never neglect the old."

Preparing for AI and quantum threats

When asked about the rise of AI-powered offensive tools and the looming challenge of quantum decryption, Shier said that organisations needed to differentiate between the near and long-term threats.

"Right now, AI poses a social threat — it's making phishing almost indistinguishable from genuine communication," he observed. "Attackers can produce flawless messages that exploit human trust. We haven't yet seen fully autonomous AI-driven attacks, but we must remain vigilant because AI learns from us."

On the subject of post-quantum cryptography (PQC), he advised that while the threat may still be a decade away, preparation must begin now. "CISOs should start mapping every asset that uses cryptography — including embedded systems and HSMs. Transitioning to PQC isn't an overnight shift. Identify which data will still matter in ten years and plan for lifecycle management to mitigate 'collect now, decrypt later' risks."

Building human-centred resilience

Sophos' State of Ransomware Report also highlighted the growing human cost of cyber incidents. Shier said that defenders were increasingly overwhelmed by alert fatigue, complexity, and constant pressure.

"When an attack occurs, it introduces

John Shier, Field CTO, Sophos, discusses the human side of cybersecurity and the company's growing focus on data sovereignty in the Middle East.

A CULTURE THAT SUPPORTS LEARNING, COMMUNICATION, AND COLLECTIVE RESPONSIBILITY WILL ALWAYS BE MORE RESILIENT THAN ONE THAT SIMPLY REACTS.

chaos and exhaustion," he said. "The answer lies in preparation and culture. Organisations need tailored incident response plans that go beyond ransomware — covering breaches, insider threats, or even natural disasters."

He emphasised that resilience must extend beyond technology. "Security is everyone's responsibility. Employees shouldn't be blamed as weak links — they should be empowered as the first line of defence. A supportive culture that promotes learning and communication will always outperform one that simply reacts."

From awareness to sustainability

As Cybersecurity Awareness Month closed in October, Shier shared practical steps for building sustainable vigilance across teams.

"First, adopt a people-centric approach," he said. "Security incidents always involve people — from IT responders to PR teams. Support them, ensure smooth handoffs, and design processes that prevent burnout."

"Second, have a clear but flexible plan. Define roles and contingencies before a crisis hits — structure reduces panic."

"Third, test and learn continuously. Run tabletop exercises, close communication gaps, and update your response plans. And finally, learn from peers. Cybersecurity is a community effort — events like GITEX remind us that collaboration is our strongest defence."

Shier concluded with a reminder that sustainable cybersecurity depends on balance. "By focusing on people, process, and collaboration, we make technology work better — and security far more resilient."

SECLORE CHAMPIONS TRUST IN AN ERA OF AI AND CYBER RESILIENCE

GITEX GLOBAL 2025 SPOTLIGHTS SECLORE'S VISION FOR A SECURE DIGITAL FUTURE WHERE AI INNOVATION, REGULATORY STRENGTH, AND TRUSTED ECOSYSTEMS DRIVE THE NEXT WAVE OF CYBERSECURITY ACROSS THE MIDDLE EAST.

Digital transformation sweeping across the Middle East is reshaping how organisations protect and govern data.

Justin Endres, Chief Revenue Officer, Seclore and Uraz Farukh, Senior Sales Director, KSA & Bahrain, Seclore spoke to Sandhya D'Mello, Technology Editor, CPI Media Group during GITEX Global 2025 about managing unstructured data and AI-driven threats to building resilience and maintaining customer trust.

The global brand's growing channel ecosystem continues to empower partners and businesses to advance towards a more secure and compliant digital economy.

You've been around the region and witnessed how fast the market is evolving. What are your impressions of the first day at GITEX Global?

Justin Endres: The general sentiment is much like always — it's a great opportunity to meet partners and customers, as well as potential new ones. It's also a fantastic occasion to catch up with other vendors we collaborate with in the field. Overall, GITEX remains an invaluable event that we always look forward to.

What is the company showcasing at GITEX this year?

Justin Endres: Unlike last year, when we presented a full suite of products on our platform, this year's focus is on discovery and AI. We're really aligning with market demand, particularly in helping organisations understand where their sensitive data resides — be it in the cloud, on desktops, or elsewhere. We're introducing a stronger discovery-to-remediation solution that offers end-to-end visibility and protection. Beyond that, GITEX is also about reconnecting with our ecosystem and partners.

With just a couple of months left in 2025, how do you evaluate the year's performance compared to 2024, and what does the 2026 pipeline look like?

Justin Endres: We've had the privilege of working with a fantastic network of partners, and our pipeline is stronger than ever. The first half of the year was excellent, and as we close the third quarter, the outlook remains very positive. That said, we continue to earn customer trust every single day — it's the foundation of our growth.

What are the top customer trends or challenges you're seeing, and how are you addressing them?

Justin Endres: It varies by country. Saudi Arabia, the UAE, and Qatar are all at different stages of maturity, but the central issue everywhere is data protection. The old perimeter-based approach no longer works. Despite higher spending, breaches and costs are still rising. AI has also introduced an explosion of unstructured data, making sensitive data protection more complex than ever. Having been in this space for nearly 15 years, we understand these challenges well and are helping organisations locate and secure their most critical data.

Is cyber resilience now the key to business success?

Justin Endres: Absolutely. Cyber resilience underpins everything — not just technology, but also trust. Whether you're a consumer brand, a service provider, or a partner, resilience ensures continuity and confidence. Technology must evolve to stay ahead of adversaries, but when it doesn't, businesses must still have mechanisms to fall back on and recover quickly.

With Saudi Arabia emerging as a key regional force and Cybersecurity Awareness Month coinciding with GITEX, how do you see this momentum influencing the market?

Uraz Farukh: The region is at a fascinating stage. In Saudi Arabia, regulations are strict and compliance-driven, while the UAE is quickly catching up. GITEX is the perfect platform for customers to discover new technologies and understand how to adopt them. Events like this encourage awareness, learning, and innovation — all vital for improving regional cyber maturity.

Both the UAE and Saudi Arabia are advancing rapidly toward digital-first economies. What are your observations on how customers are responding to the growing need for proactive cyber resilience?

Uraz Farukh: Every new technology — whether AI or GPT — brings both opportunities and challenges. AI, in particular, is reshaping business operations but also introducing new pain points. Unlike blockchain, which lost momentum, AI is here to stay. The focus now is on integrating AI responsibly into cybersecurity tools to address emerging threats. That's where we and other vendors are investing heavily.

How are you empowering your channel ecosystem to keep pace with evolving AI and cybersecurity demands?

Uraz Farukh: We're a channel-focused company with a very strong partner ecosystem. We have structured partner programmes, regular communication via newsletters and WhatsApp updates, and ongoing enablement initiatives. Our partners act as an extension of us in the market — taking our message and solutions to customers. This close collaboration is key to ensuring consistent delivery and satisfaction.

What will be your key focus for 2026?

Uraz Farukh: We're prioritising the strengthening of our channel ecosystem. The region is seeing new partners entering from Egypt and beyond, particularly into Saudi Arabia's growing cybersecurity space. Our aim is to ensure customer satisfaction through improved post-sales support. Justin and the customer success team are expanding efforts to make sure clients are fully supported and getting maximum value from our technology.

Maya Zakhour
Director of Partner Ecosystem – MEA
BeyondTrust.

BEYONDTRUST'S VISION OF TRUST AND IDENTITY INSPIRES REGIONAL GROWTH: MAYA ZAKHOUR

MAYA ZAKHOUR, DIRECTOR OF PARTNER ECOSYSTEM – MEA, AT BEYONDTRUST, SPOKE TO CNME EDITOR MARK FORKER ABOUT HER NEW ROLE, WHY THE VISION OF THE COMPANY INSPIRES HER EVERY DAY, AND THE IMPORTANCE OF HARNESSING THE CHANNEL COMMUNITY TO HELP BEYONDTRUST GROW ACROSS THE MIDDLE EAST REGION.

When it comes to leadership and channel engagement, few names in the regional ICT landscape carry as much weight as Maya Zakhour. Having recently joined BeyondTrust as Director of Partner Ecosystem – MEA, Zakhour brings with her years of experience, deep industry insight, and a passion for building trusted partner relationships.

Reflecting on what drew her to the cybersecurity leader, Zakhour says the company's clear vision immediately resonated with her.

"What attracted me to join BeyondTrust was the company's vision. They have a clarity of purpose that stands out, especially amidst the profound technological change we're seeing across the industry globally," she explains. "We live in an AI-driven world—but in the AI world, we need trust. We must foster an environment where people can collaborate confidently and know they can trust what they are buying or deploying from AI. I believe I joined the company at the perfect time."

For Zakhour, trust is not just a marketing message—it's the foundation of BeyondTrust's approach to security and a core enabler of its identity-first strategy.

"There is no impact better than trust, and that's needed for the new security perimeter, which is identity," she emphasises.

Since stepping into her new role, Zakhour has spent the past few months meeting with customers and partners across the region. The response, she says, has been overwhelmingly positive.

"Our customers love our technology," she shares. "Just last week, a large enterprise told me how much they value our solutions. They experienced an unauthorised access attempt and used BeyondTrust tools to isolate the threat. That's the power of a true zero-trust solution—it goes back to vision. When you have the right vision, you create the right solutions, which deliver the right outcomes."

THERE IS NO IMPACT BETTER THAN TRUST, AND THAT'S NEEDED FOR THE NEW SECURITY PERIMETER, WHICH IS IDENTITY.

One of BeyondTrust's key differentiators in the market lies in its expertise in privileged access management (PAM), a capability increasingly critical in today's security landscape.

"In terms of market differentiators, there's a lot," Zakhour says. "Trust is one, but our ability to determine access for the right person—whether human or agent—is essential. Privileged access is an area where we excel. Partners want to be part of this journey, and AI is central to that story. At the end of the day, it's about ensuring the right level of access and privilege, and our suite of solutions gives customers the visibility they need to detect and respond to threats effectively."

Looking ahead, Zakhour is clear about her mission: to empower customers to embrace AI with confidence and security.

"We want customers to enjoy AI—but safely and responsibly," she concludes. "With BeyondTrust, they can build a strong trust and identity security strategy. We give them the freedom to let any authorised person access specific applications from anywhere, knowing they're protected. That's how we're building trust—step by step."

Robert McNutt
Chief Strategy Officer
Forescout

FORESCOUT REINFORCES ZERO TRUST ASSURANCE WITH AI-DRIVEN VISIBILITY ACROSS IT, IOT, AND OT

ROBERT MCNUTT, CHIEF STRATEGY OFFICER AT FORESCOUT, OUTLINES HOW THE COMPANY IS HELPING ORGANISATIONS SECURE CRITICAL INFRASTRUCTURE THROUGH CONTINUOUS VISIBILITY, AI-ASSISTED DECISION-MAKING, AND A UNIFIED ZERO TRUST FRAMEWORK.

Forescout marked its 25th anniversary, celebrating a legacy of protecting some of the world's most critical organisations across banking, energy, healthcare, and government sectors.

Robert McNutt, Chief Strategy Officer at Forescout, spoke to CNME Editor Mark Forker about how the company continues to evolve amid today's rapidly shifting cybersecurity landscape at GITEX Global 2025.

McNutt discussed Forescout's mission to deliver complete visibility across IT, IoT, and OT environments, its pragmatic use of AI as an intelligent assistant for faster decision-making, and the company's unique approach to achieving Zero Trust Assurance using existing infrastructure. He also highlighted how the convergence of IT and OT systems is exposing critical infrastructure to new types of cyberthreats—and how Forescout's continuous verification model helps organisations build resilience in an era of digital and economic warfare.

What was Forescout's main message at GITEX this year?

Forescout celebrated its 25th anniversary this year, marking a quarter-century of protecting some of the world's most critical organisations—ranging from global banks and energy companies to government and healthcare institutions. The company's message focused on three core elements: complete visibility of every connected asset across an enterprise, understanding how these assets behave and whether they comply with internal or regulatory standards, and translating that intelligence into proactive and reactive security controls. Ultimately, Forescout enables organisations to achieve zero trust assurance using their existing infrastructure without requiring new investments.

How does Forescout leverage AI to strengthen cybersecurity resilience for its customers?

Forescout views AI as an assistant to human decision-making, helping cybersecurity teams process large volumes of data more efficiently. The company uses AI to make policies smarter and to reduce the time required to reach critical decisions—from hours to seconds. By applying AI across millions of connected devices, ranging from servers and laptops to IoT sensors and logic controllers, Forescout can identify risks faster, generate more accurate reports, and help customers assess whether their security controls are effective in real time.

Why is visibility across IoT and OT environments so vital to modern cybersecurity?

Visibility across IoT and OT systems is essential because these environments often include devices and operating systems that differ from traditional IT systems. While IT assets typically rely on well-known platforms such as Windows, IoT and OT systems often run on obscure or proprietary operating systems with limited third-party security tools. This creates a significant security gap. As organisations connect once-isolated OT environments to the internet, attackers exploit this exposure to target physical infrastructure—such as factories or utilities—where the potential disruption can have severe real-world consequences.

FORESCOUT CAN IDENTIFY RISKS FASTER, GENERATE MORE ACCURATE REPORTS, AND HELP CUSTOMERS ASSESS WHETHER THEIR SECURITY CONTROLS ARE EFFECTIVE IN REAL TIME.

Can you share an example that illustrates how attackers are targeting critical infrastructure?

Forescout operates a large-scale adversary engagement environment, essentially a sophisticated honeypot. In one instance, the company simulated a water treatment facility in Eastern Europe. A hacktivist group mistakenly believed they had gained control of a real water utility and attempted to sell access to it on the dark web. This incident revealed how attackers are increasingly focusing on operational and critical infrastructure targets—where disruption translates into real-world impact, economic instability, or even threats to human life.

How does Forescout interpret and implement the concept of Zero Trust?

Forescout defines Zero Trust as a strategy, not a single product or vendor solution. True Zero Trust requires coordination across multiple technologies—spanning cloud, on-premises, data centres, and remote work environments. Forescout delivers what it calls "Zero Trust Assurance," which unifies these disparate technologies under a single policy, audit, and visibility framework. This ensures that all systems operate in tandem, continuously verifying trust across the environment rather than relying on one-time authentication.

Forescout has been delivering Zero Trust Assurance long before the term became mainstream. How has the concept evolved?

Forescout's journey towards Zero Trust began long before the term was coined. The company's early focus was on network access control, unified visibility, and endpoint compliance—concepts that naturally evolved into the modern Zero Trust framework. The guiding principle remains "trust but verify," with an emphasis on continuous verification. Attackers rarely enter through the front door anymore; they compromise already trusted systems and move laterally across networks. Hence, Forescout's continuous assurance model ensures that even trusted assets are constantly validated to prevent internal breaches.

Francois Van Deventer
Director & CTO – Emerging Markets, Eastern Europe, Turkey, MENA, and Africa at Citrix.

THE BIGGEST CONCERN WE'RE SEEING IS THAT AGENTIC AI COULD BECOME THE NEXT INSIDER THREAT.

CITRIX REDEFINES HUMAN–AI COLLABORATION FOR MODERN WORKFORCE

AT GITEX GLOBAL 2025, CITRIX HIGHLIGHTED HOW AI IS NO LONGER A CONCEPT OF THE FUTURE BUT A CORE COMPONENT OF TODAY'S ENTERPRISE ECOSYSTEM, DRIVING SECURE, SEAMLESS COLLABORATION BETWEEN HUMANS AND INTELLIGENT SYSTEMS.

Francois Van Deventer, Director & CTO – Emerging Markets, Eastern Europe, Turkey, MENA, and Africa at Citrix, spoke to Sandhya D'Mello, Technology Editor at Security Advisor Middle East, during Gitex Global 2025 about the company's vision for the AI-powered workplace.

Francois shared insights on how Citrix is enabling human–AI collaboration through intelligent automation, secure virtual environments, and its flagship solutions such as Citrix Copilot and NetScaler. He also discussed the emergence of the UAE and Saudi Arabia as global hubs for digital innovation and AI talent, supported by major partnerships with technology giants like Nvidia, Google, and Amazon.

What was your impression of GITEX Global 2025 so far?

It was truly overwhelming. Even halfway through day two, the footfall and overall buzz were incredible. Compared to last year, this year's event feels busier and more dynamic, especially with the excitement around AI and robotics. It's a world-class experience and a testament to how fast the technology landscape is evolving.

You describe AI not as a future project but as a part of today's workforce. What do you mean by 'humans plus AI equals the new workforce'?

We've moved beyond the experimentation stage with AI. Organisations are already executing AI-driven strategies and integrating intelligent systems to automate processes. At Citrix, we focus on enabling collaboration between human workers and AI systems. It's about managing both entities securely and seamlessly so that intelligent humans and AI agents can work together effectively within organisations.

If AI is now part of the workforce, what are the main security challenges organisations face?

The biggest concern we're seeing is that agentic AI could become the next insider threat. Traditionally, most breaches come from within organisations — through compromised credentials or insider misuse. Now, we need to treat AI systems with the same level of security as human users. At Citrix, we help clients protect and manage these AI systems just like human workers, ensuring their actions remain within defined, secure boundaries.

How is Citrix helping organisations navigate this era of human–AI collaboration?

Citrix has launched several initiatives and solutions to ease this transition. For example, Citrix Copilot was developed to help clients reduce administrative burdens by applying intelligence to manage complex environments. Through our Virtual Desktop Infrastructure (VDI), we provide sandbox environments where autonomous, agentic AIs can operate safely without jeopardising sensitive credentials or data. Moreover, our NetScaler solutions, in partnership with Google, Nvidia, and others, enable secure communication between different AI systems, ensuring that their interactions remain transparent and protected.

Do you think the UAE has already evolved into a global hub for digital skills and AI talent?

The UAE — along with Saudi Arabia — has positioned itself as a leading global hub for artificial intelligence. The region hosts some of the world's largest data centres and maintains strong partnerships with technology giants like Nvidia, Google, and Amazon. This ecosystem attracts immense digital talent and offers organisations the perfect environment to innovate and leverage AI capabilities at scale.

SENTINELONE EMPOWERS ENTERPRISES WITH AI-DRIVEN SECURITY AT MACHINE SPEED

AT GITEX GLOBAL 2025, SENTINELONE SHOWCASED HOW ITS UNIFIED XDR PLATFORM, ENHANCED BY PURPLE AI AND INTELLIGENT AUTOMATION, IS REDEFINING HOW ORGANISATIONS DETECT, RESPOND, AND DEFEND AGAINST EVOLVING CYBER THREATS.

SentinelOne reinforced its leadership in autonomous cybersecurity at GITEX Global 2025, unveiling new advancements in its XDR platform and announcing two strategic acquisitions to expand data observability and automation.

Meriam El Ouazzani, Senior Regional Director for META, spoke to CNME Editor Mark Forker and discussed how the company is reshaping enterprise security by delivering protection at machine speed and simplifying complex security operations through AI-driven orchestration.

El Ouazzani highlighted the growing impact of Purple AI in addressing the region's cybersecurity skills gap, empowering analysts with intuitive tools for faster, smarter threat detection and response, and underlined the vital role of SentinelOne's partner ecosystem in driving scale and customer success across the Middle East.

What was SentinelOne's key focus at GITEX Global 2025?

We always use GITEX as an opportunity to announce new developments within SentinelOne. This year, we reinforced our position as an AI company that's deeply rooted in cybersecurity. Our XDR platform continues to evolve — enabling customers not only to collect and analyse intelligence from multiple sources, but also to ingest third-party data for greater control and insights. We take pride in our AI-driven EDR, as well as our cloud, identity, and mobile security solutions. At this year's event, we also announced two major acquisitions, including an observability platform from an AI company, which strengthens our data optimisation and automation capabilities.

Analysts often say SentinelOne is redefining enterprise security. How is the company achieving this?

We understand that customers today need security at machine speed. Our focus is to give cybersecurity analysts and specialists tools that help them do their jobs faster, better, and more intelligently. This involves breaking down silos — providing a unified platform that ingests data from multiple sources, runs analysis, and enables immediate action. Through our AI-powered platform play, we protect, detect, and respond autonomously, while also empowering analysts to perform threat hunting in natural language via Purple AI. We pair this with automation, allowing users to create drag-and-drop workflows with no scripting or complex configuration — delivering true scalability and operational speed.

You mentioned Purple AI — how is it helping address the skills gap and analyst fatigue in cybersecurity?

Skills shortage and analyst fatigue are major challenges. Many organisations struggle to attract and retain talent, or to train people on rapidly evolving technologies. Purple AI helps by simplifying the operational side of cybersecurity. It enables anyone — even those without deep technical backgrounds — to perform advanced threat hunting using simple language. Our "Mortal versus Machine" demonstration at GITEX showcased this perfectly: visitors from non-cyber backgrounds could use Purple AI to compete with our experts. It's a tangible way to show how simplicity and AI-driven tools can bridge the skills gap and reduce fatigue.

How vital is SentinelOne's partner ecosystem in driving success across the Middle East?

The Middle East is a 100% channel-driven market, and without the right partners, we can't scale effectively. Customers want trusted partners who can deliver services, deployment, and ongoing support. We work closely with system integrators and resellers that not only have the technical capabilities to implement our platform but also

Meriam El Ouazzani
Senior Regional Director for META
SentinelOne.

the strategic mindset to co-develop cybersecurity roadmaps with clients. The best partnerships are those where partners act as strategic advisors — working hand-in-hand with customers and other vendors to deliver end-to-end security outcomes.

What value does GITEX Global offer SentinelOne from both a business and innovation perspective?

GITEX provides a unique opportunity to showcase our technology, engage directly with customers, and gather feedback on how we can improve our platform. Many visitors tell us they're already using SentinelOne and share ideas for complementary integrations or new features. These insights often lead to future collaborations or technology partnerships. For us, GITEX is about demonstrating real, working technology — not concepts or promises. It's where we connect innovation, feedback, and relationships that drive cybersecurity forward in the region.

Tony Zabaneh
Director of Systems Engineering, Middle East South Fortinet.

FORTINET CHAMPIONS AI-DRIVEN, IDENTITY-FOCUSED SECURITY AT GITEX GLOBAL 2025

FORTINET SHOWCASED ITS LATEST INNOVATIONS ACROSS OT, SECOPS, AND SOVEREIGN SASE, AT GITEX GLOBAL 2025, UNDERSCORING ITS COMMITMENT TO AI-POWERED, CUSTOMER-CENTRIC SECURITY THAT DELIVERS FASTER DETECTION, SEAMLESS INTEGRATION, AND TRUSTED PROTECTION ACROSS HYBRID ENVIRONMENTS.

Fortinet reaffirmed its leadership in cybersecurity at GITEX Global 2025 by showcasing an extensive portfolio of solutions designed to secure the modern digital landscape. The company placed strong emphasis on Operational Technology (OT) security, Security Operations (SecOps), and Secure Access Service Edge (SASE) — including sovereign SASE models that empower enterprises and government entities to retain full control over their network traffic. With a focus on integration, flexibility, and customer-centric innovation, Fortinet demonstrated how its end-to-end security fabric enables faster detection, seamless remediation, and adaptive protection across hybrid environments.

Tony Zabaneh, Director of Systems Engineering, Middle East South at Fortinet, spoke to CNME Editor Mark Forker about how the company's long-standing expertise in AI, identity-driven security, and solution-centric design continues to help customers navigate an increasingly complex threat landscape while strengthening resilience and trust.

What did Fortinet showcase at GITEX Global 2025, and what was the key message the company aimed to convey?

Fortinet is one of the largest vendors globally in the security industry and secure technologies. This year, our focus was on showcasing specific use cases for Operational Technology (OT) security and Security Operations (SecOps). We also demonstrated live Secure Access Service Edge (SASE) solutions, including sovereign flavours of SASE — a crucial topic for customers who wish to maintain their traffic within their premises, whether in enterprise businesses or government agencies. In addition, we showcased our cloud business offerings and broader integration capabilities.

Fortinet is often described as highly customer-centric. What differentiates your approach and product offerings in such a competitive cybersecurity market?

I strongly believe in the power of people and relationships. Fortinet has a truly global presence, and our regional footprint across the Middle East is particularly strong. This helps us build deep trust with our customers. Beyond relationships, it's our breadth of technology that stands out. Fortinet leads in multiple security verticals and excels at integration, which is often a major challenge for customers. Integration allows them to accelerate detection and remediation times. We are not only customer-centric but also solution-centric — we design solutions that truly solve clients' problems rather than just selling products.

AI is often viewed as a double-edged sword in cybersecurity. How is Fortinet integrating AI into its product portfolio to strengthen security and simplify operations?

AI can be used by both defenders and adversaries — it's all about how far you leverage it to mitigate risk. The threat landscape has expanded significantly, largely because data and users are now everywhere — across clouds, applications, and connected devices. At Fortinet, we've been incorporating AI for over 12 years. It helps our products detect and respond to threats much faster.

We use AI in three key ways:

1. Enhancing our technologies – enabling faster and smarter detection and mitigation.
2. Simplifying user interaction – through GenAI tools that allow security teams to "talk" to the product, reducing complexity and technical barriers.
3. Protecting customers' own AI assets – as many organisations now deploy on-premises large language models, we secure those environments as well.

The threat landscape has increasingly shifted toward identity-based attacks — has Fortinet adjusted its strategy or technology in response?

We've always focused on customer journeys and use cases rather than isolated products. A product is only one piece of a bigger puzzle. When integrated with others, it forms a solution. At GITEX, we presented numerous integration-driven use cases demonstrating how our solutions evolve with the customer's needs — whether on-premises, hybrid, or cloud-based. Our frameworks are flexible and modular, allowing customers to plug in new technologies as their environments change. Ultimately, everything we do is aimed at reducing detection and remediation times — the critical differentiator between a quick recovery and a costly breach.

How does GITEX Global contribute to Fortinet's goals in the region, and what value did the event bring to your team and partners?

GITEX is, without question, the region's largest and most influential technology event. I've personally participated for over 15 years and have a real soft spot for it. It's the one time of year when everyone — colleagues, customers, and partners — gathers in one place. It's invaluable for relationship-building, showcasing real-time demos, and preparing complex use cases that demonstrate Fortinet's technology in action. Beyond the business aspect, it's about connecting with people, exchanging insights, and strengthening the ecosystem that drives innovation and security forward.

WE ARE NOT ONLY CUSTOMER-CENTRIC BUT ALSO SOLUTION-CENTRIC — WE DESIGN SOLUTIONS THAT TRULY SOLVE CLIENTS' PROBLEMS RATHER THAN JUST SELLING PRODUCTS.

Bernard Montel
Technical Director for EMEA
Tenable.

TENABLE REDEFINES EXPOSURE MANAGEMENT WITH AI-DRIVEN CYBERSECURITY INNOVATION

TENABLE SHOWCASED HOW ITS EXPANDED EXPOSURE MANAGEMENT PLATFORM AND AI-POWERED CAPABILITIES ARE HELPING ORGANISATIONS GAIN UNIFIED VISIBILITY ACROSS FRAGMENTED ATTACK SURFACES WHILE PROACTIVELY SECURING DATA, CLOUD, AND AI ENVIRONMENTS.

Tenable reaffirmed its leadership in cybersecurity at GITEX Global 2025, unveiling the latest advancements in its exposure management platform designed to help organisations stay ahead of evolving digital threats.

Bernard Montel, Technical Director for EMEA at Tenable, spoke to Sandhya D'Mello, Technology Editor, Security Advisor Middle East, about how the company is addressing the growing complexity of the modern attack surface—spanning cloud, AI, and operational technology—through unified visibility and proactive risk reduction.

Montel also shared insights into Tenable's innovative use of AI to detect shadow AI, secure organisational AI projects, and mitigate misconfigurations and vulnerabilities that expose sensitive or encrypted data. The technical director for EMEA also reflected on the convergence of threats, the importance

of post-quantum cryptography, and the need for businesses to adopt a prevention-first cybersecurity mindset.

What is your impression of GITEX Global 2025?
GITEX is always a huge event — one of the largest high-tech gatherings in the world, and certainly the biggest for this region. Every year, it continues to grow in scale and importance, showcasing innovation and leadership in technology.

Tenable is recognised for its focus on exposure management. How is this approach helping organisations stay ahead of cyber threats?
Cyber threats are evolving rapidly because the attack surface has become highly fragmented with cloud, AI, and multiple tools creating silos. This fragmentation makes it difficult for security teams to manage vulnerabilities effectively and results in alert fatigue. Tenable's exposure management approach addresses this by consolidating all weaknesses — vulnerabilities, misconfigurations, and risks — into a single, unified platform. This comprehensive visibility enables organisations to respond faster and more effectively to emerging threats.

AI has become a buzzword in cybersecurity. How is Tenable leveraging AI to detect and respond to threats faster?
AI is now part of everyone's daily lives, and cybersecurity is no exception. At Tenable, we focus on three major use cases. First is detecting Shadow AI, where employees use AI tools without organisational oversight. Second is identifying risks such as prompt injections and exposure of personal information. Third is securing AI projects developed by organisations themselves, which can introduce vulnerabilities and misconfigurations. Our scanners and exposure management platform can now detect these AI-related risks, giving companies a complete picture of their exposure.

ORGANISATIONS MUST PRIORITISE THE SECURITY OF AI INFRASTRUCTURE AND APPLY EXPOSURE MANAGEMENT PRINCIPLES UNIFORMLY ACROSS ALL THEIR ENVIRONMENTS TO MITIGATE THE GROWING RISKS ASSOCIATED WITH BIG DATA AND AI SYSTEMS.

What innovations and technologies is Tenable showcasing at GITEX 2025?
Tenable continues to innovate year after year. For 2025, we introduced two key advancements. First, our platform is now open to non-Tenable data, allowing integration from any system for a more holistic exposure view. Second, we have enhanced our AI capabilities following a recent acquisition, expanding our ability to manage and assess AI-related exposures, reflecting our commitment to stay ahead of the evolving cybersecurity landscape.

Looking ahead, what do you think will define the next phase of cybersecurity?
We are seeing a convergence of threats across different parts of the attack surface — no longer limited to networks or endpoints. Attackers are targeting every layer, from cloud and OT to AI environments. The next phase will focus on tackling this convergence with AI-powered defence strategies and faster exposure understanding. Attackers are already using AI; defenders must do the same to keep pace.

What advice would you give to organisations seeking to strengthen data security and ensure business continuity?
Firstly, recognise that everything is data, and attackers are increasingly targeting even encrypted data. Organisations should start preparing for post-quantum cryptography, which will reshape how we secure encrypted assets. Secondly, they must reset their cybersecurity mindset — moving from a purely detection-based approach to a prevention-first strategy. Reducing the risk of exposure proactively is far more effective than simply trying to detect attacks after they occur.

You mentioned that even encrypted data is at risk. How can organisations protect themselves?
Misconfigurations and exposure remain the biggest risks — even for encrypted data. AI projects are a prime example: 89% of organisations have initiated AI projects, over half are already in production, and a third have faced breaches due to misconfigurations or insider risks. Developers often leave training data in exposed cloud repositories, creating significant vulnerabilities. Organisations must therefore secure AI training data, encrypted data, and traditional data alike through continuous monitoring and exposure management.

With both traditional and AI-generated data growing rapidly, how can organisations manage this complexity effectively?
AI projects tend to have a much higher vulnerability rate — around 70% — compared to traditional cloud services at 50%. This happens because AI teams focus on functionality rather than security. Moreover, AI equals big data: if you breach an AI project, you inherently breach massive datasets used for training. Hence, organisations must prioritise the security of AI infrastructure and apply exposure management principles uniformly across all their environments to mitigate the growing risks associated with big data and AI systems.

UAE SHAPES FUTURE DEFINED BY AI, CYBERSECURITY AND TALENT EMPOWERMENT, SAYS AHMAD ALHAI

AHMAD ALHAI, CEO AND CO-FOUNDER OF COMPLY LLC, REFLECTS ON THE UAE'S TRANSFORMATION INTO A GLOBAL DIGITAL HUB, DRIVEN BY INNOVATION, CYBERSECURITY EXCELLENCE, AND THE CULTIVATION OF NEXT-GENERATION TALENT.

Ahmad Alhai, CEO and Co-Founder of Comply LLC, joined Sandhya D'Mello, Technology Editor at Security Advisor Middle East, for an engaging conversation during GITEX Global 2025. Drawing on his deep roots in the UAE and over three decades of first-hand experience, Alhai traced Dubai's evolution from its early development stages to becoming a leading digital-first nation. He shared how visionary leadership, strong cybersecurity frameworks, and strategic investments in AI, blockchain, and smart infrastructure have positioned the UAE at the forefront of global innovation. Emphasising education, mentoring, and belief in homegrown talent, Alhai underscored that the nation's progress is powered not just by technology, but by a relentless commitment to quality and knowledge.

How did you find the atmosphere at GITEX Global 2025?
It was truly an exceptional year. The energy and innovation on display were remarkable. Over the past five years, we have seen how artificial intelligence has evolved from being a concept to becoming an integral part of business and governance. GITEX 2025 showcased this transformation, with companies and government entities presenting real-world use cases that demonstrate how deeply AI is now embedded in our society and economy.

Given the UAE's Digital First strategy, how do you see cybersecurity evolving in the near future?
With the UAE focusing heavily on data-driven industries, cybersecurity must be at the forefront. Traditional security models no longer suffice. Today, AI is even used within defence mechanisms to secure information. Cybersecurity in the UAE has become a showcase for the world, proving that information can be safely hosted here. Leading entities like G42 and Smart Dubai have created secure digital ecosystems, and events like GITEX reflect that commitment by inviting global innovators to present their best solutions.

Dubai has become a magnet for global talent. What factors contribute to this digital hub's continued growth?
Dubai's success in attracting talent is not by chance. Since 1996, the UAE has laid the groundwork for nurturing tech professionals, building an ecosystem that welcomes innovators. In the past five years alone, Dubai has attracted over 100,000 developers, offering them a supportive environment and recognition through awards and opportunities. It's like a "garden of roses" — a place where talent can thrive, innovate, and grow globally.

You've witnessed Dubai's journey from desert to digital powerhouse. What drives this futuristic vision?
As a sixth-generation Emirati, I've seen Dubai's transformation first-hand. The city's progress is not accidental—it's the result of visionary leadership, robust planning, and collaboration. Since 1996, Dubai's long-term plans have been executed with precision. The leadership created a welcoming environment for investors, ensuring both security and opportunity. It's a two-way relationship: the UAE supports investors, and in return, it learns and grows with them.

For businesses seeking to build smart IT infrastructure, must innovation always come at a high cost?
Success begins with a clear strategy and belief in your vision. When we started, our investment was just Dh250,000. We focused on planning, setting milestones, and selecting the right people. Within five years, that investment grew into a $210 million revenue stream. The key is to plan effectively—define short, medium, and long-term goals, build networks, and execute steadily. Smart infrastructure isn't about high spending; it's about smart strategy and belief in the process.

How should organisations prepare the next generation of talent for the digital future?
Education and adaptability are essential.

Ahmad Alhai
CEO and Co-Founder
Comply LLC.

Technologies are evolving rapidly—from blockchain to IoT to AI—and every few years, a new revolution begins. To stay relevant, professionals must keep learning and earning certifications. I work with a team of young engineers who may have studied traditional engineering but now thrive in digital roles. They already have the digital mindset; they just need guidance and mentorship. Leaders must take responsibility for coaching and empowering this new generation.

How can the UAE continue to uphold its legacy while building a stronger digital future?

The UAE began its journey by focusing on quantity—building the nation and its institutions. Now, we are in the era of quality, nurturing a generation equipped with knowledge, innovation, and global thinking. Our future depends on fostering quality education and sustaining that drive for excellence. We've reached the moon; the next goal is to go beyond. That's the spirit of the UAE.

RESECURITY BRIDGES HUMAN AND ARTIFICIAL INTELLIGENCE TO REDEFINE CYBER RESILIENCE

RESECURITY SHOWCASED HOW THE FUSION OF HUMAN INSIGHT AND AI INNOVATION IS SHAPING THE NEXT ERA OF INTELLIGENCE-LED CYBERSECURITY ACROSS THE GCC AND MENA REGION DURING GITEX GLOBAL 2025.

Resecurity Inc. has been at the forefront of advancing intelligence-led cybersecurity, combining the power of human expertise and artificial intelligence to help organisations stay ahead of evolving digital threats. During GITEX Global 2025, Ahmad Halabi, Managing Director at Resecurity Inc., spoke with Sandhya D'Mello, Technology Editor at Security Advisor Middle East, about the company's mission to build a cyber-resilient ecosystem across the GCC and MENA region.

Halabi outlined how Resecurity's approach goes beyond traditional defences by studying the mindset of hackers to anticipate future attack patterns. He also discussed the company's initiatives to nurture local cybersecurity talent through university partnerships, promote cyber awareness, and deploy AI-driven tools that simplify analysis, accelerate response, and strengthen organisational resilience.

How did you find the overall energy and atmosphere at GITEX 2025?

It was fantastic — full of positive energy, great footfall, and meaningful discussions. The event provided an excellent opportunity for the industry to reconnect, exchange ideas, and strengthen relationships after a long gap.

The UAE continues to build its reputation as a Digital-First Nation. From your perspective, how did you assess the country's progress in becoming cyber resilient?

The UAE has long been one of the most progressive governments in adopting and advancing technology, including cybersecurity. The leadership here has consistently ensured that innovation goes hand in hand with resilience and proactive protection. Their approach has not just focused on detecting cyber threats but also on predicting and preparing for them. With the rise of emerging technologies like AI, this forward-thinking mindset has been crucial in maintaining robust defences against an increasingly complex threat landscape.

Could you elaborate on Resecurity's mission in the cybersecurity industry?

Resecurity has taken cybersecurity a step further by focusing on understanding the criminal mindset — the techniques, tools, and behaviour patterns of hackers. By studying how attackers think, we can better predict and counter their actions. The company combines artificial intelligence with human intelligence to deliver solutions such as threat intelligence, brand monitoring, fraud prevention, penetration testing, incident response, forensics, and threat hunting. The mission is to empower governments, law enforcement, and enterprises to leverage intelligence-led cybersecurity practices.

What differentiates Resecurity's approach from that of traditional cybersecurity vendors?

We have always believed in thinking like hackers. Instead of focusing solely on compliance or theoretical frameworks, we prioritise real-world threat scenarios to design more practical and effective defences. Hackers don't follow the rules — they work around them. Our aim has been to anticipate their moves and prevent systems from being bypassed. Through the integration of advanced intelligence, technology, and human expertise, we help clients detect potential breaches before they occur and take proactive measures to contain them.

How has Resecurity contributed to enhancing the cybersecurity maturity of organisations across the GCC and MENA region?

We entered into several collaborations with universities to train students and fresh graduates in intelligence-led cybersecurity practices. We also recruited local talent to strengthen regional expertise. Since many cyber incidents originate from human error, our initiatives have focused on promoting cyber awareness and education. By doing so, we have helped reduce fraud and threat levels while supporting the

Ahmad Halabi
Managing Director
Resecurity Inc.

region's goal of building sustainable cybersecurity maturity.

What did visitors experience when they visited Resecurity's booth at GITEX 2025?
We showcased our latest AI-driven tools designed to simplify the analyst's workflow. The objective was to help security teams automate complex processes like forensics, threat detection, and reporting. With these innovations, analysts could identify vulnerabilities, generate reports, and implement fixes with just a few clicks. Our integration of AI and DevOps enabled faster investigation and remediation, allowing teams to focus on strategic threat response rather than manual analysis.

STARLINK UNVEILS 'STARLINK 5.0' — AN AI-DRIVEN PLATFORM VISION FOR THE NEXT FIVE YEARS

MARKING ITS 20TH ANNIVERSARY, STARLINK EVOLVES FROM CYBERSECURITY DISTRIBUTOR TO AI-POWERED DIGITAL PLATFORM ENABLER, CONNECTING VENDORS, PARTNERS, AND CUSTOMERS THROUGH INTELLIGENT AUTOMATION AND DATA-DRIVEN INNOVATION.

StarLink marked its 20th anniversary at GITEX Global 2025 with a bold new chapter in its journey — the unveiling of its five-year vision, StarLink 5.0. Building on two decades of leadership in cybersecurity distribution, the company is now evolving into an AI-driven digital platform enabler, connecting vendors, partners, and customers through intelligent automation, data-driven insights, and vertical-specific solutions. In an exclusive conversation with CNME Editor Mark Forker, Ahmed Diab, COO at StarLink, discussed the company's transformation, its proactive approach to market needs, and how its AI-powered platform is redefining customer engagement, compliance, and innovation across the region's digital ecosystem.

What was StarLink's main message and focus at GITEX Global 2025?

We used GITEX as a platform to announce our strategy and celebrate our 20th anniversary. This year, we also launched our five-year vision — "StarLink 5.0." It marks our evolution from being purely a cybersecurity leader to becoming an AI-driven, digital platform enabler. Our goal is to connect the dots between vendors, partners, and customers by providing relevant solutions and practices that align with their digital transformation journeys.

How challenging has it been to transition from a traditional cybersecurity distributor to an AI-driven platform company?

It hasn't been difficult as much as it's been a lot of work. This shift has been a natural evolution rather than an overnight decision. We started this journey five years ago with what we called "Intelligent Automation," which has now matured into our AI-driven vision. It's been about formalising what we've already been doing — using intelligent systems and agentic models to evolve our business.

StarLink operates in a highly competitive distribution market. What differentiates the company from others?

Our biggest differentiator is that we are customer-centric and proactive. We don't wait for events or problems to occur before responding. Instead, we continuously engage with customers and partners to understand their needs. Internally, we leverage huge volumes of data through automation and AI to predict trends and prepare tailored approaches for different markets. Moreover, we're not just a distributor — we're a digital platform that connects vendors, technologies, services, and partners to deliver complete solutions for end customers.

Can you elaborate on StarLink's new AI-driven platform and five-year vision?

For the first time, we've announced a five-year roadmap built around an agile, flexible platform capable of adapting to rapid technological change. This platform is designed around AI agents that communicate with each other, providing internal and external collaboration. These AI agents help us deliver vertical-specific use cases to customers — for example, in government, banking, oil and gas, telecom, or education sectors — ensuring relevance and measurable outcomes.

How is StarLink addressing the challenges and opportunities of agentic AI adoption across enterprises?

We're learning and teaching simultaneously. As we develop our own AI-driven processes, we also guide our customers through how to use these technologies safely and effectively. There's a lot of potential, but also risk, if AI isn't managed properly. To address this, we've established five practice areas: Cyber Resilience, Digital Infrastructure, Cloud Transformation, Agentic Automation, and Enterprise AI. These help customers manage data securely, ensure AI-human collaboration is compliant, and govern access and privileges properly.

Ahmed Diab
Chief Operating Officer
StarLink.

WE'RE EVOLVING FROM BEING A CYBERSECURITY LEADER TO BECOMING AN AI-DRIVEN DIGITAL PLATFORM ENABLER — CONNECTING VENDORS, PARTNERS, AND CUSTOMERS THROUGH INTELLIGENT, PROACTIVE SOLUTIONS.

How does StarLink view its role in ensuring the secure and compliant use of AI?

We act as an enabler and intermediary — helping customers and partners adopt AI confidently while ensuring security and compliance. Our platform allows them to innovate with AI without losing control over data or breaching regulations. This balance between innovation and governance is key to sustainable digital transformation.

What makes GITEX such a valuable platform for StarLink?

GITEX has always been more than just a marketing or branding opportunity for us. It's a chance to meet customers and partners face-to-face, announce strategies, and most importantly, listen. Many come to us looking for answers or to understand new trends. The live feedback we receive here is invaluable in shaping our roadmap and ensuring we remain aligned with market needs. While it's emotional to leave Dubai World Trade Centre, we're excited about the new chapter at Expo City next year.

ZSCALER CHAMPIONS 'ZERO TRUST EVERYWHERE' TO SECURE THE EXPANDING CONNECTED WORLD

ZSCALER REINFORCED ITS LEADERSHIP IN CLOUD SECURITY, UNVEILING INNOVATIONS THAT STRENGTHEN ZERO TRUST ADOPTION ACROSS IOT, OT, AND AI-DRIVEN ENVIRONMENTS.

GITEX Global 2025 served as a powerful stage for Zscaler to reaffirm its global leadership in secure cloud services, processing more than 500 billion transactions each day and safeguarding around 45% of Fortune 2000 enterprises. The company placed a strong focus on its theme 'Zero Trust Everywhere', showcasing how its Zero Trust Exchange seamlessly connects users, devices, and applications in a secure, policy-driven environment.

In conversation with CNME Editor Mark Forker, Vinay Polurouthu, Product Management Director at Zscaler, detailed how the company is tackling the evolving cybersecurity landscape—particularly the vulnerabilities within IoT and OT ecosystems—through its plug-and-play SIM solution and AI-driven innovations. He also outlined how Zscaler's deep integration of AI and its unified Zero Trust approach are enabling organisations to achieve scalable, end-to-end protection across today's hyperconnected world.

Could you give us an overview of what Zscaler showcased at GITEX Global 2025 and the key message you aimed to convey?

The company highlighted its leadership in secure cloud services and its commitment to advancing Zero Trust security. Zscaler, as one of the largest secure cloud companies globally, processes over 500 billion transactions per day and protects about 45% of Fortune 2000 companies. At GITEX, we focused on our innovations around Zero Trust and Zscaler for users — underlining our theme of 'Zero Trust Everywhere'. Our booth demonstrations showcased how users, applications, and devices could securely connect through our Zero Trust Exchange platform.

How did Zscaler address the challenges surrounding OT and IoT security, particularly in environments with headless devices?

OT and IoT devices had long posed challenge for cybersecurity because they were typically headless and lacked the ability to run security agents. Many of these devices operate with default passwords, making them extremely vulnerable and easy targets for hackers. Attackers often exploit them as launch pads to reach the organisation's crown jewels. To counter this, we introduced a unique innovation for IoT, OT, and cellular devices — a plug-and-play SIM solution developed in partnership with service providers. Once connected, all traffic passes through our Zero Trust Exchange, allowing complete visibility, policy enforcement, and anomaly detection. Every data flow was inspected, offering defence in depth and comprehensive protection.

Given the exponential growth of connected devices, how did Zscaler's Zero Trust Exchange help organisations manage IoT security at scale?

The scale of the IoT ecosystem represented both a challenge and an opportunity. By 2030, we expect nearly 7.9 billion cellular IoT devices and over 40 billion IoT devices globally. Zscaler's Zero Trust Exchange was built to handle this kind of scale. It inspects traffic from billions of endpoints, ensuring consistent visibility and security. Whether it's an EV charger, a kiosk, or any industrial IoT device, customers could simply plug in the SIM and apply Zero Trust policies to ensure end-to-end visibility and protection.

AI has become both a defence mechanism and a potential threat in cybersecurity. How did Zscaler leverage AI to enhance its resilience?

The sophistication of AI-driven attacks had grown significantly and adversaries are now using AI to automate and personalise attacks — from advanced phishing campaigns to stealth ransomware that encrypts data silently. To stay ahead, we must fight AI with AI. At Zscaler, our AI capabilities power nearly every part of our platform —

from anti-malware and intrusion prevention to phishing detection and URL filtering. We also focused on protecting generative AI tools and agentic AI systems by providing visibility and security guardrails against model poisoning and data leakage. Our goal has been to embed AI deeply across our defences to stay a step ahead of attackers.

Zscaler strongly advocates for a 'Zero Trust Everywhere' approach. What did this concept mean, and why was it central to your message at GITEX?

'Zero Trust Everywhere' means applying consistent Zero Trust principles regardless of user location, device type, or workload. Whether the user is on campus, in a branch office, working remotely, or operating an IoT device, the same security policies, visibility, and enforcement apply. This unified approach ensures end-to-end protection and a single, consolidated view across the enterprise. Through our Zero Trust Exchange, users, workloads, and devices connect securely without relying on implicit trust. It's this principle that underpins everything we showcased at GITEX — ensuring customers can operate safely and efficiently in an increasingly connected world.

GE VERNOVA PUTS AI AT THE CENTRE OF FUTURE-READY GRIDS

A NEW GE VERNOVA WHITE PAPER MAPS THE PRACTICAL AI PLAYBOOK FOR RESILIENT, CYBER-SECURE, AND RENEWABLE-READY POWER SYSTEMS.

GE Vernova has doubled down on the case for AI in the grid, releasing AI at the Helm: Redefining the Future of the Grid ahead of ADIPEC 2025 (3–6 November, ADNEC, Abu Dhabi). The paper underpins the company's Gold Sponsor presence, translating AI from buzzword to blueprint for utilities across the GCC as they balance decarbonisation, electrification and cyber risk.

From ambition to architecture

The research argues that AI is now a core system capability, not an add-on. It frames five requirements that turn raw data into operational value:

- Distilling raw data from smart meters, IoT and synchrophasors to surface actionable anomalies;
- Nowcasting short-term load and renewable output to keep grids stable minute-to-minute;
- Predicting longer-horizon trends for maintenance and capacity planning;
- Optimising power flows and storage dispatch against constraints;
- Autonomous control to sense–analyse–act in near real time at the edge.

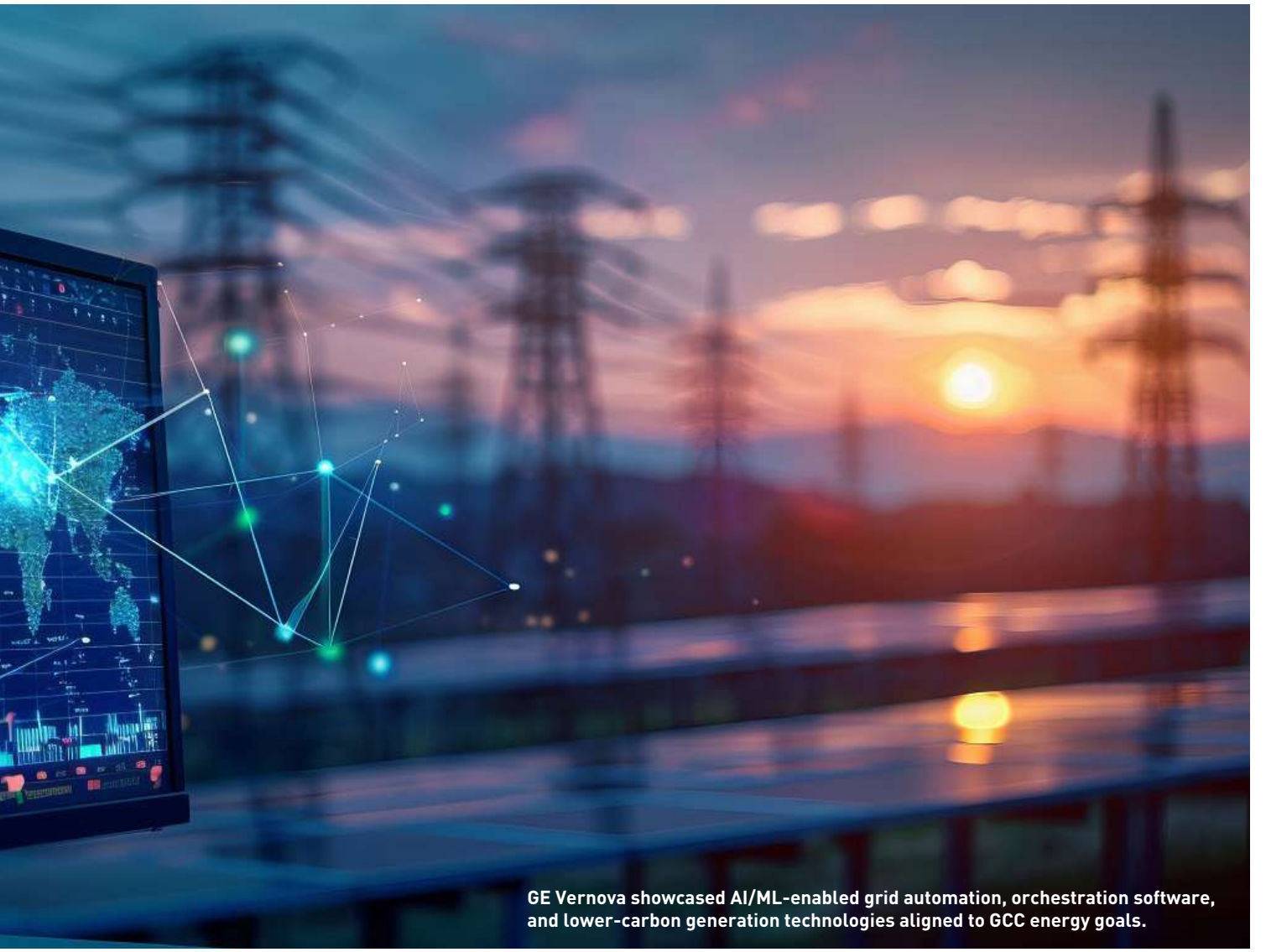
These requirements flow into five core AI applications utilities can deploy today: data analysis and prediction; near real-time adjustments (for faster load shedding and power balancing); network modelling (digital twins to test "what-ifs" before build); asset management (condition-based rather than calendar maintenance); and cybersecurity (AI-assisted anomaly detection and zero-trust by design). GE Vernova cites tangible benefits: automation that can cut response times by up to 30%, shorter outages through predictive fault detection, and more accurate planning without expensive physical upgrades.

Implementation that scales

For rollouts that stick, the paper recommends three design choices:

1. Integrate with what's there — interface with SCADA/EMS/DERMS to avoid rip-and-replace;
2. Go digital-first — software-defined automation and zonal autonomy so local issues get local responses;
3. Use hybrid cloud–edge — centralise heavy analytics while keeping sub-second decisions at substations.

It also confronts the hard parts: data



GE Vernova showcased AI/ML-enabled grid automation, orchestration software, and lower-carbon generation technologies aligned to GCC energy goals.

quality and standardisation across fragmented sources; cybersecurity for distributed, AI-infused assets; and continuous update requirements so models, algorithms and controls evolve without operational disruption.

Operating model matters

Beyond technology, the guidance is pragmatic: start with phased pilots (e.g., wind-heavy microgrids or digital substations), embed continuous monitoring and model refresh, formalise stakeholder collaboration with regulators and communities, and invest in workforce training so operators can interpret predictive alerts and manage autonomous systems. The message is clear: most AI projects fail on adoption, not algorithms.

What's next

Looking ahead, the paper points to deep learning for higher-precision forecasts and fault detection; scaled autonomous control across city-level microgrids; and tighter integration with IoT and 5G to move data and decisions at grid speed.

ADIPEC showcase

At ADIPEC, GE Vernova demonstrates how this research translates into products and projects: lower-carbon, hydrogen-capable gas turbines and carbon capture integration; synchronous condensers and BESS; SF_6-free switchgear; plus GridBeats software-defined automation and GridOS orchestration. Sessions on the stand will also cover grid cybersecurity, DER management and AI-driven diagnostics — with a regional context shaped by the company's 90-year GCC presence and recent investments, including manufacturing and service hubs in Saudi Arabia and the UAE.

For a region managing rapid renewable integration, rising demand from electrification and data centres, and intensifying cyber threats, the takeaway is actionable: put AI at the helm — and design for interoperability, security and continuous improvement from day one.

Haider Pasha
Chief Security Officer, EMEA
Palo Alto Networks.

UAE FIRMS LEAD GLOBAL CHARGE IN ADOPTING AGENTIC AI FOR CYBERSECURITY

NEW PALO ALTO NETWORKS SURVEY REVEALS 98% OF UAE ORGANISATIONS ARE USING AUTONOMOUS AI SYSTEMS TO COUNTER RISING CYBER THREATS

The UAE organisations are racing ahead in the global adoption of Agentic AI to protect their networks against a new wave of cyber threats. A new survey commissioned by Palo Alto Networks has found that 98% of companies in the country have already deployed Agentic AI in their cybersecurity operations.

Conducted by Censuswide among 250 UAE-based CEOs, the study revealed that 53.2% of organisations have AI-driven systems in full production, while 44.8% are still in pilot phases. The momentum shows no sign of slowing, with nearly all respondents planning to increase their investment in Agentic AI between 2025 and 2026.

The research also highlights a significant rise in cyber risks. Three out of four organisations (75%) reported a jump in the volume or complexity of cyberattacks this year compared to 2024. Nearly all participants (99.2%) believe that cybercriminals are already using autonomous AI agents to enhance or automate attacks, intensifying the need for defensive innovation.

Despite the growing threat landscape, UAE executives remain optimistic about the benefits of AI. The survey found that 89.2% of respondents expect Agentic AI to reduce cybersecurity risks in the next 12 months, while just 2.4% believe it could increase them.

However, several barriers are slowing adoption. The biggest challenges cited include integration with legacy systems (26.4%), lack of trust in AI autonomy (20.8%), unclear regulation (20.4%), limited in-house expertise (18.4%), and cost (13.6%).

"The survey results are a sobering reminder of the need to act decisively in using AI-based tools to combat AI-driven threats," said Haider Pasha, Chief Security Officer, EMEA, Palo Alto Networks. "While it's reassuring to see the UAE moving swiftly, the confidence levels reflected in the findings could suggest a degree of over-optimism — particularly given the challenges of integrating legacy systems. This highlights the importance of platformisation to consolidate cybersecurity functions and strengthen defences against emerging threats."

The survey also explored which cybersecurity domains are likely to be most transformed by Agentic AI over the next year. Incident response topped the list (24.8%), followed by identity and access management (22%) and attack surface management (20.4%). Other areas expected to see major automation include security operations centre (SOC) workflows and threat detection.

To ensure responsible and effective adoption, UAE businesses are calling for greater regulatory clarity (24%), access to skilled talent (23.6%), and stronger industry partnerships (18.8%). Encouragingly, 98% of respondents expressed confidence in their cybersecurity teams' ability to manage and govern Agentic AI systems responsibly — with more than half saying they were "very confident."

Palo Alto Networks showcased its latest Agentic AI innovations at GITEX Global 2025, underlining its ongoing commitment to helping regional enterprises secure their digital transformation journeys.

UAE ORGANISATIONS ARE ACTING FAST TO USE AI-BASED TOOLS TO FIGHT AI-BASED THREATS — BUT LEGACY SYSTEMS REMAIN A KEY CHALLENGE.
HAIDER PASHA, PALO ALTO NETWORKS

GULF CYBERSECURITY SPEND TO TOP DH120 BILLION BY 2030 AS AI FUELS NEW ERA OF SOVEREIGN RESILIENCE

REGIONAL CYBERSECURITY SPENDING TO DOUBLE BY 2030, WITH THE UAE'S AI-DRIVEN SECURITY MARKET SET TO GROW MORE THAN FOURFOLD TO EXCEED DH19.6 BILLION

Cybersecurity spending across the Gulf is projected to surpass Dh120 billion by 2030, as artificial intelligence, sovereign cloud strategies, and hyperscale data infrastructure redefine the region's digital future, according to a new report from Grand View Research, Cyber Resilience in the Gulf: Where Technology Meets Sovereign Risk (2025 Edition).

As both UAE and Saudi Arabia fast-track their digital transformation agendas under 'We the UAE 2031' vision and Vision 2030 programmes, the new report finds that the region's ambitious infrastructure buildout – spanning national data centers, AI clusters, and cloud corridors as part of much-talked about 'giga projects' like NEOM, Qiddiya and the Red Sea Global– is fuelling an unprecedented wave of investment in cyber resilience and data sovereignty.

"The Gulf's digital leap has been extraordinary – but it's also created a new kind of interdependence," said Swayam Dash, Managing Director of Grand View Research. "Cyber resilience has evolved from a technical discipline to a sovereign capability – it now defines how nations sustain growth, attract capital, and maintain public trust."

UAE and Saudi anchor a new model of sovereign resilience

Together accounting for over 60% of the region's cybersecurity expenditure, the two nations are transforming digital protection into a cornerstone of national policy.

In the UAE, cybersecurity investments are being channeled toward AI-driven threat intelligence, zero-trust frameworks, and sovereign cloud ecosystems – a key focus of the country's Cybersecurity Strategy 2025-31. Meanwhile, Saudi Arabia's National Cybersecurity Authority (NCA) and SDAIA are embedding data protection and cyber readiness across industrial and infrastructure projects tied to Vision 2030.

"The Gulf's new digital infrastructure – from hyperscale data centers to AI-powered governance – is the backbone of its economic transformation, securing it is no longer optional; it's the new definition of economic sovereignty," added Dash.

From firewalls to frameworks

According to Grand View Research, the region's cybersecurity approach is shifting from network defense to institutionalized resilience through policy, collaboration, and redundancy. Key milestones include the ADGM Cyber Risk Management Framework (2025), integrating cyber continuity into financial regulation, Saudi Central Bank's cyber stress-testing regime, simulating real-world digital disruption and cross-border CERT intelligence sharing, creating early-warning systems across GCC nations.

"The Gulf's greatest advantage is its ability to move as one," Dash added. "Unified governance allows GCC nations to integrate cybersecurity, business continuity and defense into a single sovereign doctrine."

Cyber resilience as an economic benchmark

As the line between cyber disruption and

THE GULF'S NEW DIGITAL INFRASTRUCTURE – FROM HYPERSCALE DATA CENTERS TO AI-POWERED GOVERNANCE – IS THE BACKBONE OF ITS ECONOMIC TRANSFORMATION, SECURING IT IS NO LONGER OPTIONAL; IT'S THE NEW DEFINITION OF ECONOMIC SOVEREIGNTY.

Swayam Dash
Managing Director
Grand View Research

economic disruption narrows, investors are beginning to treat digital resilience as a new form of sovereign credit. Gulf banks now include cyber metrics in ESG disclosures, while regulators view system uptime as a proxy for fiscal stability. "Technology can be imported – resilience must be built," Dash concluded. "The Gulf's next global advantage won't come from faster networks, but from networks that never fail."

The MEA cybersecurity sector, according to the study, generated $16.5 billion (Dh60.6 billion) in 2024 and is expected to reach $32.9 billion (Dh120.7 billion) by 2030, expanding at a compound annual growth rate (CAGR) of 12.5% between 2025 and 2030.

In the UAE, the IT & telecom cybersecurity market is set to grow from $333.2 million (Dh1.22 billion) to $740.1 million (Dh2.72 billion) by 2030 – a 14.5% CAGR while the country's AI in cybersecurity market will skyrocket from $1.2 billion (Dh4.4 billion) to $5.36 billion (Dh19.7 billion) by 2030, expanding at a 27.4% CAGR, the fastest in the region.

In Saudi Arabia, AI-based cybersecurity revenue is projected to jump from $1.25 billion (Dh4.59 billion) to $4.49 billion (Dh16.47 billion) by 2030, at a 22.8% CAGR.

From firewalls to frameworks

"The Gulf's strategy has matured from protecting networks to institutionalising resilience through regulation, coordination, and redundancy," said Dash while talking about recent milestones like ADGM Cyber Risk Management Framework (July 2025) – mandating continuity integration for all financial firms, Saudi Central Bank's stress-testing regime – simulating real-world cyber shocks and Cross-border CERT intelligence sharing – building regional early-warning systems.

"The Gulf's biggest advantage is its ability to move as one," Dash noted. "Unified governance allows GCC nations to integrate cybersecurity, business continuity, and defense into a single sovereign doctrine."

Zero-Trust and Training: Building Indigenous Capacity

The UAE zero-trust market – emphasising continuous identity verification – is forecast to grow from USD 326.2 million (Dh 1.2 billion) to $944.9 million (Dh3.47 billion) by 2030. The MEA cybersecurity training market will expand from $405.9 million (Dh1.49 billion) in 2023 to $1.36 billion (Dh4.99 billion) by 2030, reflecting a regional drive to build local expertise and sovereign data control.

Ahmed El Saadi
Vice President, Middle East Africa, Turkey, Romania, and CIS, Splunk.

DRIVING CHANGE, SEEN AND UNSEEN: LLMS IN THE MIDDLE EAST'S CYBERSECURITY ARENA

AHMED EL SAADI DISCUSSES THE ROLE OF LARGE LANGUAGE MODELS (LLMS) IN SUPPORTING REGIONAL CYBERSECURITY TEAMS.

Large language models (LLMs) are quickly becoming a defining factor in cybersecurity. For security teams, they offer faster ways to detect and investigate threats; for attackers, they lower the bar to launch phishing, fraud, and malware at scale.

In the Middle East, this dual impact is magnified by heavy government investment in artificial intelligence and digital transformation. The UAE has set its sights on becoming one of the world's top 10 AI-ready nations by 2031, while Saudi Arabia and other regional economies are prioritising AI adoption across critical sectors. Security software is projected to remain the largest technology spending area in MENA, expected to reach nearly $1.5 billion by 2025 — a reflection of both rapid digital growth and the pressing need to secure it.

Middle East Snapshot

- LLMs as a double-edged sword: LLMs can be used to streamline detection, triage, and investigation workflows for security operations centres, but also enable attackers to replicate known threats more efficiently and quickly.
- Governance is essential: PwC's 2025 Digital Trust Insights [AO2] report found that 73% of Middle East organisations view cybersecurity as a strategic growth driver, underscoring the need to balance innovation with risk management.
- Preparing for autonomy: The UAE ranks 13th globally in government AI readiness [AO3] , positioning the region to both benefit from and defend against the next generation of autonomous, AI-driven cyber threats.

Current Relationship Between LLMs and Threat Actors

LLMs can democratise access to cyber-attack knowledge, enabling individuals with limited technical skills to generate functional code or craft convincing phishing content in Arabic and English.

In recent years, the Middle East and Africa have seen a marked rise in phishing and online fraud targeting high-value sectors such as banking, energy, and government services. Regional threat intelligence reports have noted an increase in phishing websites impersonating postal services, utilities, and major brands, often designed to harvest sensitive credentials or deliver malware. Increasingly, these campaigns incorporate AI-generated text and imagery, making them more persuasive and harder for traditional security filters to detect.

Using LLMs Correctly

While LLMs offer significant operational benefits, misuse or lack of oversight can introduce new vulnerabilities.

Public-sector ambitions illustrate the opportunity. The UAE's AI Strategy 2031 aims to integrate AI across critical domains, from energy to healthcare, with an anticipated AED 335 billion [AO4] contribution to the national economy by 2031. To harness this potential safely, organizations should:

1. Identify repetitive, high-volume, text-heavy tasks where LLMs deliver measurable value.
2. Define "human-in-the-loop" checkpoints to verify outputs before they inform security decisions.
3. Regularly audit and retrain models to ensure relevance against evolving regional threats.

Underlying Potential for Cyber Defenders

Once analyst teams determine when and how to use AI effectively, there is a real chance to optimise productivity using LLMs. Just like LLMs can help mitigate burnout for content creation or research, they can also help analysts streamline and triage security alerts and event review.

Due to their ability to comprehend human language, cyber analysts can fine-tune LLMs to help with increasingly specific cyber-domain-related tasks. Models can also help speed up post-cyber incident issues, such as summarising the details of an attack and the SOC's corresponding response.

In a Splunk threat hunting exercise, multiple open-weight LLMs were evaluated on their ability to classify the intent of 2,000 PowerShell scripts – 1,000 benign and 1,000 malicious. The results produced a promising combination of high accuracy, with very few false negatives. Classification time ranged from 0.75 seconds to 3 seconds per script, representing a 99% reduction compared to the 5–12 minutes typically required by a human analyst.

In a Middle East context, this capability could dramatically improve SOC efficiency, particularly in sectors like banking, oil & gas, and government services, where incident response windows are often measured in minutes.

What the LLM Future Holds for Both Defender and Attacker

The next wave of LLM adoption will see greater use of agentic AI — systems capable of making and executing decisions independently. For defenders, this could automate large portions of SOC workflows; for attackers, it could mean more adaptive and persistent cyber campaigns.

The UAE has announced plans to integrate an AI advisory system into its federal cabinet in 2026 [AO5] , signalling the speed with which AI is being embedded in governance. Across the GCC, AI is projected to contribute up to USD 260 billion to GDP [AO6] , further entwining these technologies with national infrastructure.

This deep integration makes it essential for governments and enterprises to:

- Invest in AI literacy and skills for SOC teams.
- Establish robust governance for AI deployment.
- Expand cross-border intelligence sharing to counter emerging threats.

The Middle East's AI-driven transformation brings unparalleled opportunities for cyber defence – but also new attack surfaces for adversaries. LLMs will be central to both. The advantage will go to those who combine advanced tooling with human expertise, cultural and linguistic awareness, and a readiness to adapt as technology and threats evolve.

SECURITY SOFTWARE IS PROJECTED TO REMAIN THE LARGEST TECHNOLOGY SPENDING AREA IN MENA, EXPECTED TO REACH NEARLY $1.5 BILLION BY 2025 — A REFLECTION OF BOTH RAPID DIGITAL GROWTH AND THE PRESSING NEED TO SECURE IT.

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

REOLINK UNVEILS REONEURA AI AND TRACKFLEX FLOODLIGHT WIFI AT GITEX

PRODUCTS ON SHOW REFLECTED INNOVATION, INTELLIGENCE, AND IMPACT

Reolink, an innovative leader in intelligent visual technology for home and businesses, today announced ReoNeura, its next-generation AI system transforming smart security, and unveiled the TrackFlex Floodlight WiFi, the world's first 4K 360-degree PTZ floodlight camera with local AI Video Search at GITEX GLOBAL 2025.

ReoNeura: AI Security for Every Moment

Tired of endless video scrubbing, missed events, or false alerts? ReoNeura™ is designed to tackle these challenges. It is Reolink's intelligent AI system that sees smarter, understands deeper, and responds faster.

In July, Reolink debuted ReoNeura, powering its AI Video Search to make video review faster and more precise. At GITEXGLOBAL 2025, the company is expanding ReoNeura™ with even more AI features. Two highlights include:

- **Smart Detection:** Includes Person & Object Detection, which identifies people, animals, vehicles, bikes and parcels. Custom zones and schedules help reduce false alerts. And Smart Event Detection (Beta), adds the ability to track deliveries and detect when objects appear or disappear, sending alerts that matter most.
- **AI Video Captioning:** Automatically converts footage into clear, natural-language summaries, allowing users to grasp what happened at a glance without watching lengthy clips.

Reolink also offers business-focused AI features, such as Customer Flow Analysis, which helps small and medium-size businesses track visitor traffic, generate 24-hour heat maps of busy zones, and receive real-time crowding alerts. These insights support clearer decision-making and more efficient operations.

Reolink is committed to bringing these smart AI features across more of its product lines. ReoNeura delivers AI across Reolink security cameras, network video recorders, and the cloud, giving users the flexibility to deploy smart features wherever they need them most.

TrackFlex Floodlight WiFi: Safety in Sight, Moments in Light

Expanding its Floodlight Camera |

Reolink Outdoor Cam with Floodlight, Reolink introduced TrackFlex Floodlight WiFi, a dual-lens hardwired PTZ floodlight camera that combines 4K ultra-HD resolution, smooth pan-tilt control, and a triple PIR sensor array. TrackFlex delivers full 360° coverage and 270° out-of-field motion detection—even auto-rotating to capture movement before subjects enter the frame. With AI Video Search built in, users can quickly locate key events for smarter, more efficient security management.

When night falls, TrackFlex shines. Its dual adjustable floodlights provide up to 3000 lumens of illumination and support both warm (3000K) and cool (6000K) color temperatures, balancing visibility, aesthetics, and security deterrence.

COMMVAULT APPOINTS DR. MAZEN ABDULJABBAR AS COUNTRY MANAGER FOR SAUDI ARABIA

VETERAN EXECUTIVE TO DRIVE COMMVAULT'S GROWTH AND CYBER RESILIENCE STRATEGY ACROSS THE KINGDOM.

Commvault has announced the appointment of Dr. Mazen Abduljabbar as its new Country Manager for the Kingdom of Saudi Arabia, marking a significant step in the company's expansion and leadership strategy across the region.

Based in Riyadh, Dr. Abduljabbar will oversee Commvault's operations, strategic growth, and customer engagement in the Kingdom as part of the company's broader Emerging Markets division.

A seasoned business leader with more than 25 years of experience, Dr. Abduljabbar brings a wealth of expertise in business development and strategic management. His previous roles include Executive Customer Director at Alstom Saudi Arabia and Executive Director of Business Development at Siemens KSA, where he managed operations across Saudi Arabia and Bahrain. Throughout his career, he has been recognised for fostering strong customer relationships and leading high-impact projects that align technology with business outcomes.

"I'm delighted to join Commvault at such a pivotal time for both the company and the region," said Dr. Abduljabbar. "Cyber resilience has become a business necessity, and Commvault plays a critical role in enabling enterprises to safeguard operations and maintain continuity. I look forward to collaborating with our customers and partners to strengthen resilience across the Kingdom."

Dr. Mazen Abduljabbar.

Yahya Kassab, Senior Director and General Manager for the Gulf and KSA at Commvault, welcomed the appointment, adding: "Dr. Mazen's proven leadership and deep understanding of the Saudi market will be instrumental in supporting our customers as they enhance their cyber resilience strategies."

Dr. Abduljabbar holds a Doctorate in Business Administration from University Technology MARA in Malaysia and an MBA from King Abdulaziz University in Saudi Arabia. His combination of academic insight and strategic leadership has consistently driven innovation and growth in complex business environments.

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

LINKSHADOW®

UNIFIED IDENTITY, DATA & NETWORK ANALYTICS PLATFORM

POWERED BY CYBER MESH ARCHITECTURE