

Security

ADVISOR

MIDDLE EAST



ERA OF CYBER CONVERGENCE

POWER. RISK. RESILIENCE.



ASUS ExpertBook B5 B5405

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



AI-empowered
productivity



Light weight and portable



Long Battery Life



Accelerate business success

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

CONTENTS



14 COVER STORY



20 CYBERWISE's vision for Middle East: Staying ahead of threats through clarity and commitment.

44 Nutanix makes NC2 generally available on Google Cloud.

34 GCC technology advancements are being driven from momentum to maturity.

48 PointGuard AI names Dev Mehta marketing director, plans to drive AI security demand



معرض و مؤتمر الخليج العالمي للأمن المعلومات

05 - 07 MAY 2026 DUBAI EXHIBITION CENTRE (DEC), EXPO CITY

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT



SCAN HERE



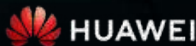
ENQUIRE FOR 2026!

#gisecglobal
gisec@dwtc.com

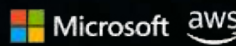
OFFICIAL DISTRIBUTION PARTNER



LEAD STRATEGIC PARTNER



STRATEGIC PARTNER



DIAMOND SPONSOR



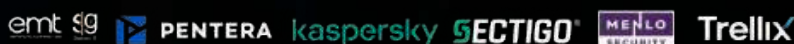
PLATINUM SPONSOR



GOLD SPONSOR



GOLD SPONSOR



EDITOR'S NOTE



Talk to us:

E-mail:
sandhya.dmello@cpimediagroup.com

Sandhya DMello
Editor

SECURITY ENTERS A NEW ERA

The year 2026 marks a decisive shift in how cybersecurity is understood, governed, and applied. No longer confined to isolated systems or technical teams, security now sits at the intersection of artificial intelligence, data sovereignty, digital infrastructure, and geopolitical influence. Across this issue of Security Advisor Middle East, one theme is unmistakable: cybersecurity has entered an era of convergence.

Our cover story, "Cybersecurity at the Centre of Power in 2026," examines this transformation in depth. From sovereign AI platforms and identity-driven attacks to risk-first security models and community-scale defence, the narrative is clear. Cyber resilience is no longer a tactical objective; it is a strategic imperative shaping national ambitions and enterprise survival alike. The challenge ahead is not innovation itself, but the ability to govern complexity, risk, and trust at scale.

This perspective carries through the pages that follow. The issue explores how organisations are rethinking AI deployment, demanding environments they can control

and trust. It also examines the growing importance of identity security in an AI-driven world, where human and non-human identities must be governed with equal discipline. At the same time, emerging threat patterns—from globally coordinated scams to regulatory milestones such as FedRAMP authorisation—highlight how quickly cyber risk adapts to real-world events.

Innovation continues to accelerate. Secure autonomy technologies are crossing borders, startup ecosystems are shaping the future of cloud security, and research featured in this

CONVERGENCE CHANGES EVERYTHING

issue reveals both progress and persistent gaps in AI governance. Together, these stories reinforce a central insight: sovereignty is not only about where data resides, but how it is used, monitored, and protected.

In the era of cyber convergence, resilience can no longer be built in isolation. It depends on shared intelligence, disciplined governance, and security strategies aligned with real business and societal outcomes. This issue aims to provide the clarity and context needed to navigate that reality with confidence and purpose.

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

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

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehanjan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

© Copyright 2026 CPI
All rights reserved

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

SAAL.AI AND NUTANIX INTRODUCE SOVEREIGNGPT, MARKING A BREAKTHROUGH IN SECURE AI INNOVATION



Vikraman Poduval, CEO of Saal.ai



Raif Abou Diab, Sales Director, South Gulf and Sub-Saharan Africa, at Nutanix

Saal.ai, a prominent UAE leader in

AI cognitive solutions, and Nutanix, a leader in hybrid multicloud computing, announced a strategic collaboration on SovereignGPT, a next-generation Agentic AI platform purpose-built for the region's most security-focused organisations.

The event was held at an exclusive gathering held at The Ritz-Carlton Abu Dhabi, Grand Canal in the presence of senior government representatives and private sector leaders,

Engineered in the UAE by Saal.ai and powered by Nutanix's globally trusted hybrid multicloud infrastructure, the platform introduces fully sovereign, on-premise Generative AI that helps ensure data never leaves the organisation's environment, whether operating on hyperconverged, hybrid, or cloud infrastructure.

Vikraman Poduval, CEO of Saal.ai, said, "SovereignGPT embodies our vision

of building AI that empowers nations and enterprises to unlock the full value of their data without compromising sovereignty or security. Together with Nutanix, we are delivering an intelligent, autonomous platform built in the UAE, for the region, enabling organisations to make faster decisions, break down data silos, and accelerate digital transformation with complete trust."

SovereignGPT gives governments, and large enterprises a fully sovereign AI platform that turns all types of data into actionable insights while staying entirely within their own infrastructure. Its advanced Agentic AI can reason and act autonomously across enterprise systems, enabling faster, smarter decisions. Built on the Nutanix Cloud Infrastructure solution, it meets strict government-grade security requirements and delivers the resilience, scalability, and high availability needed for mission-critical environments.

Raif Abou Diab, Sales Director, South Gulf and Sub-Saharan Africa, at Nutanix, commented: "Our collaboration with Saal.ai brings together world-class hybrid cloud infrastructure and advanced regional AI expertise to deliver secure, on-premise Generative AI at scale. With SovereignGPT, organisations across the Middle East can deploy high-performance AI directly where their data resides—ensuring resilience, compliance, and the freedom to innovate without constraints."

SovereignGPT represents one of the region's first fully integrated, AI-in-a-Box certified architectures. It unifies compute, storage, security, and advanced AI capabilities within a single platform, enabling organisations to accelerate digital transformation, eliminate data silos, enhance operational and supply chain performance, and activate AI-ready data foundations—all without moving sensitive information outside their infrastructure.

KASPERSKY IDENTIFIES GLOBAL SCAM ACTIVITY LINKED TO RELEASE OF AVATAR 3

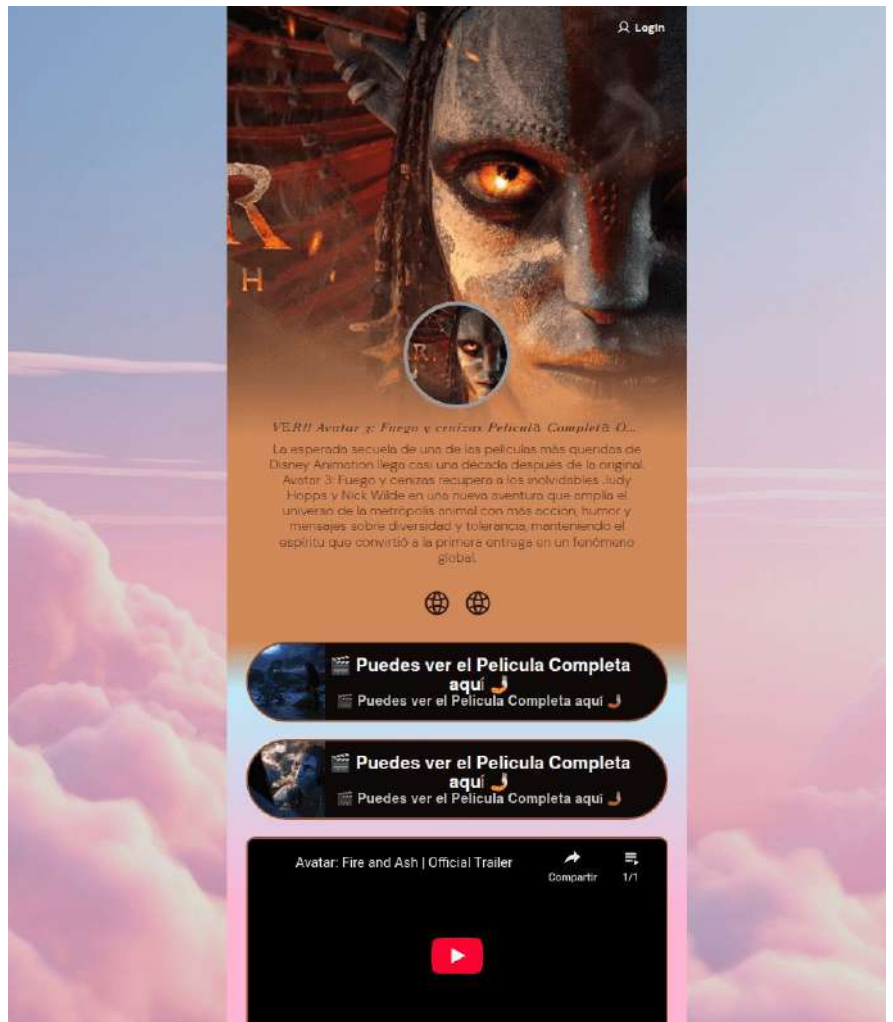
The premiere of Avatar 3 has taken place in several countries and has been accompanied by a noticeable increase in online interest. Amid the heightened attention surrounding the release, Kaspersky experts have identified an increase in cyber-scam campaigns that exploit the movie's launch and users' desire to watch it online. The fraudulent websites target users across multiple regions, indicating attempts by attackers to reach a global audience.

The scam operates as follows: cybercriminals create suspicious websites that offer online access to the Avatar 3 movie. Attackers place particular emphasis on localisation, publishing the sites in multiple languages to attract users from different countries. However, the translations are often poorly executed and contain grammatical errors and inconsistencies, which may serve as indicators of fraudulent activity.

When users attempt to start the video, they are presented with a fake media player and prompted to register in order to obtain "full" or "unlimited" access to the film. As part of the registration process, users are asked to provide personal information, including an email address and mobile phone number.

At later stages, scammers may request additional data, including payment details, under the guise of activating a "free trial." This creates risks of credential compromise, particularly if users reuse passwords across multiple services, and may also lead to financial losses.

"Cybercriminals consistently exploit major movie premieres to capture users' attention and increase the effectiveness of their schemes. We advise accessing films only through official platforms and exercising caution when encountering websites that request personal or payment information. It is also important



to use reliable security solutions to protect all devices, including mobiles," comments Olga Altukhova, Senior web content analyst at Kaspersky.

To avoid falling victim these scams, Kaspersky advises users to:

- Check the authenticity of websites before entering personal data and only use official webpages to watch movies. Double-check URL formats and company name spellings.
- Always choose official and reputable streaming platforms to protect your personal data from theft and misuse.
- Use a reliable security solution,

such as Kaspersky Premium, that identifies malicious attachments and blocks phishing links. The quality of security solutions' phishing detection is annually evaluated by independent testing labs. For example, in 2025 and 2024 Kaspersky Premium achieved a 93% detection rate with 0 false positives in AV-Comparatives anti-phishing tests, and was awarded with the "Approved" certificate.

- Enable multi-factor authentication and monitor accounts: Activate 2FA on Apple ID and financial apps and regularly review statements for unauthorised activity.

UAE SECURE AUTONOMY TECH SET FOR EUROPE VIA VENTUREONE PARTNERSHIPS

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

VentureOne, the Advanced Technology

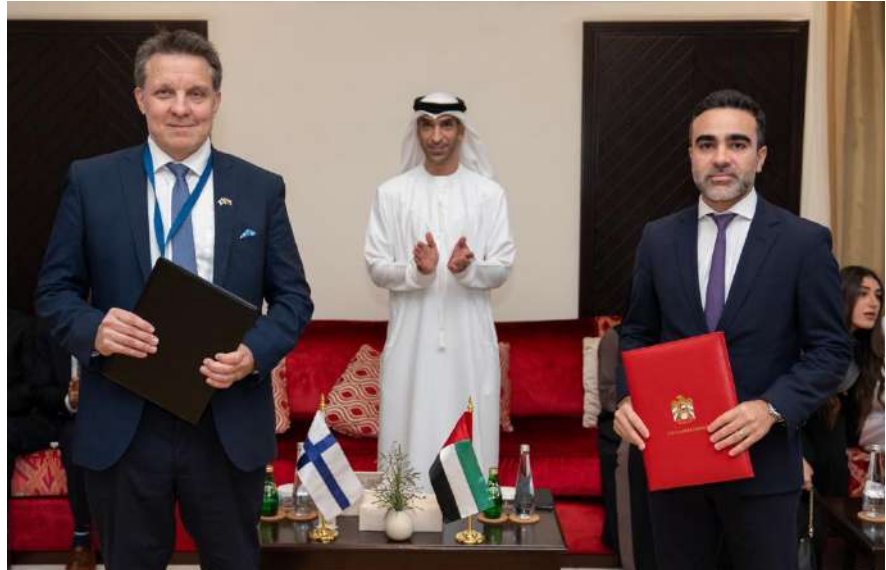
Research Council (ATRC)'s venture builder, has confirmed its first European deployment through new agreements with Finland's Unikie and Solita. The partnerships will explore integration of UAE-made secure technologies into public safety, security, and infrastructure projects across Finland and northern Europe as nations worldwide accelerate efforts to strengthen critical systems.

Unikie, a global software engineering and innovation company, and Solita, a European AI and data transformation company, will add several of VentureOne's secure flight technologies to their portfolios: Saluki, a high-security flight control and mission computing solution, as well as a mesh networking system that enables secure communications and mission orchestration. The companies will also explore applications for VentureOne's GNSS-Less, a navigation solution that does not require GPS signals to operate.

"VentureOne exists to put made-in-the-UAE deep tech to work driving tangible positive change on an international scale," said Chris Walton, VentureOne's Senior Director. "Unikie and Solita bring extensive expertise in integrating smart technology and autonomy into critical infrastructure projects, making them an ideal European deployment partner for us. We're just getting started on what these partnerships will deliver."

Developed by the Technology Innovation Institute (TII), ATRC's applied tech research arm, the solutions support secure, resilient, autonomous operations in drones and vehicles, even in challenging environments:

Saluki offers Zero Trust architecture



Juha Ala-Laurila, CEO of Unikie, and Reda Nidhakou, CEO of VentureOne, with His Excellency Dr. Thani bin Ahmed Al Zeyoudi, UAE Minister of Foreign Trade.

for autonomous systems that supports AI and multi-vehicle operations, enabling safeguarded commercial flights, mission-critical reliability, and hardened control logic for drone missions.

The mesh networking system extends the range of human-machine collaboration by powering secure, tamper-proof communications from one drone to another and between drones and humans, as well as enabling mission orchestration.

GNSS-Less offers a secure, vision-based alternative to satellite navigation. While traditional GPS can be vulnerable to interference, leading to compromised navigation and tracking, GNSS-Less prevents jamming and spoofing, significantly increasing flight safety and security.

"Unikie is one of the leading tech companies developing intelligent autonomous systems for vehicles and drones," said Juha Ala-Laurila, Unikie's

CEO. "We have extensive expertise in autonomous operations, security, and the application of AI within software engineering. Through this partnership with VentureOne, we are even better equipped to provide advanced secure technologies to our customers, thus contributing to a safer Europe."

"Contributing to the security of Europe's critical infrastructure is a mission we are deeply invested in," said Ossi Lindroos, Solita's CEO. "By combining VentureOne's state-of-the-art technological solutions with our long-standing expertise of secure software systems, data, AI, and connectivity, we are well positioned to help build safer and more resilient societies."

These new agreements build on a recently announced partnership between Business Finland and ATRC, designed to accelerate R&D exchange, co-develop new solutions, and strengthen innovation in each ecosystem.

CROWDSTRIKE, AWS, AND NVIDIA SELECT 35 STARTUPS FOR THE 2026 CYBERSECURITY STARTUP ACCELERATOR

CrowdStrike has announced the 35 startups selected for its third annual Cybersecurity Startup Accelerator with Amazon Web Services (AWS) and NVIDIA through its Inception program, fuelling the next generation of AI-driven cloud security innovation. Chosen from hundreds of global applicants, the elite group was selected for the strength of their innovation, potential to make market impact, and caliber of their teams.

The free, eight-week program runs from today through March 3, 2026, providing startups with mentorship, technical expertise, funding and go-to-market support, along with access to top cybersecurity experts and global visibility across partner ecosystems.

The program will culminate in a final pitch day for five finalists during the RSA Conference in



Daniel Bernard, chief business officer at CrowdStrike.

San Francisco on March 24, 2026, where an expert panel will select one innovation award winner, with potential for investment from the CrowdStrike Falcon® Fund.

“The Cybersecurity Startup Accelerator has become a launchpad for the next era of AI-driven security innovators,” said Daniel Bernard, chief business officer at CrowdStrike. “This year’s cohort reflects a global movement: founders building cloud- and identity-first defenses that put security teams ahead of the speed and scale of AI-emboldened adversaries. With AWS and NVIDIA, we’re creating community and growing “the crowd,” giving these startups the opportunity to turn breakthrough ideas into market-shaping technologies, and push the industry forward.”

“Startups continue to push the boundaries of what’s possible in AI-driven security,” said Chris Grusz, managing director,

technology partnerships at AWS. “The third year of the Cybersecurity Startup Accelerator once again brings together the power and expertise of AWS, CrowdStrike, and NVIDIA to help these innovators accelerate development, strengthen their platforms, and scale their transformative solutions faster.”

“AI is reshaping cybersecurity at every level, demanding new approaches that can operate at cloud scale and defender speed,” said Bartley Richardson, senior director of agentic AI and cybersecurity engineering at NVIDIA. “Through the accelerator, NVIDIA, AWS, and CrowdStrike are empowering startups with the compute, frameworks and guidance they need to advance agentic AI and build the next wave of intelligent, resilient security technologies.”

- | | |
|------------------|-------------------|
| The 2026 cohort | Mars Security |
| Above Security | Mate Security |
| Aira Security | NANO Corp |
| Artemis | Nebari |
| Astelia | Nimble Security |
| Averlon | Opti |
| Capsule Security | Pluto Security |
| Dash Security | QIZ Security |
| Drift Security | Raven |
| Dux Security | Sevii |
| Evoke Security | Simbian AI |
| Fabrix | SurePath AI |
| Fortyx Security | Synqly |
| Geordie AI | Tika Security |
| Haleum AI | VisionHeight |
| Hush Security | Vivid Security |
| Huskeys | Zepo Intelligence |
| Jazz | |

CIQ DELIVERS TURNKEY SOVEREIGN AI WITH SERVICE ENDPOINTS CAPABILITY, TRANSFORMING FUZZBALL INTO COMPLETE TRAINING, INFERENCE PLATFORM

CIQ, the founding support and

services partner of Rocky Linux and a leader in high-performance software infrastructure, today announced Service Endpoints, a new capability for its Fuzzball platform. Service Endpoints enables Fuzzball to be a turnkey, sovereign AI infrastructure platform by unifying model training, fine-tuning, validation and inference in single, portable workflows. Organisations can now develop and serve AI models entirely from on-premises or hybrid environments, eliminating reliance on external platforms while maintaining complete control over proprietary and sensitive data.

Service Endpoints brings training and inference into a single, portable workflow so teams stop treating deployment as a separate platform and a manual handoff. Service Endpoints lets users define and run persistent endpoints alongside training and fine-tuning steps within the same orchestrated pipeline. The result is accelerated time to first token, fewer brittle deployment pipelines, less unbudgeted technical debt and more time reclaimed for iteration and innovation as AI initiatives scale.

The capability combines batch computing (for training and fine-tuning) with persistent services (for high-performance inference and interactive development) in unified workflow definitions. This solves a critical challenge in sovereign AI: existing platforms force organisations to choose between cloud convenience and data sovereignty, or to custom build separate systems for model development and deployment. Fuzzball delivers both capabilities in a single platform leveraging workflows that run identically on premises, in cloud or across hybrid

environments.

“Organisations want to use AI with their proprietary data in environments that they control, without sending their data to external platforms,” said Jonathon Anderson, Fuzzball Product Lead at CIQ. “Fuzzball Service Endpoints treats the entire AI stack as a composable unified workflow that can be iterated on and refactored to meet your specific requirements. This gives you complete control over your AI experience, whether you’re fine-tuning a model or orchestrating a suite of coordinating agents.”

Beyond sovereign AI, Service Endpoints fundamentally changes how researchers and engineers interact with other use cases of high-performance computing. Service Endpoints provides native support for Jupyter, VDI, visualisation and other services while enabling real-time inspection and adjustment of running workflows. This allows researchers to observe simulations in progress, validate results midstream and guide

computations as they run, accelerating innovation cycles across research domains.

All batch jobs, internal services and interactive endpoints are defined and managed within a single, portable Fuzzball workflow. This unified approach eliminates the complexity of coordinating separate systems and ensures workflows remain reproducible and portable across any Fuzzball environment.

The new capability enables three distinct categories of high-impact use cases:

- Turnkey sovereign AI: Fuzzball simplifies technical complications in sovereign AI. With it, teams can deploy the complete AI lifecycle, from data ingestion through training, fine-tuning, validation and inference, as a single workflow without external dependencies. Your AI stack runs identically on-premises or in the cloud and eliminates the complexity of integrating separate systems. Teams maintain complete control over proprietary data while achieving simplicity previously only available through proprietary cloud platforms. For regulated industries, defense applications and organisations with data sovereignty requirements, this delivers both compliance and velocity.
- High-performance service (inference) processes: Traditional microservice platforms often prioritise web functionality at the expense of performance. Fuzzball Service Endpoints supports automated coordination within and between workflows, allowing batch jobs and persistent services (such as databases, parallel compute environments



Jonathon Anderson, Fuzzball Product Lead, CIQ

and APIs) to communicate seamlessly without impacting performance.

- Interactive access to HPC resources: Whether you use Jupyter notebooks, virtual desktops or other interactive or visualisation tools, Fuzzball makes it easy to use your high-performance

resources interactively in real time. This democratises HPC access for data scientists and researchers who need or prefer GUI-based environments while working at cluster scale.

Fuzzball Service Endpoints is designed specifically for performance-sensitive

environments. It preserves bare metal performance while introducing service-oriented flexibility. Reference workflows and catalog examples, including virtual desktops, Jupyter notebooks, visualisation tools and sovereign AI stacks are available at launch to help users get started quickly.

CORALOGIX ANNOUNCES U.S. DEPARTMENT OF EDUCATION SPONSORSHIP FOR FEDRAMP AUTHORISATION

Coralogix, the leading full-stack

observability platform, today announced that the U.S. Department of Education's Federal Student Aid will serve as the official sponsoring agency for the company's pursuit of a FedRAMP Moderate authorisation. Coralogix will be the first AI observability platform to achieve this milestone.

Upon earning this certification, Coralogix will be approved to provide U.S. federal agencies with its secure AI-powered observability platform, which delivers real-time visibility into all AI applications. By offering comprehensive, real-time insights into AI performance, quality, security, and governance within a single platform, Coralogix will empower agencies to accelerate AI adoption and manage AI agents with confidence.

As federal agencies increasingly adopt AI-driven analytics and multicloud strategies, the need for secure, centralised oversight has never been greater. Unlike other AI observability vendors, Coralogix reviews the content of the user and the AI to determine whether, for example, an exchange contains toxicity, the AI is hallucinating, or a bad actor is trying to breach the chatbot to steal data. By consolidating capabilities that typically require up to ten separate solutions, Coralogix's platform will allow agencies to do more with less, delivering efficiency, security, and measurable savings for government sector customers.

Coralogix recently launched Olly, the



Ariel Assaraf, CEO and co-founder of Coralogix.

first autonomous observability agent that identifies and resolves production issues in real time. Olly analyses telemetry data and provides clear, evidence-backed answers without prompts. Unlike AI assistants that only respond to commands, Olly acts as a proactive intelligence layer, anticipating problems, adapting to context, and evolving with users. It works like an engineering teammate, deciding what to analyse, running queries, explaining its decisions, and suggesting next steps.

"We are grateful to the U.S. Department of Education-Federal Student Aid office for its trust and sponsorship of our platform," said Ariel Assaraf, CEO and co-founder of Coralogix. "Coralogix is committed

to bringing U.S. federal agencies a streamlined, secure solution that simplifies operations and accelerates decision-making, so they can focus on delivering results rather than managing complexity."

FedRAMP is a federal program providing a standardised, reusable approach to security assessment and authorisation for cloud service offerings. Its certification process involves a thorough review of a solution's data protection, governance, and cloud security practices. In collaboration with the FCC and coordination with the FedRAMP Program Management Office, Coralogix has finished all preliminary requirements and is on track to achieve FedRAMP certification within the next year.

CISCO UNVEILS KEY STRATEGIES FOR SECURING AI APPLICATIONS AMIDST RAPID ADOPTION IN MIDDLE EAST

Cisco highlights four priority focus areas

organisations should consider to secure AI applications as they scale adoption. The guidance outlines how security teams can adapt proven application security practices to AI, helping organisations across the Middle East manage emerging risks and maintain digital trust.

As AI adoption scales across the Middle East, including government, financial services, energy, and critical infrastructure, CISOs and IT leaders are under pressure to secure AI applications across the full lifecycle, from the data they rely on to the models they deploy.

Four focus areas for AI applications security:

1) Open-source scanning

AI application development relies heavily on components such as open-source models, public datasets, and third-party libraries. These dependencies can include vulnerabilities or malicious insertions that compromise the entire system.

2) Vulnerability testing

Static testing for AI applications involves validating the components of an AI application, including binaries, datasets, and models, to identify vulnerabilities like backdoors or poisoned data. Dynamic testing evaluates how a model responds across various scenarios in production. Algorithmic red-teaming can simulate a diverse and extensive set of adversarial techniques without requiring manual testing.

3) Application firewalls

The emergence of generative AI applications has given rise to a new class of AI firewalls designed around the unique safety and security risks of LLMs. These solutions serve as model-agnostic guardrails, examining AI application traffic in transit to identify and prevent failures and enforce policies that mitigate



Fady Younes, Managing Director for Cybersecurity at Cisco Middle East, Africa, Türkiye, Romania and CIS,

threats such as PII leakage, prompt injection, and denial of service (DoS) attacks.

4) Data loss prevention

The rapid proliferation of AI and the dynamic nature of natural language content makes traditional DLP ineffective. Instead, DLP for AI applications examines inputs and outputs to combat sensitive data leakage. Input DLP can restrict file uploads, block copy-paste functionalities, or restrict access to unapproved AI tools. Output DLP uses guardrail filters to help ensure model responses do not contain personally identifiable information (PII), intellectual property, or other sensitive data.

Fady Younes, Managing Director for Cybersecurity at Cisco Middle East, Africa, Türkiye, Romania and CIS, said: "As AI adoption accelerates across the region organisations are moving quickly from pilots to production, and that shift

changes the risk profile. Securing AI applications requires looking beyond traditional application controls to protect the full AI lifecycle, from the data and third-party components feeding models to how those models behave in real world use. By applying familiar security principles in AI specific ways, organisations in the Middle East can scale innovation with confidence while reducing risks such as prompt injection and sensitive data leakage."

Protecting AI applications from development to production

Risk exists at virtually every point in the AI lifecycle, from sourcing supply chain components through development and deployment. The security measures highlighted above help mitigate different risk areas and each plays an important role in a comprehensive AI security strategy.

HEXNODE EXPANDS INTO UAE'S ENDPOINT SECURITY SPACE WITH HEXNODE XDR

Hexnode, the enterprise software

division of Mitsogo, released Hexnode XDR, its extended detection and response platform, marking a significant step in its effort to strengthen cyber resilience across organisations in the UAE.

As the UAE continues its rapid digital transformation, it has also become a prime target for sophisticated cyber threats. The nation regularly confronts a surge of malicious activity, with security authorities blocking more than 200,000 cyberattacks every day across critical infrastructure and business environments.

"As digital adoption accelerates across the UAE, security teams are under pressure to respond faster and with better context," said Tim Bell, VP of Sales, EMEA & APJ. "Hexnode XDR helps bring structure and context to endpoint security operations, allowing organisations to respond with greater clarity and confidence."

Security Simplified for IT Admins

Hexnode XDR reimagines the XDR experience with usability at its core. Its clean, structured dashboard unifies endpoints, alerts and vulnerabilities into a single view, simplifying how IT teams assess and respond to threats.

Key Features Include:

Unified Incident Visibility: Real-time overview of threats, alerts, and vulnerable devices, helping IT admins assess their security posture quickly.

Automated Correlation: Collect and analyse signals across endpoints to uncover malicious activity, supported by severity levels, device impact, and threat lifecycle logs.

Contextualised Alerts: Alerts enriched with device and policy insights for focused response decisions.

One-Click Remediation: Instant coordinated response to kill processes, quarantine or delete files, and isolate



devices for swift threat containment.

Complete Audit Trail: Searchable and exportable logs of threats, actions and system events, preserving full traceability for efficient analysis and compliance.

By emphasising clarity and automation, Hexnode XDR helps IT teams respond to threats faster and with greater certainty.

One Ecosystem

Hexnode XDR integrates seamlessly with Hexnode UEM, creating a single connected environment for endpoint management and security. This unified approach reduces tool sprawl and shortens response time.

Integration Highlights:

Effortless Setup: Extends protection from existing Unified Endpoint Management (UEM) environments with minimal configuration.

Centralised Control: Manage devices, monitor threats, and enforce policies from one intuitive interface.

Real-Time Feedback Loop: XDR insights flow directly into Hexnode UEM for consistent device and security visibility.

Familiar Workflows: Built on the same design principles as Hexnode UEM to ensure quick adoption.

Future-Ready Scalability: Scales with workforce growth, cloud adoption, and hybrid work models.

This synergy enables organisations to

manage, secure, and respond all within a single, cohesive platform.

Built for What's Next

Hexnode XDR is engineered to evolve into a fully advanced XDR platform that adapts to growing enterprise security demands.

Upcoming features include:

Broader Endpoint Coverage: Support for macOS, Linux and mobile devices alongside Windows.

Third-Party UEM Integration: Compatibility with external UEMs, allowing organisations to leverage Hexnode XDR without replacing existing tools.

Actionable Security Prompts: Suggests timely security actions, enables one-click setup through pre-filled UEM policies, and tracks impact to refine future recommendations.

Hexnode Genie AI support: An intelligence layer that powers guided troubleshooting and quick chat-based responses to admin queries.

Intelligent Threat Response: Automated threat remediation and technician assignment for faster containment.

Application Vulnerability Insights: Visibility into system and user-installed apps, with alerts to help IT teams identify risky software.

Hexnode XDR equips organisations of all sizes, offering simplified threat management for SMBs and full-scale orchestration through UEM integration for enterprises.

CYBERSECURITY AT CENTRE OF POWER IN 2026

THIS YEAR MARKS A TURNING POINT WHERE CYBERSECURITY, AI, AND GEOPOLITICS CONVERGE—AND RESILIENCE BECOMES A SHARED RESPONSIBILITY.

By Sandhya D’Mello

Entering 2026, organisations across the Middle East are confronting a hard reality: cybersecurity no longer exists at the margins of business or quietly within IT functions. It has moved to the centre of geopolitics, economic ambition, artificial intelligence, and national resilience. The events of 2025—from GPS disruption and large-scale telecom intrusions to the industrialisation of cybercrime—have stripped away any remaining abstraction, revealing that digital infrastructure is now inseparable from power, stability, and trust.

Ziad Nasr, General Manager at Acronis Middle East, observes, “The cyberwar that has simmered for a decade is gaining shape and definition.” What was once hidden beneath layers of attribution and denial is now increasingly acknowledged in public

disclosures and real-world impact. Cyber operations are no longer confined to digital boundaries; they bleed into physical logistics, communications, and economic confidence.

This convergence has fundamentally altered the threat landscape. Cybercrime now mirrors legitimate business models, with ransomware groups and access brokers operating like scaled enterprises. Attackers are abandoning traditional malware in favour of identity abuse, cloud-native access, compromised APIs, and trusted administrative tools. A stolen credential or session token today can deliver more operational reach than any exploit kit.

For defenders, this evolution exposes a hard reality: visibility gaps are widening just as attack surfaces fragment. Neoclouds, agentic AI, distributed workforces, and IT-OT convergence are expanding digital estates faster than security teams can map them. Tool sprawl and telemetry overload have left many CISOs drowning



in alerts while struggling to translate exposure into business risk.

2026 will mark a decisive shift toward risk-first cybersecurity, Hadi Jaafarawi, Regional VP for the Middle East and



Africa at Qualys, said, “Decision makers are entering an era of risk-first cybersecurity.” The rise of the Risk Operations Center (ROC) reflects a broader move away from asset

counting toward understanding how vulnerabilities intersect with revenue, regulation, and operational continuity. Boards are no longer asking how many threats were blocked—they are asking

which risks truly matter.

Artificial intelligence further complicates this equation. While the UAE continues to lead on AI adoption, responsibility for AI risk can no longer

be deferred or abstracted. Autonomous agents, shadow AI, and AI-driven automation introduce compounding exposure that cannot be offset simply by adding more tools. In 2026, security leaders will be judged not on how quickly AI is deployed, but on how rigorously it is governed and justified in business terms.

Meanwhile, long-standing security assumptions are collapsing. VPNs are losing relevance, network perimeters are dissolving, and the workforce is no longer bound by geography. Identity has become both the primary control plane and the primary attack vector.

Christopher Hills, Chief Security Strategist at BeyondTrust, notes, "So much of what we seek to defend is the digital record of who we are and what we do." Compromising identity is now the fastest route to privilege, persistence, and profit.

Against this backdrop, no organisation can defend in isolation. Community-scale intelligence sharing is emerging as a critical layer of defence, compressing detection and response timelines and allowing defenders to learn collectively from emerging tradecraft. When attackers collaborate and automate at scale, defence must evolve in kind.

The cyber reality of 2026 is not defined by any single threat or technology. It is defined by interdependence. Power, crime, and defence now operate across shared digital ecosystems. For Middle East organisations navigating this turbulent landscape, resilience will depend on embracing risk economics, identity-first security, disciplined AI governance, and a willingness to defend together—or face the future alone.

This growing interdependence is also reshaping how organisations adopt and operationalise artificial intelligence. As AI systems move deeper into core business processes, they are no longer isolated innovations but integral components of shared

SO MUCH OF WHAT WE SEEK TO DEFEND IS THE DIGITAL RECORD OF WHO WE ARE AND WHAT WE DO
CHRISTOPHER HILLS,
CHIEF SECURITY STRATEGIST AT BEYONDTRUST.

digital ecosystems spanning cloud, on-premise, and edge environments.

Reflecting this shift, Cloudera has identified 2026 as the start of the "Era of Convergence," a phase in which AI leaves experimentation behind and becomes embedded in production environments where governance, data access, and security must operate in unison.

Cloudera, the only company bringing



Christopher Hills.

AI to data anywhere, announced that the 'Era of Convergence' will be the next phase of AI in 2026. "In 2026, the adoption of Artificial Intelligence will continue to grow at a constant rate, despite market deceleration predictions," said Manasi Vartak, Chief AI Officer at Cloudera., "When companies overcome the experimentation phase and find the most suitable measurable return on investment for their projects, they will continue to demand both generative AI and agentic AI."

At this point, the most important challenge will be connecting AI agents with corporate data and context, an indispensable requirement for these systems to be truly useful. Many organisations have already demonstrated their agentic capabilities, but now they must prove these systems are ready for production and they can overcome barriers related to data access, governance, security, and permissions.

At the same time, the definition of



**THE CYBERWAR
THAT HAS SIMMERED
FOR A DECADE IS
GAINING SHAPE AND
DEFINITION**
***ZIAD NASR, GENERAL
MANAGER AT ACRONIS
MIDDLE EAST.***



Ziad Nasr.

'Responsible AI' will continue to evolve. As AI systems become increasingly complex, Responsible AI must address not only model bias and equality but also end-to-end accountability, encompassing data handling and system behaviour.

Companies adopting agentic AI will need to implement stricter governance frameworks with new features such as agent logs, observability, and version control for complete agentic workflows. Although public models will continue to dominate in 2026, we will see an increase in specific adaptation for each company.

Hadi Jaafarawi.



Era of convergence

2026 is expected to be the first year of real convergence: the start of a new stage where the boundaries between the cloud and data centers blur. After several decades in which control of on-premise was prioritised first and then the flexibility of the cloud, we now enter a reality where both coexist seamlessly, thanks to unified management platforms. Workloads will run where it makes the most sense, considering security, compliance, and efficiency, rather than prioritising location.

Sergio Gago, global CTO of Cloudera, said, “The true competitive advantage will not come from who has a bigger model, but from who makes the smartest and most efficient use of resources. In the Era of Convergence, AI must be managed as another part of the workforce. It is not necessary to

DECISION MAKERS ARE ENTERING AN ERA OF RISK-FIRST CYBERSECURITY
HADI JAAFARAWI, REGIONAL VP FOR THE MIDDLE EAST AND AFRICA AT QUALYS.

choose sides (cloud versus on-premise or human versus machine), but to unify them under the same shared, efficient, and trusted architecture.”

The concept of performance will also be redefined: as AI and computing capacity demands soar, companies

will position energy efficiency as a primary KPI and not as a secondary consideration.

The defining challenge of 2026 will not be the absence of technology or intelligence, but the ability to govern complexity at scale. As cyber threats grow more identity-driven, AI systems move into production, and digital infrastructure converges across cloud, data centre, and edge, security can no longer be managed in silos. The future belongs to organisations that understand risk in business terms, treat identity as the new perimeter, and embed governance into every layer of their AI and data strategies. In an era shaped by interdependence, resilience will hinge not on who moves fastest alone, but on who builds trust, visibility, and collective defence across an increasingly connected digital world. 🔒

 tahawultech.com

Women in TECHNOLOGY FORUM AND AWARDS

Give to gain. Powering women in tech



05th March 2026



Dubai



9:00 AM to 1:00 PM

#WomenInTech2026 | #IWD2026 | #tahawultech

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

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

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

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

OFFICIAL PUBLICATIONS

cnme
computer news middle east

Reseller MIDDLE EAST
THE VOICE OF THE CHANNEL

Security MIDDLE EAST
MIDDLE EAST

HOSTED BY

 tahawultech.com

For more information about the event and nomination details, please visit the event website below :-

<https://www.tahawultech.com/women-in-tech/2026/>

CYBERWISE'S VISION FOR MIDDLE EAST: STAYING AHEAD OF THREATS THROUGH CLARITY AND COMMITMENT

The pace of digital change across the Middle East has rarely been faster. From national digital agendas to enterprise cloud migrations, organisations are building at speed — often under intense pressure. As innovation accelerates, so does the complexity of securing it, placing trust, clarity and resilience at the centre of the cybersecurity conversation.

This is precisely where CYBERWISE positions itself. Security Advisor Middle East spoke to Kadir Yuceer, Regional Director EMEA, about the company's founding philosophy.

"From the very beginning, we built CYBERWISE on a simple belief," he says. "Cybersecurity must deliver real outcomes — not just activity or noise."

This mindset has shaped the company's journey from its early days across Türkiye and Europe, where it supported some of the world's most regulated and technically demanding environments. Exposure to sectors such as finance, payments and critical infrastructure helped define a delivery model built on precision and execution. "Those experiences taught us what really matters," Yuceer explains. "Long-term value, not short-term wins."

CYBERWISE's presence in the Middle East is not a recent development. The company has been active in the region for more than a decade, working alongside organisations during key moments in their digital transformation journeys. As modernisation accelerated across the

GCC, the need for cybersecurity partners with deep technical capability and regional understanding became increasingly evident. "We've grown with the region," Yuceer notes. "And that history shapes how we engage today."

Rather than pursuing growth for its own sake, CYBERWISE's current focus is on reinforcing that long-term commitment. With digital services expanding rapidly across government and enterprise, the challenge is no longer adoption — it is sustainability. "The region is moving fast," Yuceer says. "Our role is to help organisations build security that keeps up, scales responsibly and supports innovation, instead of slowing it down."

At the centre of this approach is a philosophy anchored in clarity, collaboration and accountability — supported by a strong security-by-design mindset. These principles are not framed as abstract ideals, but as practical responses to the realities organisations face today.

Clarity, in particular, has become a differentiator in an increasingly noisy security landscape. Many environments are crowded with tools generating endless alerts, but little insight. CYBERWISE's focus is on helping organisations see what truly matters. "We aim to deliver real visibility and real improvement," Yuceer says. "Not more complexity."

Collaboration follows naturally from this. Cybersecurity strategy only works when it translates into operational reality, and that requires alignment across the

organisation. By working closely with IT, risk, compliance, operations and executive leadership, CYBERWISE ensures security initiatives support both technical and business objectives. "When everyone is working from the same playbook," Yuceer explains, "security becomes far more effective."

Accountability underpins everything else. CYBERWISE stands behind its assessments, recommendations, and delivery, with clients engaging directly with experienced practitioners rather than layered account structures. "We don't compete on volume," Yuceer says. "We compete on quality, depth and the ability to turn cybersecurity into a business capability, not just a compliance requirement."

These principles define the practical value CYBERWISE delivers across the Middle East. The company's work consistently centres on three areas: building lasting maturity, applying threat-led expertise and maintaining a strong local presence.

Maturity building focuses on creating capabilities that endure.

Maturity building focuses on creating capabilities that endure. This includes compliance, audits, consultancies, trainings and gap assessments for PCI Programs such as PCI DSS, PCI 3DS, PCI PIN, PCI CPP, PCI ASV ISO Standards such as ISO27001, ISO22301, ISO27017, ISO27019, ISO27701, ISO9001, ISO20000-1, ISO15004 and SWIFT CSP Framework, security frameworks such as CIS, NIST,

Kadir Yuceer
Regional Director EMEA, Cyberwise.



Cobit, NIS, red teaming, detection engineering and incident preparedness. The emphasis is always on resilience by design — avoiding fragmented fixes that solve isolated problems.

Threat-led expertise complements this foundation. Drawing on real-world incidents across financial services, critical infrastructure, telecoms, and digital-first enterprises, CYBERWISE translates global threat intelligence into practical, locally relevant action. “Our experience allows us to make threats tangible,” Yuceer explains. “And that makes them manageable.”

Local presence ensures these capabilities are delivered in a way that reflects regional realities. With teams based in the UAE and across EMEA, CYBERWISE works closely with clients, regulators and partners. “Resilience grows faster when support is close,” Yuceer says, highlighting the importance of proximity in fast-moving markets.

In a region crowded with cybersecurity providers, differentiation comes down to more than messaging. Many organisations already have advanced technology stacks in place. The real challenge lies in understanding risk, prioritising controls, and operating security consistently at scale. “What’s missing is often clarity,” Yuceer notes.

CYBERWISE addresses this by focusing relentlessly on execution and outcomes, rather than short-term transactions. Commitments are kept realistic, delivery is measured, and relationships are built over time. “Trust doesn’t come from promises,” Yuceer says. “It comes from consistency.”

As that trust develops, the relationship evolves. CYBERWISE moves beyond the role of vendor and becomes a trusted advisor, often operating as an extension of internal teams. “We show up, we deliver and we stay accountable,” Yuceer explains. “That’s what changes the dynamic.”

This approach is especially relevant in nationally significant sectors like financial, telecommunication, energy, e-commerce, fintech sectors facing advanced cyber threats. In this context, our wiser solutions



such as vciso, managed security services, continuous vulnerability management services provide sustainable security journey to the customers.

Critical infrastructure represents another major area of engagement, particularly where IT and OT environments intersect. In these settings, traditional security models fall short. CYBERWISE brings extensive OT cybersecurity expertise built through years of work with large industrial organisations operating across multiple continents.

By applying threat modelling, segmentation, continuous validation and security-by-design principles, CYBERWISE helps organisations strengthen OT security across complex, globally distributed environments. These capabilities are increasingly vital for sectors such as energy, oil and gas, utilities, transportation and manufacturing.

Government organisations also play a central role in national digital resilience. CYBERWISE supports public sector entities through advisory programmes, readiness exercises, managed services, and capability-building initiatives across identity, cloud and threat detection — strengthening the broader digital

ecosystem in the process.

Partnerships reinforce this work. CYBERWISE collaborates with global technology leaders including Thales, Microsoft, and IBM, alongside a regional network of more than 30 partners across 12 MENA countries. These relationships enable co-delivery, deeper local engagement and alignment with regulatory and sector-specific priorities.

Looking ahead, Yuceer sees CYBERWISE contributing to the region’s digital resilience over the long term. The focus will be on helping organisations shift from tool-centric to capability-centric security, strengthening cross-industry collaboration through realistic simulations and building local talent.

This long-term commitment will be reinforced by the planned opening of CYBERWISE’s local company in Saudi Arabia in early 2026, underscoring the company’s dedication to the Kingdom and the wider region.

Ultimately, Yuceer frames CYBERWISE’s role in simple terms. “We stand alongside organisations as a trusted partner,” he says. “Providing clarity, technical depth and consistent support — so they can stay ahead of threats instead of constantly reacting to them.” 🔒

KSA FUTURE ENTERPRISE AWARDS 2026



12th April
2026



Radisson Blu Hotel & Convention Center
Riyadh Minhal



06:30 PM onwards

#KSAFEA2026 | #tahawultech

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

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

GOLD SPONSORS



OFFICIAL PUBLICATIONS



HOSTED BY



SECLORE STRENGTHENS COMMITMENT TO SAUDI ARABIA'S DIGITAL TRANSFORMATION AGENDA

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

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

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

priorities. Endres also highlighted the strategic importance of Black Hat MEA as a platform for customer engagement, collaboration, and innovation.

Interview Excerpts:

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

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

that protects this next generation of digital ecosystems — wherever the data travels.

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

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

The new framework addresses three core challenges:

Visibility Gaps

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

Misuse and Insider Risk

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

AI + Data Governance

As organisations adopt AI, data becomes both fuel and risk.

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

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

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

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

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

Our platform directly supports national objectives by enabling:

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

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

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

Black Hat MEA has become one of the most influential cybersecurity events globally.

For us, the value is clear:

- Direct customer engagement with enterprises and government entities
- Insight into emerging regional



Justin Endres
Chief Revenue Officer
Seclore

challenges

Collaboration opportunities with partners and innovators

A platform to showcase our newest capabilities

A space to learn — not just exhibit

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

NEW RESEARCH REVEALS MIDDLE EAST DATA SOVEREIGNTY PROGRESS MASKS CRITICAL AI GOVERNANCE GAPS

56% OF UAE ORGANISATIONS SEE AI VENDOR RISK – BUT ONLY 19% HAVE JOINT INCIDENT PLAYBOOKS. SAUDI TRAILS GLOBAL BENCHMARKS ON EVERY SUPPLY CHAIN METRIC. CONTROLLING WHERE DATA LIVES ISN'T THE SAME AS CONTROLLING HOW IT'S USED.

Kiteworks, which empowers organisations to effectively manage risk in every send, share, receive, and use of private data, released its Data Security and Compliance Risk: 2026 Forecast Report. A comprehensive analysis revealing that Middle East organisations have made significant strides in data sovereignty infrastructure, but lag on the governance controls needed to manage AI-era risks.

The research, based on a survey of security, IT, compliance, and risk leaders across 10 industries and 8 regions, exposes a fundamental gap between sovereignty capability and governance execution in the Middle East. Whilst UAE leads on data localisation and cross-border mechanisms (55% to 62% adoption), critical governance controls remain underdeveloped: UAE shows 54% AI anomaly detection versus Saudi at just 32%, a 22-point regional gap. Only

19% of UAE organisations and 12% of Saudi organisations have joint incident playbooks with AI vendors.

“The Middle East has moved faster than any other region on data sovereignty infrastructure. Localised data centres, cross-border controls, regulatory frameworks. That’s real progress,” says Dario Perfettibile, GM of EMEA GTM & Customer Operations, Kiteworks. “But governance controls how data is used, who accesses it, and what happens when things go wrong. The gap between sovereignty investment and governance maturity is where risk accumulates. And that gap is widest around AI vendor relationships and incident response capabilities.”

The report identifies five predictions for Middle East organisations in 2026:

- AI-specific incident response will remain uneven across the region. UAE leads at 54% AI anomaly detection, but Saudi trails at 32%. A 22-point gap that



creates a fragmented regional security posture. Organisations operating across both markets face inconsistent protection.

- Third-party AI vendor risk will be recognised but under-controlled. 56% of UAE organisations cite AI vendor risk as a top concern, yet only 19% have joint incident playbooks. Saudi shows the same pattern: 48% concern, 12% playbooks. Awareness without action is exposure.
- Software supply chain controls will remain sector and country skewed. Saudi trails global averages on every supply chain metric: SBOM adoption at 22% versus 28% global, secure SDLC at 34% versus 41% global. UAE performs better but still shows gaps – 62% lack SBOM coverage.
- Compliance automation will remain incomplete. 48% of UAE organisations lack full compliance automation; 62% of

Saudi organisations still rely on partial or manual processes. As regulatory scrutiny intensifies, manual compliance won't generate the continuous evidence auditors expect.

- Key AI risks will be underweighted relative to global peers. Saudi organisations cite training-data poisoning as a top concern at just 22% versus 29% globally, and PII leakage at 24% versus 32% globally. Lower concern doesn't mean lower risk, it means lower preparedness.

The gap between UAE and Saudi Arabia on multiple metrics – anomaly detection, SBOM adoption, compliance automation – suggests that regional progress is uneven. Organisations with cross-border operations face the challenge of managing different maturity levels across markets, creating governance complexity that sovereignty infrastructure alone cannot address.

The global report, which includes

15 predictions across data visibility, AI governance, third-party risk, and compliance automation, identifies “keystone capabilities” – unified audit trails and training-data recovery – that predict success across all other metrics, showing up to 32-point advantages for organisations that have implemented them. The Middle East's strong performance on cross-border mechanisms (55-62%) demonstrates capability that can be extended to other governance domains.

“Sovereignty is table stakes for the Middle East—and organisations have invested accordingly. The next phase is governance maturity,” adds Perfettibile. “Controlling where data lives is necessary but not sufficient. Controlling how AI vendors use that data, how incidents are detected and responded to, and how compliance is demonstrated continuously. That's where the Middle East's next infrastructure investment needs to focus.” 🔑



MUDDYWATER SHIFTS TO RUST-BASED MALWARE IN TARGETED MIDDLE EAST CYBER-ESPIONAGE CAMPAIGN

NEW CLOUDSEK RESEARCH REVEALS HOW THE APT GROUP HAS EVOLVED ITS TOOLING WITH A STEALTHY RUST IMPLANT TO STRENGTHEN PERSISTENCE, EVASION, AND INTELLIGENCE COLLECTION ACROSS CRITICAL SECTORS.

CloudSEK has uncovered a sophisticated spearphishing campaign attributed to the MuddyWater advanced persistent threat (APT) group, signalling a notable evolution in the actor's malware development strategy. The campaign, which targets diplomatic, maritime, financial, and telecommunications organisations across the Middle East, introduces a previously

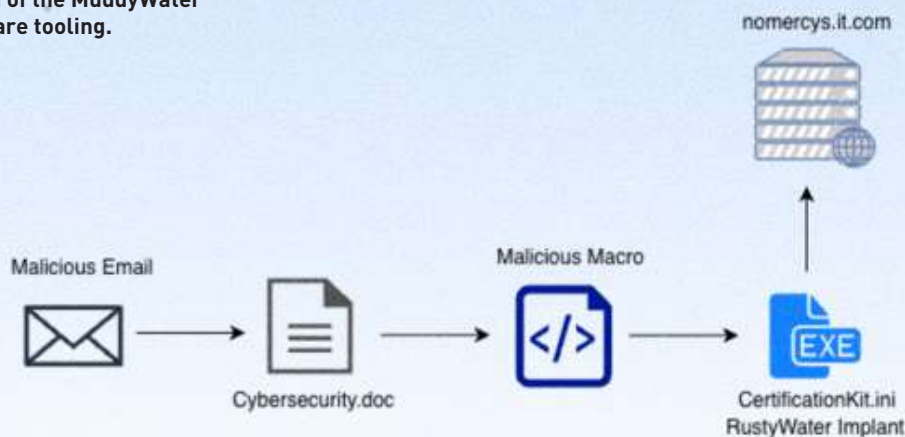
underreported Rust-based remote access implant dubbed RustyWater.

According to CloudSEK's threat intelligence team TRIAD, the campaign begins with carefully crafted phishing emails impersonating legitimate government and enterprise entities in the region. Victims are lured into opening malicious Microsoft Word documents that rely on embedded VBA macros to drop and execute the next-stage payload.

While MuddyWater has historically favoured PowerShell and Visual Basic-based tooling, the use of Rust marks a shift towards more structured, modular, and stealth-oriented malware.

Once executed, the RustyWater implant establishes persistence through Windows registry modifications and deploys multiple anti-analysis and anti-debugging mechanisms to evade detection. The malware encrypts all embedded strings,

CloudSEK research highlights the technical evolution of the MuddyWater APT group's malware tooling.



Reborn in Rust: MuddyWater Evolves Tooling with RustyWater Implant

CloudSEK TRIAD



actively scans for more than two dozen antivirus and endpoint detection products, and leverages asynchronous execution to complicate forensic analysis. Its command-and-control communications are handled via HTTP using the Rust request library, with layered encryption and randomised beaconing intervals designed to frustrate network-based detection.

CloudSEK's analysis shows that RustyWater supports modular post-compromise capability expansion, allowing attackers to selectively enable surveillance, data collection, or credential theft without deploying additional binaries. This approach

significantly reduces the operational footprint on compromised systems while increasing the longevity and flexibility of access.

The campaign has also demonstrated extensive regional targeting. Researchers identified multiple decoy documents impersonating UAE government entities, including the Ministry of Foreign Affairs, as well as lures aimed at the Middle East's maritime and education sectors. Further investigation revealed that some phishing emails were sent using compromised legitimate accounts, increasing their credibility and success rate.

From a defensive perspective, CloudSEK warns that traditional

static indicators such as IP blocking or signature-based detection may be insufficient against this threat. The report highlights the heightened risk of long-term silent persistence, reduced visibility for incident response teams, and the growing intelligence exposure for organisations operating in geopolitically sensitive sectors.

CloudSEK recommends that organisations strengthen monitoring of registry-based persistence mechanisms, focus detection efforts on behavioural indicators rather than single indicators of compromise, and closely scrutinise memory allocation and process injection activity within legitimate Windows processes.

The emergence of RustyWater underscores a broader trend among advanced threat actors towards modern programming languages and low-noise malware architectures, reinforcing the need for continuous threat intelligence, behavioural monitoring, and proactive defence strategies across the Middle East's critical infrastructure landscape. **1**

THE MOVE TO RUST-BASED IMPLANTS MARKS A SIGNIFICANT EVOLUTION IN MUDDYWATER'S OPERATIONAL MATURITY, ENABLING LOW-NOISE PERSISTENCE AND MODULAR POST-COMPROMISE CAPABILITIES.

Matthew Prince
co-founder and CEO, Cloudflare



**OUR MISSION—TO
HELP BUILD A BETTER
INTERNET—IS THE
DRIVING FORCE
BEHIND EVERYTHING
WE DO**

CLOUDFLARE DETAILS GLOBAL CYBER DEFENCE, AI PROTECTION EFFORTS IN IMPACT REPORT

REPORT DETAILS KEY MILESTONES IN HELPING SECURE DEMOCRATIC ELECTIONS WORLDWIDE, PROTECT INDEPENDENT JOURNALISM AND NON PROFITS FROM AI SCRAPING, AND CREATE A MORE SUSTAINABLE INTERNET

Cloudflare, Inc. (NYSE: NET), the leading connectivity cloud company, today published its fifth annual Impact Report showcasing its commitment to building a faster, more secure, and more sustainable Internet for everyone. Highlights include defending democratic institutions from cyberthreats, empowering journalists and non-profits to control how AI uses their original content, and promoting digital inclusion and economic development through better access to AI.

“Our mission—to help build a better Internet—is the driving force behind everything we do,” said Matthew Prince, co-founder and CEO, Cloudflare. “In 2025, we took critical steps to further that mission by making our products free and accessible to those who need them most, from journalists facing attacks to startups and developers around the world working on the next generation of AI-native applications. A principled, accessible, and sustainable Internet is not just a goal; it’s our responsibility.”

Key milestones highlighted in

Cloudflare’s 2025 Impact Report include:


- Protected 3,000+ vulnerable Internet properties from an average of 9.9 billion cyber attacks per month through Project Galileo: Journalists, human rights defenders, and humanitarian organisations are

often targets of sophisticated cyber attacks designed to silence them. Cloudflare’s Project Galileo shields these public interest groups across 120+ countries, blocking a record volume of attacks against independent news organisations in 2025—an average of 290 million attacks per day.

- Helped nonprofits and independent media better protect their websites from unwanted AI crawlers—for free: To help local news outlets survive and thrive in a challenging digital landscape, Cloudflare has incorporated Bot Management and AI Crawl Control in its package of free services for entities in Project Galileo and has committed to train news outlets on new AI tools. These tools will help independent news websites compete in an AI-powered world and empower them to better control how AI services access and use their content.
- Secured elections across 33 U.S. states and 7 countries against major cyber threats: Democratic elections are critical infrastructure, and the Athenian Project provides our highest level of security to defend the websites and systems of those running elections. The project now protects 441 state and local government Internet properties, and during the critical period between

September and November 2024 successfully blocked 200 million DDoS attacks directed at those sites. Cloudflare also helped secure the Moldovan Parliamentary elections despite a significant foreign influence campaign and persistent cyberattacks against Moldovan government institutions

- Achieved key emissions commitments, offsetting 31,000 metric tons of CO2e: Cloudflare successfully completed its commitment to offset or remove all emissions associated with powering its network from its launch up until its first renewable energy purchase in 2018. This was accomplished by investing in verified projects totaling approximately 31,000 metric tons of CO2e.
- Committed to training the next generation of technology leaders with a major focus on AI application: Recognising the need for a diverse and skilled future workforce, Cloudflare plans to hire 1,111 interns over the course of 2026. This initiative will place a special emphasis on encouraging the creative and widespread application of Artificial Intelligence across various disciplines.

Overall, Cloudflare has provided more than \$19 million in donated products and services in 2025 through these Impact programs. 

IBM UNVEILS TECHNOLOGIES DEFINING THE GLOBAL AND UAE BUSINESS LANDSCAPE IN 2026

KLEIN BRINGS 25+ YEARS OF CYBERSECURITY AND CUSTOMER JOURNEY EXCELLENCE TO TRANSFORM FORCEPOINT CUSTOMER SUCCESS INTO GLOBAL GROWTH ENGINE FOR COMPANY'S DATA SECURITY CLOUD PLATFORM

The IBM Institute for Business Value (IBV) has unveiled Five Trends for 2026, a new report identifying the forces that will redefine competitive advantage for organisations in the UAE and around the world in the year ahead. As 2026 begins, the research shows that uncertainty isn't slowing business down – it's accelerating transformation.

To thrive, companies are doubling down on technologies that provide speed, resilience, and insight. AI has shifted from experimental to essential, redefining decisions, roles, and customer expectations at an unprecedented pace. Enterprises are moving towards operating with AI at the core, and soon, quantum will help tackle their most complex problems.

"The findings point to a fundamental shift in how organisations are

approaching growth and competitiveness in 2026," said Shukri Eid, General Manager, IBM Gulf Levant and Pakistan. "In the UAE, leaders are accelerating decision-making, embedding AI at the core of their operations, and strengthening resilience and sovereignty across their technology environments. At the same time, there is a clear focus on building trust - with employees, customers, and partners - as AI becomes more deeply integrated into everyday business. Together, these priorities are shaping organisations that are better prepared to adapt, collaborate across ecosystems, and take advantage of emerging technologies such as quantum."

Fast decisions turn disruption into opportunity

Of the executives surveyed in the UAE,

95% say they increasingly need to make fast decisions, and all believe the highest-stakes decisions they made in 2025 were the right ones – that's 4% above the global average. Uncertainty can become the greatest business asset for those who embrace it, with 63% of the respondents saying economic and geopolitical volatility will create new business opportunities for their organisations in 2026. The report notes that 93% of UAE executives fear they'll lose their edge if they can't operate in real time.

Employees are ready to embrace AI-driven role changes

The research shows that employees no longer fear AI – they want to embrace it, even if that means their roles will change significantly. Globally, 81% are confident they can keep up with new technologies, and 61% think AI makes their job less mundane and more strategic. Across all generational groups – from digital natives to seasoned veterans – at least twice as many employees would welcome rather than resist greater use of AI by their employers in 2026. In addition, 63% would work with an AI agent.

Consumers are excited about AI, but transparency is mandatory

While consumers don't need AI to be flawless, they do need to be in the loop. Easy-to-understand explanations of how

- Fast decision-making will turn disruption into opportunity, with 63% of UAE executives saying economic and geopolitical volatility will create new business prospects for their organisations.
- At least twice as many employees worldwide would embrace rather than resist greater use of AI by their employers in 2026.
- Customers across the globe will hold AI accountable, with four in five inclined to trust a brand less if it intentionally concealed AI use.
- Global AI resilience will require a local safety net, with 98% of UAE executives believing in the importance of factoring in AI sovereignty into their 2026 business strategy.
- Quantum is the next frontier, with quantum-ready organisations worldwide three times more likely to belong to multiple ecosystems than their least ready counterparts.



Shukri Eid
General Manager, IBM Gulf
Levant and Pakistan.

AI is using their data are what make consumers most comfortable engaging with it. Among the consumers surveyed worldwide, 89% want to know when they're interacting with AI, and four in five say they would trust a brand less if it intentionally concealed AI use. Two-thirds would switch brands – and half would even pay more – to avoid hidden AI. Meanwhile, 95% of global executives believe consumer trust in their AI will define the success of new products and services.

AI resilience and sovereignty become essential

In the face of growing uncertainty, AI resilience and sovereignty – an organisation's ability to control and govern its AI systems, data, and infrastructure at all times – have become mission-critical. In the UAE, 98% of executives say AI resilience and sovereignty must be part of their 2026 strategy, and 63% worry about overdependence on compute resources.

Quantum will require deep ecosystem collaboration

Quantum demands resources no single entity can realistically maintain alone – in short, it takes an ecosystem, or several. Quantum-ready organisations (QROs) worldwide are three times more likely to participate in multiple ecosystems than their least ready counterparts. In the UAE, four in five executives (80%) say ecosystem partners help accelerate technology adoption, while 88% believe these partners enable their company to limit the impact of disruption, and an equal number agree that partner data improves business outcomes. The findings indicate that enterprises forging the best ecosystem alliances today are positioning themselves to lead in the quantum era. 📌

**IN THE UAE, LEADERS ARE ACCELERATING
DECISION-MAKING, EMBEDDING AI AT THE CORE
OF THEIR OPERATIONS, AND STRENGTHENING
RESILIENCE AND SOVEREIGNTY ACROSS THEIR
TECHNOLOGY ENVIRONMENTS.**

GCC TECHNOLOGY ADVANCEMENTS ARE BEING DRIVEN FROM MOMENTUM TO MATURITY

2025 marked a turning point for digital transformation across the GCC. What began as ambitious experimentation matured into execution at scale. AI became more evident in production, national digital platforms expanded, sustainability targets became operational mandates, and cybersecurity rose to the level of national resilience.

Most importantly, technology adoption became planned and aligned well with national visions, regulatory clarity, and long-term economic diversification strategies. This momentum sets the foundation for 2026, when we will see not just isolated innovation, but by well entrenched integrated, intelligent, and robust digital ecosystems.

Some of the accelerating of technology advancements in the region can be attributed to:

1. National vision led demand for intelligent platforms, for example the Saudi Vision 2030, the UAE Digital Government Strategy, Qatar National Vision 2030, Oman Vision 2040, and Kuwait Vision 2035 are driving demand for platform-based transformation. Governments are prioritising AI-enabled public services, smart cities, digital infrastructure, and automation at



Walid Gomaa
CEO – Omnix International.

national levels and creating strong pull for advanced AI, Digital Twins, robotics, and sovereign cloud capabilities.

2. Regulation and governance enabling confident AI adoption with AI governance in the GCC evolving rapidly from strong ethics to enforceable frameworks. Uniform AI risk classifications, sector specific rules, and mandatory audits are giving organisations the confidence to deploy AI responsibly at scale. This regulatory maturity is now more of

a catalyst and not a constraint for innovation.

3. Sustainability and energy transition are key technology accelerators. Net Zero commitments, circular carbon strategies, and energy diversification agendas are reshaping technology investment. Sustainability is no longer treated as a reporting obligation, but it is driving adoption of Digital Twins, AI-powered optimisation, green cloud infrastructure, and carbon-intelligence platforms across industries. 📌

AI WILL EVOLVE FROM ASSISTING TASKS TO INDEPENDENTLY MANAGING MULTI-STEP PROCESSES.

CIO

LEADERSHIP AWARDS 2026



05th February 2026



Dubai



6:30 PM onwards

#CIOLeadershipAwards2026 | #tahawultech

The CIO Leadership Awards is an annual event hosted by CPI that brings key stakeholders from the entire IT ecosystem together.

Our CIO Leadership Awards is designed to get all the prominent CIOs from the Middle East region into the one room to discuss how they have overcome certain challenges, their plans to capitalize on future opportunities and of course to celebrate the incredible success they have engineered for their respective companies.

The CIO Leadership Awards at its core, and since its inception, has always been a knowledge-driven event, and that is evidenced by the high-quality panel discussions, keynote presentations and fireside chats that we have every single year. It is an event that recognizes excellence and engages in robust conversations around the technologies that are reshaping IT.

OFFICIAL PUBLICATIONS

cnme
computer news middle east

Reseller MIDDLE EAST
THE VOICE OF THE CHANNEL

Security ADVISOR
MIDDLE EAST

HOSTED BY

 **tahawultech.com**

For more information about the event and nomination details, please visit the event website below :-

<https://www.tahawultech.com/cio/2026/>

COMPUTE SOVEREIGNTY SET TO DEFINE GULF'S AI LEADERSHIP

I FROM HEALTHCARE TO NATIONAL INFRASTRUCTURE, THE GULF'S AI AMBITIONS HINGE ON SECURING HUNDREDS OF THOUSANDS OF GPUS—AND BUILDING RESILIENT, SOVEREIGN COMPUTE ECOSYSTEMS.

The Gulf's AI journey is entering a transformative phase. AI is shifting from experimentation to scale, agentic systems are proliferating, and Gulf nations are building AI ecosystems featuring homegrown champions and local models, such as KSA's Allam, UAE's Falcon, and Qatar's Fanar. This phase of AI development requires a critical enabler: sovereign compute processing power at scale. Now, Gulf nations must assess their future compute needs and act decisively to secure compute capacity.



Fawaz Bou Alwan

In the Gulf, AI is already reshaping sectors. In healthcare for instance, AI agents are reviewing patient test results, suggesting diagnoses, generating treatment plans, and managing patient journeys based on individual needs – updating records, scheduling follow-ups, and coordinating medication orders.

Sustaining these AI models requires vast processing power. The greatest demand for compute power will come from running models for real-time, low-latency inference. Compute will also be needed to build and train local models, and to fine-tune global models for regional and sector-specific applications.

To forecast how much compute power Gulf nations will require in the near term, we analysed the volume of data that AI models will process – measured in model tokens, or small fragments of text, images, or other inputs – across training, fine-tuning and inference. We then translated this demand into the processing required (FLOPS, or floating-point operations per second) and the hardware needed to deliver it through GPUs. Our analysis reveals that the region will need 400,000–500,000 GPUs by 2028. This level of demand is significant: for context, xAI's supercomputer



Ali Ghaddar

COMPUTE DEMAND REMAINS UNCERTAIN AND VOLATILE, AND RAPID CHANGES IN AI ADOPTION COULD CREATE OVERCAPACITY OR SHORTAGES.

Colossus currently uses 200,000 GPUs with a trajectory towards 1,000,000.

Beyond the near term, the next wave of AI – real-world models that integrate digital intelligence with physical data and enable robots to operate in dynamic environments – is likely accelerate compute demand even further.

Data sovereignty mandates require that much of the Gulf’s compute demand – particularly across government, regulated industries, and critical infrastructure – be met locally. Accordingly, Gulf countries are making bold moves to secure compute sovereignty. Initiatives such as KSA’s HUMAIN AI data center and UAE’s Stargate project aim to build hyperscale capacity on domestic soil. With these efforts, the region is on track not only to meet local GPU demand, but also export compute power.

Risks to meeting demand remain, however. GPUs needed for the Gulf’s infrastructure initiatives will be shipped gradually over years, and access can be interrupted by export controls and geopolitical shifts. Technology cycles move fast, and each refresh renews dependence on external supply chains. Compute demand remains uncertain and volatile, and rapid changes in AI adoption could create overcapacity or shortages. Rising energy demand from AI workloads could strain energy systems without coordinated planning. Critical government and security workloads can be crowded out by commercial and export demand without careful governance.

Gulf governments can mitigate these risks and address the compute sovereignty imperative through the following multi-layered strategies.

First, governments can secure supply chains by working with the private sector to maintain GPU reserves, diversify global vendors, and deepen partnerships with chipmakers through long term

contracts and strategic investments. The UK government is partnering with multiple U.S. tech firms to expand supercomputing capacity. In the Gulf, HUMAIN and G42 – in collaboration with their governments – continue to develop partnerships with chipmakers such as NVIDIA, AMD, and Cerebras to enhance access resilience.

Second, governments can strengthen local compute ecosystem capabilities – from semiconductor design and manufacturing to data-center setup and operations – through investment programs, targeted incentives, and regulatory support. Examples in the semiconductor space include the U.S. CHIPS and Science Act to boost domestic chip production, and KSA’s Alat and National Semiconductor Hub initiatives to build semiconductor design and manufacturing capabilities.

Third, governments can improve infrastructure efficiency and access resilience through regional cooperation. A Gulf-wide compute infrastructure initiative, such as the European High-Performance Computing Joint Undertaking, could optimise investments, improve utilisation, and enhance the Gulf’s



Hani Zein




Mahsa Etefagh

collective bargaining power in global supply chains.

Fourth, governments can safeguard critical workloads during compute demand peaks through rigorous capacity allocation governance. High-performance computing initiatives in Japan and Europe illustrate how access tiers and allocation rules preserve capacity for essential and emergency applications.

Fifth, governments can institutionalise continued compute capacity forecasting that is informed by compute usage observatories and integrated with energy planning. This would enable more effective capacity management and alignment between compute infrastructure, energy systems, and national priorities.

Gulf countries have a successful history of anticipating bottlenecks in essential arenas such as food and water security. Now, they must address the compute imperative to seize control of their AI journeys and evolve into global AI leaders.

This opinion piece is authored by Hani Zein and Fawaz Bou Alwan, Partners, Ali Ghaddar, Principal, and Mahsa Etefagh, Manager, at Strategy& Middle East, part of the PwC Network 

WHY DATA PORTABILITY IS FOUNDATION OF SOVEREIGN CLOUDS

The rise of sovereign clouds has become inevitable as regulatory demands, and geopolitical pressures push enterprises to rethink where their data resides. Localised cloud environments are increasingly becoming essential, allowing organisations to keep their data within specific jurisdictions to meet compliance requirements, and provide risk mitigation. But sovereign clouds can't succeed without data portability, which is the ability to move data seamlessly between systems and locations. Today organisations shouldn't wait to be pushed by regulations, they need to be ahead of the game.

Enterprises need to address the reality that moving data across hybrid environments is far from straightforward. It's not just about relocating primary data, you also must keep it protected while considering associated datasets like backups and the information used in AI applications. While some may need to address the protection of Large Language Model (LLM) training data, many organisations are instead turning to Retrieval-Augmented Generation (RAG) or AI agents to bring intelligence to their proprietary data without building models from scratch. Either way, data sovereignty is a valid approach to the pressures facing organisations today, but the focus should always be on data resilience first, no matter where it's stored.

It's a familiar tale - the cloud will give businesses more options and flexibility, but to take advantage of these properly, they'll need some joined up thinking.

Today's forecast

Regulators around the globe are driving organisations to look at their data differently, appearing at pace in response to increasing data globalisation as countries try to get a better grasp on their data. The European Union (EU) has been particularly stringent, introducing the comprehensive General Data Protection Regulation (GDPR) that stipulates data sovereignty. Under it, the laws of the country where data is stored or processed are now applicable to the data, regardless of where the data was originally collected. Special attention is also being paid to the chain of custody of data in the EU with both the NIS2 and DORA regulations demanding robust risk management for data, especially when held or handled by third parties.

As data, including highly sensitive and classified data, is being increasingly handled by these third parties, namely cloud providers, keeping it bound under privacy laws has become a priority for both organisations and governments as their data moves across borders.

With this increased movement of data between countries, or even continents, global instability concerns have become unavoidable, especially for governments. Some have already adopted sovereign clouds to protect their most sensitive data from potential malevolent access. And some have taken it one step further. With cloud services completely reliant on data centre infrastructure, some governments have started to divest their interest in foreign cloud and data infrastructure, reinvesting instead in their

own. This way, they can avoid storing their most sensitive data with foreign providers.

But cloud sovereignty is not a silver bullet. For those utilising multinational cloud providers, there might be the option to stipulate where your data is ultimately stored and what countries' laws it will be held under, but there is no guarantee that it will not change. The issue isn't just solved by relocating the primary data. Sure, it needs to be protected, but what about all the related data? Backups and Large Language Model training data sets for example, all need to be carefully considered to meet data sovereignty – or alternatively, organisations can utilise RAG or AI agents to level up their data without having to deal with reams of AI training datasets in the first place.

Freedom of Movement

But to do all of this, organisations need to ensure that data portability is enshrined in their data resilience planning. After all, there's a fine line between protecting your data and inadvertently restricting it beyond the point of use. If organisations are unable to ensure data portability, then moving to a hybrid cloud environment to take advantage of both sovereign clouds and localisation of data storage is a non-starter.

There are SaaS (Software-as-a-Service) and DRaaS (Disaster Recovery-as-a-Service) providers that can simplify the process, but it's not a task that can be completely offloaded to a third party. Organisations still need to take a hands-on approach, planning and

managing it thoroughly to ensure data remains secure throughout the process. Otherwise, organisations will be unable to utilise sovereign clouds to adhere to the myriad data residency and sovereignty regulations.

It's not without caveats though. For those larger, multinational organisations operating across countries and continents, multiple cloud environments will be required to house multiple sovereign clouds. But this also brings increased complexity for both the monitoring and management of data across jurisdictions. Not only will multiple cloud environments need to be considered, but also multiple sets of data regulations across countries. And, for those organisations that do get it right, the benefit of enhanced data resilience comes with the added risk of data fragmentation.

There's no easy win, but what's certain is that data portability will be an essential part of any solution that organisations settle on. Whichever approach is taken, being able to move data seamlessly across platforms and clouds will be a necessity as organisations wrestle with data sovereignty. And, as regulations continue coming down the line, data portability will give organisations a head start on future compliance, allowing them to flex more easily to meet regulations, where less portable counterparts will struggle.

Tying down the cloud

Data globalisation is showing no signs of slowing, with information flows now their own form of trade, even generating their own economic value. And with global instability as an ever-present factor, data sovereignty will only move higher up the priority list. But it's not a task that



Michael Cade
Global Field CTO, Veeam.

can just be passed onto a third-party provider.

Although organisations may not fully realise it yet, data sovereignty and operational clarity are closely linked. To start securing your data, you need to know exactly where it's stored and how. Then, with this comprehensive understanding of your data landscape, you can pinpoint those operations or processes where data resilience might be lacking and tackle your data portability.

By reworking data resilience from the ground-up, organisations can cement security, compliance, and sovereignty into their operations, and actively manage them through risk assessments, compliance audits, and strategies that take into account multiple suppliers.

With this in place, organisations can start leveraging hybrid cloud environments effectively, perhaps storing the most sensitive data on-premises under precise data sovereignty regulations, while offloading less critical data to the cloud. But this can only be utilised by organisations that have prioritised data portability. Rather than waiting for regulations to enforce it, organisations need to be proactive to take advantage of the flexibility, longevity, and most importantly, security of the cloud. **!**

MOVING DATA ACROSS HYBRID ENVIRONMENTS IS COMPLEX, AND ENTERPRISES MUST PROTECT PRIMARY DATA, BACKUPS, AND AI-RELATED DATASETS.

FROM PANICKED TO PREPARED: 5 WAYS MSPS CAN UPLEVEL CLIENTS' INCIDENT RESPONSE PLANNING

I SMBS OFTEN RELEGATE INCIDENT RESPONSE PLANNING — AND CYBERSECURITY IN GENERAL, IN SOME CASES — TO THE BACKBURNER. THIS HAPPENS DUE TO A LACK OF TIME AND RESOURCES.

There was a time when large enterprises were cybercriminals' primary focus. But today, small and midsize businesses (SMBs) account for nearly half of all attacks.

SMBs store valuable data similar to their larger counterparts, but budgetary constraints and a lack of internal expertise make it difficult for smaller organisations to implement comparable defenses. Yet the financial impact and reputational damage of an attack can be particularly devastating to a small business — especially with the cost of a data breach rising more \$3 million on average.

No matter how you slice it, cyber preparedness has never been more critical for SMBs. And it's up to managed service providers to help their customers become incident-ready through proactive and actionable incident response planning.

Support Through IRP

SMBs often relegate incident response planning — and cybersecurity in general, in some cases — to the backburner. This happens due to a lack of time and resources.

But with the threat landscape intensifying and the average ransom doubling, a comprehensive incident response plan (IRP) now is a must. It's the best way to preserve your customers' cybersecurity hygiene as well as their bottom lines.

Take a thoughtful and tailored approach that addresses your SMB customers' needs and resource constraints. That way, you will know if they are equipped to effectively respond to attacks.

Here are five ways to do just that:

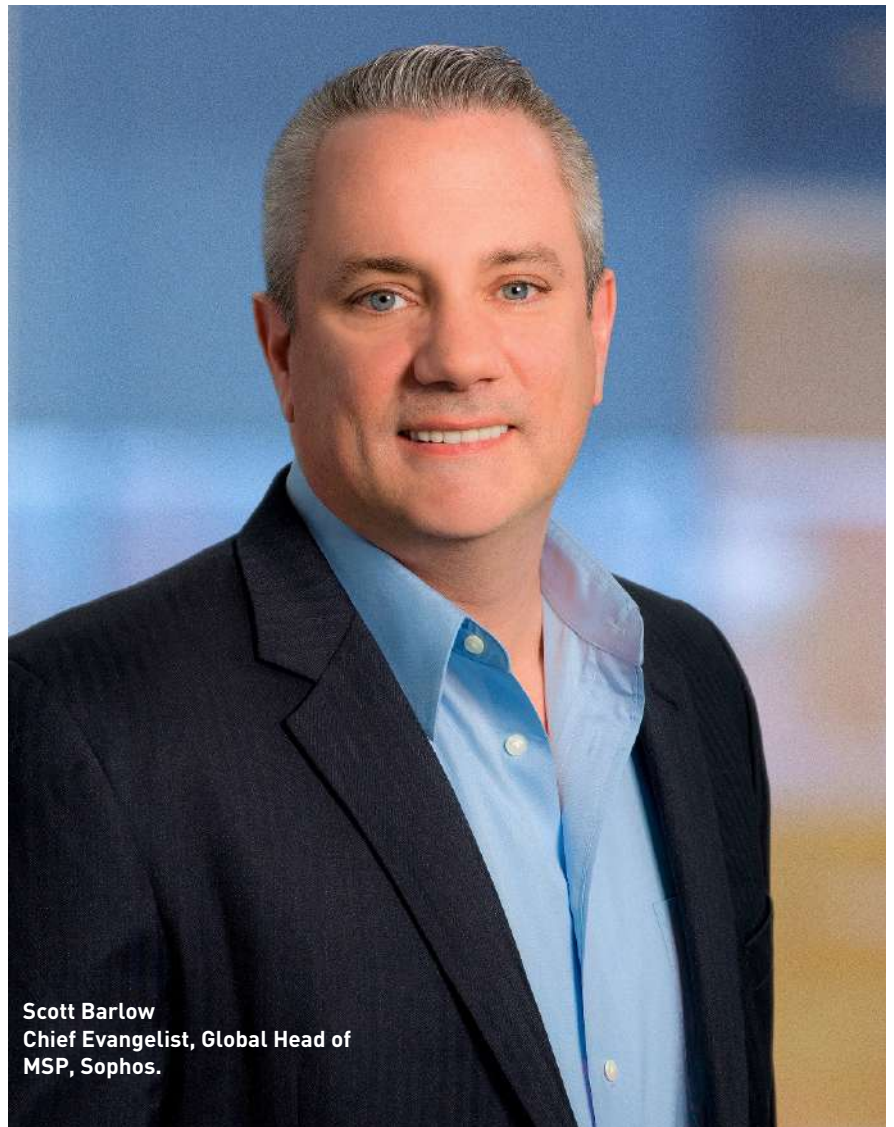
1. Assess Customers' Preparedness. If you haven't discussed IRP with your customers, start a conversation to

assess their current plans. Do they have an IRP in place? If so, when was it last updated? Have you reviewed the plan? Asking these questions can help determine next steps, whether it's refining a customer's current IRP or starting from scratch.

2. Assist in creating an Actionable Plan. If a customer lacks a comprehensive and up-to-date IRP, CISA offers advice and guidance as a starting point. For instance, CISA recommends organisations select a security program manager to create their written IRP, which should include actions to take before, during, and after a security incident. Ask customers to appoint this individual, who also can serve as your point of contact regarding the IRP. As you offer guidance, consider the following: Does it outline specific roles and responsibilities

so employees know what to do in the event of an incident? Is the plan straightforward, actionable and tailored to the organisation's risks and resources? Additionally, make sure the IRP is available to all members of the organisation and review it as a group.

3. Facilitate Tabletop Exercises (TTXs). Encourage customers to host simulated cybersecurity incidents designed to test an organisation's ability to respond to a real-world attack — with you as a facilitator. These exercises are an effective way to test your customers' IRPs. To facilitate TTXs, either develop your own scenarios or leverage CISA resources that offer practice exercises and discussion questions. After each exercise, hold retrospectives and work with the customer to refine their plan, ensuring it reflects their resource availability and evolving threats.
4. Fill in Customer Security Chasms with Third-party Services. You may uncover gaps in customers' defenses where both you and the customer lack resources to address a given issue. In these cases, many MSPs turn to third-party cybersecurity providers to complement their services. For an upfront cost, services like managed detection and response (MDR) equip customers with a dedicated team of experts to navigate dynamic threats, helping decrease their likelihood of falling victim to costly data breaches. Some cybersecurity providers also offer incident response retainers that enable experts to quickly jump into active threats, investigate, and remediate them. Collaborate with customers to assess their specific security needs and provide insights to guide strategic investments in third-party services.



Scott Barlow
Chief Evangelist, Global Head of
MSP, Sophos.

5. Promote a Culture of Security. While helping customers build their IRP, don't overlook day-to-day security hygiene. Help establish and promote a security-first culture through education and training, such as phishing training, to lay the foundation for an effective IRP. Make sure customers have adequate defenses in place, like multi-factor authentication (MFA) and strong password policies. Even the most thorough IRP can't rectify human error or lax security practices.

Build SMB Resilience By Being Proactive

The overlap is growing between the technologies and infrastructure used by SMBs and large enterprises. This means that their attack surfaces have more in common than ever.

Often, your SMB customers face the same sophisticated threats as large enterprises. However, SMBs lack the same depth of resources and expertise to prevent and mitigate the resulting attacks.

Tailor your comprehensive incident response planning to your customers' resource availability and risk exposure. Make sure they are prepared to act before, during and after a cyberattack. 🔒

KEY TECHNOLOGY TRENDS ENTERPRISE LEADERS SHOULD PREPARE FOR IN 2026

The year ahead will be a crucial turning point for how emerging technologies are implemented in companies. Businesses are now transitioning from experimentation to large-scale execution. Automation, AI, and cybersecurity now come together to form intelligent, scalable systems that have a direct impact on long-term growth, efficiency of business operations, and business adaptability. 2026 for business leaders will be all about embracing new tools, techniques, and incorporating this intelligence into the heart of their business models.

AI is no longer meant to just assist, it has evolved into goal-driven systems that have the capacity to make decisions autonomously. Agentic AI is capable of planning, reasoning, and actioning multi-step tasks without human involvement at every stage. It can further adapt to dynamic environments while taking decisions based on predefined objectives. This is in stark contrast to traditional AI, which highly depends on supervision and prompts. Agentic AI can now support processes by making them smoother, helping with planning in enterprise operations, and optimising workflows.

The issue that now comes up is the 'danger' and 'complexity rise' in tandem with autonomy. AI is already being abused by adversaries to automate assaults, produce deepfakes, and evade detection by conventional threat hunting techniques. Phishing attempts are becoming more focused, malware is becoming more evasive, and attack

cycles are progressing. This forces companies to reevaluate their security strategy and move toward AI-based cybersecurity postures that can analyse massive amounts of data, identify anomalies instantly, and respond at machine speed. This change highlights the need to bring together human skills and consistent protection that can operate at a scale and speed that manual methods cannot comprehend. In the upcoming year, the strength of an organisation's security strategy will rely on intelligent systems that are able to autonomously learn, adapt, and respond, while still having human intervention for oversight and governance.

Automation is now moving beyond digital environments into the real world. We can anticipate that Robotics-as-a-Service (RaaS) will gain traction as enterprises are looking for flexible and budget-friendly robotics deployment. Companies can have the option to subscribe to scale-based robotic abilities and benefit from regular updates instead of making large upfront investments in hardware. This will help in reducing entry barriers and increasing adoption, especially in industries where automation can directly enhance the delivery, efficiency, and safety.

Along with this, we can also see that there is a noticeable change in the development and deployment of software. Rather than seeing it as an add-on, organisations incorporate intelligence directly into the application lifecycle, thereby emphasising on being AI-native. Consequently, release cycles become faster, the quality of

code improves and there is a better possibility of technical execution meeting business requirements. Thus, AI-native development improves productivity while lowering the risk of human error in complex systems.

As technology is penetrating every aspect of our lives, it is also a call to look at the human aspect of this digital transformation. In 2026, we can expect to see a more human-centric design shaped by transparency, trust, and collaboration between us and machines. Businesses that ensure usability and explainability will succeed as this ensures that technology is a pillar that enhances human decision-making rather than casting a shadow over it. This is becoming more significant, especially in risk management, governance, and strategic planning.

Additionally, businesses should take the initiative to invest in management changes, upskilling, and ethical frameworks that support innovation in a responsible way. This is the point at which leadership becomes important in digital transformation. Only by coordinating people, applications, and procedures can businesses benefit from new technologies.

Executives will now be judged on how well they incorporate new technology into their operations rather than how quickly they adopt. Building resilient, adaptable, and sustainable operational models will be aided by the alignment of autonomy, security, automation, and human insights. Ultimately, the real differentiator as technology develops will be strategic integration in 2026. 📌



Ranjith Kaippada
Managing Director
Cloud Box Technologies

NUTANIX MAKES NC2 GENERALLY AVAILABLE ON GOOGLE CLOUD

The journey to a true hybrid multicloud reality takes a major leap forward with Nutanix announcing the General Availability (GA) of the Nutanix Cloud Clusters (NC2) on Google Cloud solution. This launch marks a significant milestone in the company's commitment to providing freedom of choice, enabling enterprises to seamlessly run, manage, and modernise applications, data, and AI anywhere — on-premises, at the edge, and in public clouds, now including Google Cloud.

Organisations are navigating increasingly complex IT landscapes, seeking to harness the power of the public cloud whilst still needing to manage on-premises and edge footprints. With NC2 on Google Cloud, Nutanix is breaking down the barriers to hybrid cloud adoption. NC2 offers a consistent platform that accelerates migration, simplifies operations, and unlocks future innovation in the cloud without the need for refactoring or rearchitecting applications. Uniquely, NC2 is a software solution, not a

managed service, so enterprises are in control of their deployments and data, but without the management overhead of a data center.

At the core of this solution is the power of Google Cloud's new Z3 and C4 Bare Metal instances powered by Titanium. These Google Compute Engine (GCE) bare metal instances are purpose-built for high-performance and storage-intensive workloads. By running Nutanix Cloud Platform (NCP) directly on these physical servers within a company's Google Cloud environment, NC2 offers a differentiated solution for virtualisation in the cloud. This means the most demanding applications and databases can run, with the performance and resilience expected from Nutanix, while taking full advantage of the elasticity and massive scale of Google Cloud.

Go Global in Hours with Google Cloud's Worldwide Reach

In today's global economy, business agility depends on the ability to deploy infrastructure where and when it is needed. NC2 on Google Cloud leverages

Google's vast and expanding global network. This allows rapid scaling of infrastructure footprint into new regions, bringing applications and data closer to customers to drive performance and support, data sovereignty and other regulatory requirements. This global reach, combined with the ability to deploy a full Nutanix cluster in just a couple of hours, unburdens IT teams from lengthy hardware procurement cycles and provides unprecedented agility for businesses. NC2 will initially be available in 17 Google Cloud global regions at GA, expanding over time, and will be available on the Google Cloud Marketplace allowing Google customers to draw down Nutanix software on their existing spending commitments.

"Nutanix Cloud Clusters on Google Cloud is more than another cloud service; it's a catalyst for real business transformation. It gives organisations a fast, flexible way to extend into the cloud, scale globally, and modernise at their own pace — all without the usual complexity. By bringing on-prem and cloud environments together under one simple operating model, it helps teams stay focused on innovation. And with easy access to Google Cloud's powerful AI and analytics capabilities, NC2 ensures businesses are ready not just for today's demands, but for the opportunities of tomorrow," said Hady Salameh, Senior Regional Sales Lead, SSA, Middle East, Egypt & Turkey at Nutanix. 

BY BRINGING ON-PREM AND CLOUD ENVIRONMENTS TOGETHER UNDER ONE SIMPLE OPERATING MODEL, IT HELPS TEAMS STAY FOCUSED ON INNOVATION.



Hady Salameh
Senior Regional Sales Lead,
SSA, Middle East, Egypt &
Turkey at Nutanix

FORCEPOINT NAMES EVA KLEIN AS CHIEF CUSTOMER OFFICER

I KLEIN BRINGS 25+ YEARS OF CYBERSECURITY AND CUSTOMER JOURNEY EXCELLENCE TO TRANSFORM FORCEPOINT CUSTOMER SUCCESS INTO GLOBAL GROWTH ENGINE FOR COMPANY'S DATA SECURITY CLOUD PLATFORM

Global cybersecurity leader Forcepoint today announced Eva Klein has joined the company as Chief Customer Officer. Klein will lead Forcepoint's global customer success organisation, overseeing onboarding, adoption, retention and long-term value realisation as customers operationalise data security in the AI era. She reports to Rick Hanson, President of Go-to-Market.

As sensitive data moves across cloud platforms, SaaS applications, endpoints and AI-driven workflows, organisations face mounting pressure to turn security investment into measurable outcomes. Agentic AI and the rapid growth of synthetic data are accelerating how data is created, shared and reused, often beyond traditional controls. Visibility alone is not enough; customers need confidence that insight leads to action and that protections adapt as

risk and regulatory demands change for enterprises and governments.

Forcepoint's AI-native Data Security Cloud helps organisations identify sensitive data in context, understand how it is accessed and shared and adapt protection in real-time through a unified, single-policy framework. The platform is built to close the visibility-to-control gap facing organisations as they scale AI adoption to support back-office processes, infrastructure management, vibe coding and beyond.

With more than 25 years of experience spanning customer success, partner enablement and sales, Klein will focus on strengthening the customer journey as a continuous loop of 'always-on' operational excellence. Most recently, she served as Vice President of Global Customer Success at Mimecast, where she led global teams focused on customer retention, value delivery and operational scale. Prior to Mimecast, she held senior

customer leadership roles including Vice President of Customer Success at HubSpot and Vice President of Customer Experience at Rapid7, building and leading organisations through periods of rapid growth and platform expansion.

"Eva joins Forcepoint at a moment when customer success is inseparable from security outcomes," said Hanson. "Customers need both data visibility and control to help them navigate the many unknowns and complexities of AI operationalisation, risk mitigation and compliance. Eva has built global success organisations that help customers realise value in exactly these environments, and her leadership will be critical as we continue to scale."

"Customers don't measure security by features — they measure it by whether it works when risk changes," said Klein. "Forcepoint's approach to data security is grounded in that reality. Helping customers turn insight into confident action, and sustain that over time, is what drew me to the company. Now is the time to hit the ground running with customers and teams worldwide as Forcepoint continues to redefine how data is protected in the AI era." **i**

CUSTOMERS DON'T MEASURE SECURITY BY FEATURES — THEY MEASURE IT BY WHETHER IT WORKS WHEN RISK CHANGES



Eva Klein

POINTGUARD AI NAMES DEV MEHTA MARKETING DIRECTOR, PLANS TO DRIVE AI SECURITY DEMAND



Dev Mehta.

I'M EXCITED TO JOIN POINTGUARD AI AS ORGANISATIONS ARE JUST BEGINNING TO UNDERSTAND THE RISKS AND OPPORTUNITIES OF AI AND AGENTIC SYSTEMS

PointGuard AI, a leader in AI and Agentic Security, today announced the appointment of Dev Mehta as Director of

Marketing. In this role, Dev will lead global demand generation strategy and initiatives as the company continues to expand its enterprise customer base in the rapidly emerging AI security market.

Dev will focus on building scalable, data-driven marketing programs to reach security, engineering, and AI leaders who are building and deploying critical AI applications to keep their business competitive.

"We're thrilled to have Dev on board at such a pivotal time for both PointGuard AI and the broader AI security landscape," said Willy Leichter, Chief Marketing Officer at PointGuard AI. "Enterprises are moving fast into an AI- and agent-driven world, and they need a trusted partner to help them secure it. Dev's experience in global B2B demand generation and partner marketing will be instrumental in helping us reach and educate those customers globally."

"I'm excited to join PointGuard AI as organisations are just beginning to understand the risks and opportunities of AI and agentic systems," said Dev Mehta. "There's a huge need for clarity and leadership in this space, and I'm looking forward to helping PointGuard AI define and lead the category." 🗣️



Empowering Cybersecurity Across the Middle East & Africa

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

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

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

→ Regional Reach, Global Partnerships

Connecting leading global vendors with the MEA region cybersecurity ecosystem.

→ End-to-End Enablement

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

→ Trusted Expertise

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

Partnering with the Best to Deliver Advanced Cybersecurity Solutions

DATAPATROL

CLOUDMON

FourCore

fileorbis

efficient iP

LEVO

Discover more at evad-me.com



25 hour
battery life on
one charge*

Meet the EM45

Serious about work and
simple to use

The Zebra EM45 Mobile Computer brings all the features your workers need in a consumer style they'll love to use. It's quick to deploy and built for retail, hospitality, transport, healthcare, and mobile workforces.

- The power of Zebra with sleek consumer ergonomics
- Unmatched productivity and flexibility for your frontline
- Personalised user experience and an intuitive interface
- Latest and fastest wireless connectivity: 5G and Wi-Fi 6E
- Processing power unlocks AI potential
- Simple to set up and manage with Zebra DNA enterprise software



Built for Work.
Designed for You.
www.zebra.com/em45



* Estimated based on average performance under typical usage conditions.

