

Security **ADVISOR**

MIDDLE EAST



BEYOND BACKUP

MIDDLE EAST ORGANISATIONS ARE EMBEDDING CYBER RECOVERY, IDENTITY SEPARATION, AND RESILIENCE INTO CORE INFRASTRUCTURE



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



22 Commvault urges regional enterprises to redefine resilience amid rising cyber risk

26 Agentic AI powers CISO accountability and mandate in AI era, says latest Splunk report

30 AI, cyber risk, digital sovereignty reshape security priorities in Mideast, says Rapid7

44 Heightened cyber risk during Middle East escalation: An ICS perspective for security leaders



CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD
CLEANROOM™ RECOVERY



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

EDITOR'S NOTE



Talk to us:

E-mail:
sandhya.dmello@
cpimediagroup.com

Sandhya DMello
Editor

CYBER RESILIENCE DEFINES NEW SECURITY AGENDA

March's edition of Security Advisor Middle East highlights a clear shift in cybersecurity across the region. Security is no longer defined only by prevention, but by how well organisations can withstand disruption, recover quickly, and maintain trust amid AI adoption, cloud dependency, and regulatory pressure.

Our news pages bring that momentum into focus through brands such as Coralogix and Skyflow, UiPath and Microsoft, Darktrace, OPSWAT, Qualys, Cohesity with Sophos, and SentinelOne. Together, they reflect a market centred on privacy-safe observability, security automation, adaptive human defence, zero-day detection, smarter patching, malware scanning, and AI-led protection, underlining how innovation is increasingly being shaped by resilience, speed, and operational confidence.

The cover story, Beyond Backup, shows why cyber recovery must now sit at the heart of enterprise resilience. Backup alone is no longer enough.

Organisations need stronger recovery frameworks, realistic testing, and architectures built to endure both cyber threats and operational instability.

Our special focus also includes Commvault's

recent Save The Day webinar with MDS, where Ravi Baldev Singh, Senior Director Systems Engineering (Emerging Markets), Commvault and Hazem Abushaban, Cyber Resilience SME and Sr. Systems Engineer (UAE Enterprise), Commvault, highlighted why traditional disaster recovery models are struggling to keep pace with ransomware, destructive malware, and outages.

The discussion reinforced a clear message for regional enterprises: backup alone is no longer enough, and resilience, clean recovery, and business continuity must now take priority.

SHAPING RESILIENT ENTERPRISE SECURITY

The interview section expands the discussion further, with Rapid7 and Splunk examining how AI, governance, and resilience are reshaping the security agenda for today's leaders.

Our opinion and research sections add valuable perspective on data sovereignty, OT security, identity risks, cybercrime, and digital trust, while our appointments coverage reflects continued momentum in the AI-native security market.

One message stands out across this edition: resilience is no longer optional. It is now central to business continuity, cyber strategy, and digital progress.

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

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

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehanjan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

© Copyright 2026 CPI
All rights reserved

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

CORALOGIX AND SKYFLOW PARTNERSHIP TO HELP PROTECT SENSITIVE CUSTOMER DATA WITHIN LOGS

Coralogix and Skyflow are launching

a strategic partnership designed to help organisations safeguard sensitive customer data within logs. This collaboration ensures robust data protection without compromising the ability to perform searches, investigations, or leverage AI-driven operations.

Logs and telemetry play a critical role in debugging, incident response, security analysis, and AI workflows. However, they often contain sensitive customer data, embedded both in structured fields and unstructured text. While many observability tools mitigate this risk through redaction, this approach comes at a cost—eliminating exposure but also stripping away context. The result? Logs become more difficult to query, correlate, and operationalise effectively.

“The traditional approach of redaction creates a false trade-off between safety and usefulness,” said Anshu Sharma, CEO of Skyflow. “Once sensitive data is stripped out, teams lose the ability to search effectively, investigate incidents, or let AI agents reason over what actually happened. As a Runtime AI Data Control Platform, Skyflow ensures sensitive customer data stays governed and isolated, while observability data remains fully usable.”

Coralogix and Skyflow take a fundamentally different approach: protect sensitive customer data by default while preserving the usability of observability data across humans and AI systems.

Ariel Assaraf, CEO, Coralogix, said: “Coralogix customers rely on observability data as a trusted system of record—supporting engineers, security teams, and the growing demands of AI-driven automation. Customers shouldn’t have to choose between safeguarding sensitive customer data and maintaining



Ariel Assaraf, CEO, Coralogix.

operational efficiency. By partnering with Skyflow, we ensure they can achieve both seamlessly.”

Why Traditional Approach Falls Short

In conventional observability pipelines, sensitive customer data is simply masked or completely removed, breaking functionality:

- Identifiers no longer match across events
- Search and correlation degrade
- AI tools lose critical context
- Teams introduce risky exceptions to get work done

Instead of permanently removing sensitive values, Skyflow replaces them with consistent, privacy-preserving tokens, allowing logs to remain searchable and analysable while the underlying data is centrally controlled, access-governed, and auditable.

Data Residency and Sovereignty by Design

Coralogix already enables customers to deploy observability workloads in specific geographic regions to meet data residency requirements. By combining this with Skyflow’s runtime data control capabilities, organisations can continue to meet strict data sovereignty obligations—ensuring sensitive customer data is governed, isolated, and accessed only under policy, while observability data remains local, usable, and compliant across regions. This approach helps organisations operating in regulated or multi-region environments reduce cross-border data exposure while maintaining full visibility and operational effectiveness.

Built for AI-Driven Observability

The joint approach enables organisations to:

- Keep sensitive customer data out of

- logs, dashboards, and downstream tools
- Preserve search, filtering, and correlation across events
- Enable AI agents to operate safely on

- telemetry, without direct access to raw sensitive data
- Allow policy-based rehydration only for approved workflows
- Reduce data sprawl and strengthen

compliance across the observability stack

The result is observability that is privacy-safe by design, operationally effective, and ready for AI-native workflows.

OPSWAT INTRODUCES AI-NATIVE DECISION ENGINE FOR RAPID, HIGH-CONFIDENCE ZERO-DAY DETECTION

OPSWAT, a global leader in critical infrastructure protection (CIP) cybersecurity solutions, has introduced MetaDefender Aether, an AI-powered decision engine for fast zero-day detection, purpose-built for the perimeter.

Unlike traditional sandbox or antivirus solutions designed for endpoint protection, MetaDefender Aether intercepts files at every entry point, e.g. file transfers, removable media, email attachments, cloud storage, and web traffic, to detect unknown threats before they reach users, devices, or internal systems. Every file is processed through four progressively deeper AI-powered layers of threat reputation, dynamic analysis, threat scoring, and threat hunting. By chaining them into a single pipeline, MetaDefender Aether delivers 99.9% zero-day detection efficacy¹, 100x greater resource efficiency than VM-based sandboxing, and a unified, confidence-scored verdict per file.

Why It Matters

Perimeter security is not just a detection problem; it is a decision problem. Security teams must rapidly determine whether a file is safe, malicious, or suspicious, and then act with confidence. Traditional antivirus and sandbox tools were never architected for this scale or complexity. Endpoint-class tools deployed at the perimeter create queue backlogs, inconclusive results, and alert fatigue. Modern adversaries now leverage AI and ML to generate evasive, obfuscated threats that bypass static and signature-based analysis.



Jan Miller, Global CTO, OPSWAT.

MetaDefender Aether was designed specifically to solve this perimeter-scale challenge and improve operational performance inside modern SOC's:

- **Faster decision velocity:** Pre-correlated verdicts with full threat-family attribution arrive in near-real time, shrinking the gap between detection and response.
- **Higher-confidence automation:** Structured outputs integrate directly into SIEM and SOAR workflows, enabling accurate automated response without manual pivots.
- **Reduced analyst fatigue:** Unified

verdicts eliminate fragmented tool outputs and false-positive overload.

- **100x greater resource efficiency:** Instruction-level emulation and intelligent pipeline layering reduce infrastructure demands compared to VM-based sandbox approaches.
- **Continuous AI-powered intelligence loop:** Every analysed file strengthens the global intelligence graph, ensuring detection improves over time.

By resolving nearly half of threats in the initial reputation layer and progressively escalating only what requires deeper analysis, MetaDefender Aether reduces

unnecessary processing and prevents perimeter-scale inspection from becoming a bottleneck for business-critical file flows.

“Traditional sandboxing was never built for AI-driven threats at scale,” said Jan Miller, Global CTO of OPSWAT. “Security teams don’t need more telemetry, they need decisive answers. MetaDefender Aether delivers on what sandboxing was not designed to do: replacing isolated analysis with an AI-native pipeline that delivers a single, high-confidence verdict that SOC teams and automation platforms can act on immediately before any file reaches the network.”

How It Works:

Layer 1 — Threat Reputation (48.7% efficacy)

Files are evaluated against OPSWAT’s continuously updated global threat intelligence databases. Known malicious files are blocked immediately, and trusted files are fast-tracked, preserving pipeline capacity for deeper analysis only when required.

Layer 2 — Dynamic Analysis (83.4% cumulative efficacy)

Files that require deeper inspection enter MetaDefender Aether’s adaptive sandbox, which uses instruction-level CPU and operating system emulation vs. virtual machines to trigger the full execution path across more than 120 file types. This exposes evasive behavior that VM-aware malware often conceals. Newly discovered indicators of compromise (IOCs) are then fed back to Layer 1 while the file is sent for downstream AI analysis.

Layer 3 — ML-Driven Threat Scoring (99.3% cumulative efficacy)

Multiple machine-learning engines analyse behavioral signals, anomaly patterns, and IOCs to assign structured, confidence-weighted risk scores. This transforms raw telemetry into high-clarity decisions, dramatically reducing false positives and analyst noise.

Layer 4 — AI-Powered Threat Hunting (99.9% cumulative efficacy)

Similarity search maps behavioral fingerprints against a database of more than 100 million analysed malware samples, automatically attributing files

to known threat families, campaigns, and attack toolkits. Unknown files are converted into actionable intelligence, enriching both global and local detection models.

MetaDefender Aether replaces fragmented sandbox, reputation, and threat intelligence lookups with a single unified decision pipeline. After completing all four stages, it delivers a single, unified verdict per file, which is fully contextualised, confidence-scored, and structured for immediate consumption by SOC analysts, SIEM platforms, and SOAR playbooks. No file enters the network partially scanned or without a decision.

Enterprise Scale and Compliance

MetaDefender Aether operates across cloud, hybrid, and air-gapped environments and supports regulatory frameworks including NERC CIP, NIS2, SWIFT CSP, CMMC, IEC 62443, GDPR, and HIPAA. The solution integrates natively across the MetaDefender ecosystem, including Core, Cloud, Email Security, MFT, ICAP, Storage, Kiosk, and Cross-Domain.

QUALYS INTRODUCES AI-POWERED PATCH RELIABILITY SCORING IN TRURISK ELIMINATE TO REDUCE PATCH ROLLBACKS

Qualys has announced the availability of AI-Powered Patch Reliability Scoring — a new capability within TruRisk Eliminate that enables organisations to predict patch impact before deployment and improve risk-based patching decisions.

“Patch rollbacks aren’t just inconvenient — they’re disruptive. They burn time, trigger outages, and create security gaps while teams scramble to stabilise production. And as patch volumes and critical vulnerabilities keep rising, the old approach of “deploy and hope” or “test everything forever”, doesn’t scale,” said Eran Livne, Sr Director of Product Management, Qualys.



Eran Livne, Sr Director of Product Management, Qualys.

“Patch Reliability Score uses artificial intelligence to analyse large-scale real-world feedback signals to forecast the likelihood that a patch will create issues in customer environments.”

The new feature continuously aggregates and evaluates data from a broad set of public sources to generate simple, actionable scores throughout a patch’s lifecycle. A high reliability score gives teams confidence to deploy more rapidly, while a low reliability score signals the need for further testing, staging, or mitigation planning.

Based on anonymised Qualys telemetry from 2025, some of the

most frequently rolled-back patches, or patches that had to be undone after deployment, included advisory USN-7545-1 and Windows updates KB5065426, KB5063878, KB5055523, and KB5066835. When Qualys Research analysed these patches against the new scoring capability, it was shown that the AI scored these patches as “Low Reliability” — matching what was ultimately experienced.

In addition to scoring reliability, organisations can pair the insights with

Qualys-curated mitigation techniques, enabling risk reduction while patches are thoroughly tested or staged for safe deployment.

Key customers benefits include the ability to:

Anticipate patch instability before outages occur

Prioritise testing efforts where needed most

Accelerate deployment when confidence is high

Deploy mitigations to maintain security during testing

“Patch management isn’t just about speed anymore — it is about predictability. With the release of this AI-powered Patch Reliability Score capability, customers can expect less guessing, fewer rollbacks and better security outcomes,” added Livne.

The AI-Powered Patch Reliability Scoring capability is now included for all Qualys TruRisk Eliminate customers.

COHESITY ENHANCES CYBER RESILIENCE WITH NEXT-GENERATION MALWARE SCANNING POWERED BY SOPHOS

Cohesity, the leader in AI-powered

data security, announced the availability of next-generation malware scanning powered by Sophos, integrated natively into Cohesity Data Cloud. Cohesity Data Cloud is the first and only data security platform to embed next-generation antivirus malware detection alongside advanced threat intelligence feeds, enabling organisations to detect malware that bypasses primary defenses and validate clean recoveries after cyberattacks.

As ransomware and supply-chain attacks grow more sophisticated, malware is increasingly present in backup data, creating the risk of reinfection during recovery. Cohesity’s Sophos-powered scanning detects zero-day, polymorphic, and fileless threats that evade signature-based tools. The feature is included with Cohesity Data Cloud Enterprise Edition and does not require a separate Sophos license.

“Cyber resilience is a team sport, and our focus is on delivering the best outcomes for customers by bringing together the strongest technologies regardless of who developed them,” said Vasu Murthy, chief product officer, Cohesity. “By deeply integrating market-leading Sophos next-generation malware



Mazin Bayado, Technical Leader-Middle East, Cohesity.

detection into Cohesity Data Cloud, we’re giving customers a single, seamless experience that helps them uncover hidden threats in backup data and recover with confidence.”

Mazin Bayado, Technical Leader - Middle East, at Cohesity, said: “In the Middle East, where cyber threats are increasing in scale and sophistication,

organisations also face growing challenges around supporting cloud data to be safely replicated to secure on-premises environments—helping customers reduce reinfection risk and maintain control over their data. By embedding advanced malware scanning into Cohesity Data Cloud, we’re enabling continuous validation of clean recovery

points so operations can be restored with confidence.”

The Sophos-powered engine uses signature-based detection, heuristic analysis, and file

emulation techniques to inspect backups in three scenarios: during routine backups, before

restoration, and after indicators of compromise (IOCs) or YARA-based matches are detected.

Incremental scanning of newly ingested data minimises operational overhead while maintaining visibility into backup integrity. Triggered and pre-restore scans validate trusted recovery points when risk is identified. The result is deep, snapshot-level inspection far beyond approaches that rely solely on metadata.

Sophos X-Ops draws on one of the industry’s most extensive threat

intelligence networks,

spanning tens of millions of endpoints and hundreds of thousands of firewalls globally, using AI-powered classification to continuously sharpen detection of known and emerging malware families.

“Attackers are sophisticated. They have proven time and again that no environment is off limits, including what was once considered the safe haven of backup and recovery systems,” said Simon Reed, chief security officer, Sophos. “By embedding Sophos’ deterministic and machine learning-based detection into Cohesity’s platform, Sophos is helping customers reduce reinfection risk and recover with confidence.”

Key benefits of the new Sophos-powered malware scanning include:

Advanced threat detection: Identifies known, unknown, and zero-day threats through heuristic and behavioral analysis

Operational efficiency: Always-on incremental scanning, with automated scans triggered by IOC or YARA-based detections

Clean recovery assurance: Pre-restore inspection to prevent reinfection and reduce recovery risk

SOC integration: Shares scan results with SIEM and SOAR tools for centralised visibility and response

The addition of Sophos next-generation malware scanning further differentiates Cohesity as a leader in incident response and recovery, delivering one of the industry’s most comprehensive data security platforms. Learn more about Cohesity Data Cloud threat protection capabilities.

SENTINELONE UNVEILS NEW AI SECURITY OFFERINGS TO GIVE DEFENDERS A DECISIVE ADVANTAGE

Agent security, Agentic investigations, and integrated AI data pipelines build on SentinelOne’s battletested AI security portfolio.

SentinelOne, the AI Security leader, has just revealed a new line up of AI security offerings, all designed to give defenders a decisive advantage. Covering both security for AI and the use of AI to automate and transform security operations, the new offerings build on SentinelOne’s market-leading AI security portfolio. From securing autonomous agents to executing full agentic investigations with a single click of a button, all the new offerings were on display at RSAC 2026 (Booth N-5863).

As organisations race to embrace AI to speed innovation, scale operations and boost productivity, AI itself has become the new attack surface and primary source of risk. Not surprisingly, Gartner has reported that AI cybersecurity – defined as both securing AI and AI-amplified security – will be amongst the

most significant and fastest growing markets in all AI spend over the next few years. In a January 2026 forecast, Gartner projected that AI cybersecurity spend will grow at an impressive 73.9% CAGR from 2024-2029, more than double that of AI spend overall.

New Prompt AI Agent Security

Building upon SentinelOne’s holistic end-to-end approach to securing AI, Prompt AI Agent Security provides a new, real-time discovery and governance control plane for AI agents and agentic workflows. It takes advantage of the same Autonomous Security Intelligence that powers SentinelOne across endpoint, cloud, and identity, extending that proprietary AI and automation into the agentic layer – monitoring, controlling, and enforcing policy on agent

interactions in real time, at machine speed. The result is full visibility, risk assessment, and policy enforcement in every MCP server operating across a customer’s environment. Also in preview, customers can manage the posture of every AI agent and agentic workflow and automatically remediate agentic behavior before unauthorised actions occur like an OpenClaw agent sending corporate data to an external endpoint without user awareness, or a Claude Cowork agent escalating privileges across enterprise systems through unauthorised action chaining.

New Prompt AI Red Teaming

Prompt AI Red Teaming gives security and product teams first-of-their-kind capabilities to test and fortify homegrown and first-party AI applications. As

developers embrace the use of agents to build new tools, applications and workflows in their enterprise environments, traditional security testing is inadequate to address the inherent AI-specific threats. With Prompt AI Red Teaming, organisations can maintain their innovation advantage without exposing their business or customers to critical risks by simulating real AI attacks (prompt injections, jailbreaks, privilege escalation, data poisoning, etc.), hardening AI apps before they ship, and continuously evaluating risks (detecting model drift, emerging vulnerabilities, new attacks vectors, etc.) as models and threats evolve.

New Purple AI Auto Investigation Now GA

At RSAC 2026, SentinelOne is building on Purple AI's lead with the general availability of new one-click Auto Investigation. Natively integrated into the Singularity Platform, this new capability allows analysts to launch complete, agentic investigations with a single click. Moving beyond rigid playbooks, Purple AI autonomously gathers cross-stack evidence, synthesises threat data, and constructs complete attack timelines in real time. It delivers clear, explainable verdicts that instantly trigger closed-loop remediation via Singularity Hyperautomation—all while maintaining strict, analyst-in-the-loop governance.

Purple AI uses an agentic framework and human-level reasoning to give security teams the advantage of speed, scale, and skills needed to stop sophisticated attacks. It also delivers intuitive human-in-the-loop automation to amplify and free up human defenders to focus on the most strategic work.

First introduced at RSAC 2023 and battle-tested in thousands of real-world SOCs and customer environments, SentinelOne's Purple AI has become the defining agentic AI security analyst offering on the market. It has also become one of the most deployed. In SentinelOne's Q4 FY26 earnings call, the



Tomer Weingarten, co-founder and CEO of SentinelOne.

company reported a record attach rate for Purple AI, as it was included in over 50% of all licenses sold during the fourth quarter.

Agentic Auto Investigations now embeds Purple AI reasoning into the most difficult part of security operations, allowing for a complete cross source deep forensic investigation at machine speed, and without additional data routing or extended permissions. All of this is delivered within the bounds of the fully regulated Singularity data platform and AI SIEM.

As a result, Purple AI's new agentic Auto Investigations shrinks security investigations that took hours and days into minutes and seconds - helping defenders level the playing field and equalise the speed of AI-driven, machine speed attack.

Purple AI Auto Investigations is available for all Purple AI Analyst customers, with no further deployment or configuration needed.

New AI Data Pipelines in Singularity AI SIEM

Following the Observo AI acquisition, SentinelOne is integrating AI-native data pipeline capabilities directly into Singularity AI SIEM to offer the only SIEM on the market to provide both pre-ingestion analytics and flexible

data collection in a single platform. Bundled as part of Singularity AI SIEM, this integrated AI data pipeline includes intelligent filtering, enrichment, ND normalisation — all operating upstream before data reaches the Singularity Platform. This reduces data noise by up to 80% before ingestion, reducing infrastructure costs, while unlocking AI-detection and response across third party data at enterprise scale.

"From our founding SentinelOne has embraced AI and automation to give those that defend our world a deciding operating advantage," said Tomer Weingarten, co-founder and CEO of SentinelOne. "Many of the world's largest and most critical organisations trust SentinelOne's AI Security portfolio to safeguard AI use and amplify human defenders. With these new innovations, organisations can now ingest and sanitise security source data on the fly into the Singularity Platform and have complete human supervised agentic investigations to bring their security operations to machine speed - today. The new innovations build on our proven and production-grade foundation, to ensure customers can confidently harness the full power of AI today, knowing their initiatives are secure, well-governed, and resilient against future threats."

PHANTOM LABS ANALYSIS OF BEYONDTRUST DATA FINDS AI AGENTS UP 466.7%

BeyondTrust, the global leader in privilege-centric identity security protecting Paths to Privilege, has released new research from its Phantom Labs team revealing a 466.7% year-over-year increase in AI agents operating inside enterprise environments. The findings, surfaced through BeyondTrust's Identity Security Insights on the Pathfinder Platform, point to the rapid emergence of what researchers call a "shadow AI workforce"—AI-driven identities deployed across cloud services and enterprise applications without centralised governance or clear visibility into the privileges they hold.

"Organisations are introducing thousands of new machine identities through AI agents, often without realising the level of access those agents inherit," said Fletcher Davis, Director of Research for BeyondTrust Phantom Labs. "In many environments we studied, AI agents were operating with privileges comparable to human administrators. As organisations move from chatbot use cases to more autonomous agentic AI, the identity attack surface will only expand."

Key Findings

Phantom Labs researchers identified several concerning patterns across assessed environments:

- Shadow AI agents operating outside formal IT governance, often deployed through low-code platforms or embedded enterprise applications
- AI agent identities that appear



Fletcher Davis, Director of Research, BeyondTrust Phantom Labs.

appropriately governed in static reports but can elevate privileges in unexpected ways during use

- Machine and AI identities outnumbering human identities by orders of magnitude, with the ratio accelerating
- Long-lived API keys and static credentials used by AI agents without rotation policies or lifecycle controls

This growth is being driven by rapid adoption of AI-enabled enterprise platforms, including Microsoft Copilot and Azure AI Foundry, AI capabilities embedded in Salesforce and ServiceNow, AI-powered coding assistants, and AI features within collaboration tools such as Jira and Confluence. Some organisations already operate well over 1,000 AI agents, many of which security teams were not fully aware existed.

Unlike traditional service accounts, AI

agents can inherit permissions from users or service roles, interact with APIs and enterprise tools, and act autonomously across systems. That combination of autonomy and privilege creates attack paths that traditional security tools were not designed to detect. BeyondTrust's Identity Security Insights is purpose-built to uncover these hidden identity relationships, map real-world attack paths, and provide actionable guidance to reduce risk.

Building on Ongoing Phantom Labs Research

These findings build on a growing body of Phantom Labs research into how AI platforms introduce identity and privilege risks:

- In earlier work, researchers demonstrated a real-world breach scenario involving Microsoft Copilot Studio where AI agents leaked secrets and granted unauthorised access to cloud infrastructure despite existing security controls.
- Separate research into AWS Bedrock uncovered how long-term API keys can automatically create IAM users with overly broad permissions, and the release of bedrock-keys-security, an open-source tool for detecting and blocking those exposures (available on GitHub).

Free AI Security Posture Assessment

BeyondTrust's Identity Security Risk Assessment (ISRA), powered by Identity Security Insights, gives organisations visibility into AI agent risk as part of a broader identity security posture analysis. The assessment connects across enterprise identity systems and AI agent infrastructure to identify unmanaged AI identities, detect shadow AI, and map cross-domain privilege paths with prescriptive remediation guidance aligned to MITRE ATT&CK.

ORGANISATIONS ARE INTRODUCING THOUSANDS OF NEW MACHINE IDENTITIES THROUGH AI AGENTS, OFTEN WITHOUT REALISING THE LEVEL OF ACCESS THOSE AGENTS INHERIT.

UIPATH COLLABORATES WITH MICROSOFT TO ACCELERATE SECURITY, CONFIDENCE FOR AUTOMATED WORKFLOWS

Integration demonstrates the power of agentic automation and security platforms working together to protect modern enterprises.

UiPath, a global leader in agentic automation, announced a new security automation capability, built in collaboration with Microsoft, to help organisations accelerate security operations when applying automation to business workflows. The solution automates threat detection, enrichment, and response workflows across Microsoft Defender for Cloud, Microsoft Sentinel, and integrated Microsoft threat intelligence.

“This collaboration brings security automation closer to where work actually happens,” said Andrei Oros, Director of IT Automation at UiPath. “The combination of our automation capabilities with Microsoft Defender, Sentinel, and Security Copilot gives enterprises the ability to embed security controls into operational processes. It’s the peace-of-mind businesses need to adopt automation across their organisation, with the confidence that the data and information driving their most important workflows is compliant and secure, and that it won’t interrupt their business.”

The combination of UiPath’s enterprise automation platform with Microsoft’s suite of security offerings enriches security detection with business context, ensuring that an enterprise’s security operations center can stay ahead of the pace of business. Security and mitigation efficiency and productivity are elevated, accelerating mean time to resolve (MTTR) and minimising process and business disruption. Designed for enterprise scale and aligned with Microsoft’s security ecosystem, the solution will be available in the UiPath Solutions Marketplace, making it easy for organisations to discover, deploy, and operationalise



Andrei Oros, Director of IT Automation, UiPath.

UiPath-powered security automation as part of their existing Microsoft security investments.

“UiPath’s integration with Microsoft fuses automation with built-in security and governance – enriching signals with business context, empowering human-in-the-loop decisions, and accelerating detection and response – so enterprises can scale agentic automation with confidence,” said Ruthy Kaidar, Managing Director Solutions, Software Companies, Microsoft EMEA.

Files and signals originating from automated business workflows can be scanned automatically using Microsoft Defender for Cloud, enriched with business context, and forwarded to Microsoft Sentinel for investigation. Once

forwarded, security analysts can then leverage Microsoft Security Copilot for guided, human-in-the-loop analysis of those artifacts and data, while UiPath automations execute follow-up actions such as quarantining files, pausing workflows or escalating incidents, reducing mean time to respond, and improving overall SOC efficiency.

“Security teams need solutions that move at the speed of modern threats,” said Steven Spirou, Senior Product Manager, Microsoft Security. “UiPath’s work with Microsoft Sentinel and Security Copilot demonstrates how partners can extend the platform with automation, richer context, and faster response, bringing real, production-grade value to SOC teams.”

DARKTRACE INTRODUCES NEW GENERATION OF PERSONALISED, REAL-TIME SECURITY TRAINING AND PROTECTION

The platform uses the results of those micro-coaching sessions to fine-tune safeguards around each person's inbox, delivering personalised protection across the organisation.



Darktrace, a global leader in AI for cybersecurity, announced the launch of Darktrace / Adaptive Human Defense, a new generation of security coaching that replaces static, scheduled security awareness training with adaptive real-time coaching and protection.

Darktrace / Adaptive Human Defense applies behavioural AI to teach users during their work day, notifying them of risky behaviour and providing short, relevant coaching on those risks before bad habits form. The platform uses the results of those micro-coaching sessions to fine-tune safeguards around each person's inbox, delivering personalised protection across the organisation.

The launch comes as new Darktrace research points to a gap between

employee confidence from existing security awareness training and actual preparation for modern phishing attacks. While 80% of US office workers surveyed by Darktrace say they are confident they could spot a phishing email in their day-to-day work, in a test of realistic messages only 32% confidently identified an actual phishing email. The findings suggest that established training approaches may be building confidence faster than real-world phishing readiness.

The challenge is not limited to employees. Darktrace's research suggests security professionals are not strongly convinced that conventional security awareness training is keeping pace with modern phishing. While 62%

of security professionals surveyed agree it is effective at preparing employees to identify phishing attempts, only 11% strongly agree, and just 2% say they see no limitations in conventional training. The biggest limitations surveyed professionals identify are training being too one-size-fits all (31%); too focused on failure (27%); and too difficult to measure meaningfully beyond completion or click rates (23%).

In 2025, Darktrace detected 32 million phishing emails targeting its customers, with more than a third (38%) using novel social engineering techniques, likely enabled by AI[1]. As bad actors use AI tools to evolve their phishing to the limits of human detection and move beyond email into collaboration tools,

organisations need an approach that both strengthens human judgment and the protections around them.

Manasseh Tsekpo, Network Security Administrator at City of St. Catharine's, a Darktrace / Adaptive Human Defense early access customer, commented "While traditional security awareness training clearly helps with confidence, it often doesn't prepare people for modern phishing attacks. That's because it's usually generic and disconnected from what's really in people's inboxes. This is the first time we've had something that feels like it's really changing behavior. The coaching is brief, contextual, and it's helping people build better habits instead of just completing training and moving on. At the same time, we know that Darktrace / EMAIL is in the background giving them the best possible protection, based on that coaching."

"Security awareness training has become an admin task for employees and a tick box for security teams, not a system that meaningfully reduces risk," added Jack Stockdale, Chief Technology Officer, Darktrace.

"Darktrace / Adaptive Human Defense replaces generic modules and ever more generative AI content with adaptive coaching that meets people in the moment, built around how they actually communicate. And through its two-way connection with Darktrace / EMAIL, organisations can finally create a closed loop where human behavior and technical defenses continually and autonomously strengthen each other."

Darktrace / Adaptive Human Defense: Security That Learns With Your People

Generative AI is making phishing attacks more convincing and targeted, making it harder to rely on people to spot every threat. Darktrace / Adaptive Human Defense works with Darktrace / EMAIL to combine real-time technical protection with personalised, behavioural AI-based coaching, helping security improve continuously at both the human and system level.

Organisations using the platform can:

- deliver contextual, real-time coaching within suspicious email threads, helping users recognise and avoid risky actions before they become habits;
- tailor phishing simulations to each user, with difficulty increasing based on behaviour and performance, including simulations shaped by live inbox activity;
- link individual coaching and email-security signals so protections can automatically adapt as users learn;
- track meaningful risk analytics and trends beyond course completion rates, helping teams identify repeat offenders and high-risk users;
- support compliance and awareness goals with customisable e-learning content aligned to internal policies.

Industry First Cross Channel Full-Message Analysis for Email, Slack, Teams, and Zoom

As social engineering increasingly starts in one channel and escalates in another, Darktrace also today announced that Darktrace / EMAIL is the first solution to provide cross-channel, full-message analysis across email, Microsoft Teams, Slack and Zoom. With the addition of Slack and Zoom to existing protections for email and Microsoft Teams, Darktrace / EMAIL now brings unified security across the channels employees use most to communicate at work for the first time, helping security teams identify blended campaigns and subtle, context-driven manipulation wherever it appears.

As a result, Darktrace / EMAIL eliminates the cross-channel blind spots attackers exploit for pretexting, escalation, and account takeover by detecting phishing, malware, and conversational manipulation with consistent behavioral depth everywhere that workers are communicating. Dedicated models also surface emerging prompt-injection threats targeting corporate AI assistants, helping reduce

the risk of silent compromise earlier.

DMARC Upgrades: Reducing Impersonation Risk At The Source With Attack Surface Management Integration

Alongside increasingly sophisticated phishing attacks, AI is enabling bad actors to more effectively impersonate established brands and exploit the trust placed in them. DMARC provides an established standard to help organisations prove that emails sent in their name are authentic and Darktrace is today introducing the first DMARC solution with two-way, first-party integration to attack surface management and leading email security to help teams reduce impersonation risk at the source.

Most organisations still treat domain protection as two separate tasks: DMARC tools validate whether messages claiming to be from your domain are authenticated, while attack surface management maps exposed internet-facing assets and configuration risks. By connecting DMARC, attack surface management, and email security with signals flowing between all three, Darktrace helps teams move faster from inbox events to the underlying fixes. Teams can unify SPF, DKIM, and DMARC configuration with external exposure and DNS-level insights to identify and correct weaknesses before attackers exploit them, and pivot between Darktrace / EMAIL and Darktrace / EMAIL-DMARC to streamline triage.

"Attackers do not care which app your company uses to communicate. They exploit people, context, and trust, then move across channels until they find a moment to succeed," said Stockdale. "That is why the future of protection is unified and adaptive. If your human layer is trained in isolation, and your security controls are tuned in isolation, you are leaving gaps. With Darktrace / Adaptive Human Defense and expanded cross-channel coverage in Darktrace / EMAIL, we are closing those gaps with a single self-learning AI architecture."

DATA BACKUP AND RESILIENCE: BUILDING CYBER RECOVERY INTO CORE OF ENTERPRISE SYSTEMS



IMMUTABLE BACKUPS, RAPID RECOVERY, HYBRID ARCHITECTURE, AND IDENTITY SEPARATION FORM THE BACKBONE OF MODERN RESILIENCE STRATEGIES IN AN AI-DRIVEN THREAT LANDSCAPE.



Organisations across the Middle East are operating in an environment where cyberattacks, infrastructure instability, and regulatory complexity intersect. Backup is no longer a secondary IT function. It is operational insurance — and, increasingly, a strategic pillar of business continuity.

Ransomware actors now target recovery environments as aggressively as production systems. At the same time, national data sovereignty requirements, cloud dependency, and AI adoption introduce new architectural considerations. Resilience demands a deliberate shift from simple backup routines to comprehensive recovery strategies.

Backup Alone Is Not Enough

Fred Lherault, CTO EMEA/Emerging at Everpure, reinforces the need for a broader approach and said, “Backing up data remains critical for data protection, but it’s not enough. Implementing advanced data protection capabilities helps companies better plan for — and recover quickly from — ransomware and cyberattacks. This essentially requires a two-pronged approach: taking regular, immutable, and indelible copies of data, and having the necessary infrastructure to rapidly restore from backups at speed and scale.”

Immutable and indelible copies ensure data cannot be altered, encrypted, or deleted — even if administrative

**Fred Lherault,
CTO EMEA/Emerging, Everpure.**



credentials are compromised. In a ransomware event, organisations can restore clean versions of critical systems without negotiating with attackers.

Protection, however, is only half the equation. Recovery speed determines business impact. Modern flash-based storage platforms now enable restoration

at scale — often reaching hundreds of terabytes per hour — reducing downtime from weeks to hours and significantly limiting operational disruption.

Independence Determines Availability

Ziad Nasr, General Manager for Acronis Middle East, argues that backup must be treated as core operational infrastructure rather than an add-on service.

During a crisis, failure often begins with identity systems, connectivity, or centralised management layers. When backup platforms rely on the same credentials, network paths, or control planes as production systems, recovery can become inaccessible at the moment it is most needed.

Administrative separation is essential. Dedicated accounts, strict privilege control, and strong authentication reduce exposure when credentials are

BACKING UP DATA REMAINS CRITICAL FOR DATA PROTECTION, BUT IT’S NOT ENOUGH. IMPLEMENTING ADVANCED DATA PROTECTION CAPABILITIES HELPS COMPANIES BETTER PLAN FOR — AND RECOVER QUICKLY FROM — RANSOMWARE AND CYBERATTACKS.

FRED LHERAULT, CTO EMEA/EMERGING, EVERPURE.

stolen. Geographic distribution further strengthens resilience. Combining local recovery copies for rapid restoration with offsite or cross-region replicas mitigates concentration risk and limits the impact of facility outages or regional disruptions.

Disaster recovery (DR) strategies must extend beyond data restoration. Secondary recovery sites and cross-cloud failover capabilities allow critical workloads to restart in alternate environments if primary infrastructure becomes unavailable.

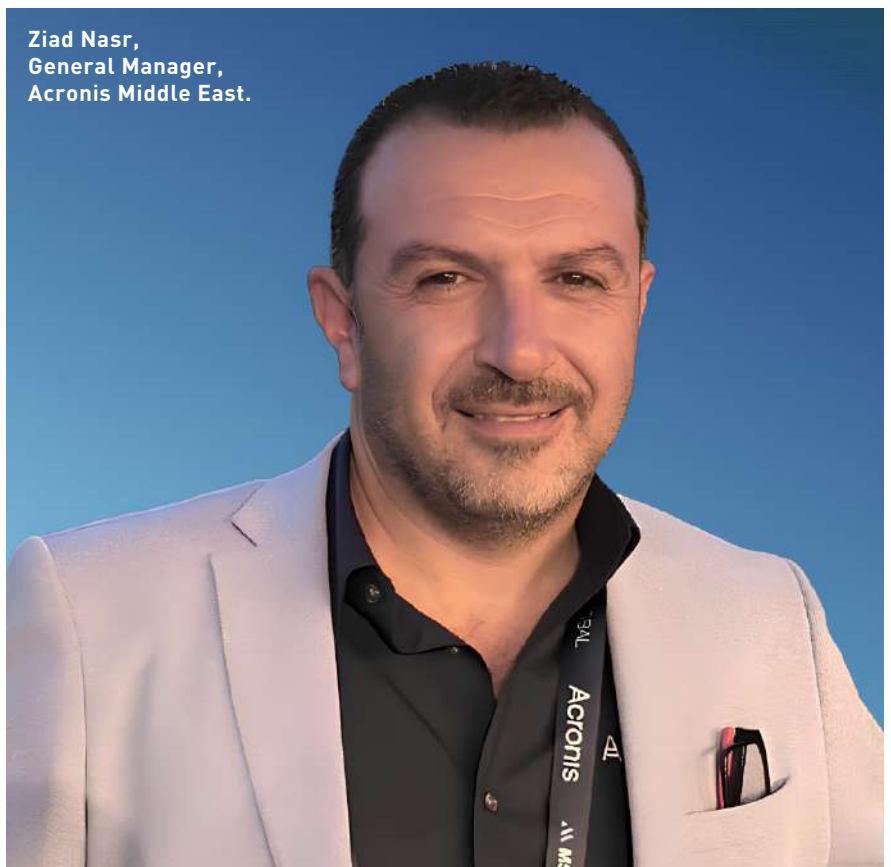
"Recovery should be exercised against realistic disruption scenarios. Simulating prolonged outages or loss of a primary site reveals operational gaps before a real crisis does. Backup is valuable only if it remains accessible and usable when infrastructure is under pressure, and DR is effective only if workloads can be restored and operated in an alternate location without relying on the compromised environment," said Nasr.

Testing Under Constraint

Recovery exercises often assume full connectivity and stable conditions. Real-world incidents rarely unfold so neatly.

Organisations must validate restoration processes under constrained scenarios: limited bandwidth, offline identity systems, restricted facility access, or partial network outages. Full-site failover testing confirms applications and services can operate in alternate environments rather than merely restoring raw data.

National infrastructure disruption introduces additional risk factors,



Ziad Nasr,
General Manager,
Acronis Middle East.

including power instability and backbone connectivity loss. Diversification across facilities, providers, and jurisdictions reduces exposure to single points of failure. Cross-border or multi-cloud DR architectures provide controlled recovery options when regional disruption or regulatory restrictions interfere with operations.

Local restore capabilities, documented offline procedures and clearly defined escalation paths reduce reliance on fragile external dependencies during instability. DR environments capable

of independent operation for defined periods offer an additional safety net.

Navigating Data Sovereignty and AI Dependency

Andreas Hassellöf, Chief Executive Officer at Ombori, highlights the architectural complexity created by regional data sovereignty laws. Regulatory requirements often concentrate infrastructure within a single geography, increasing exposure during disruption.

Hybrid strategies offer a balanced path. Compliant regional storage can be paired with structured redundancy models, selective on-premise capabilities and edge computing nodes supporting critical workloads.

AI adoption introduces further dependency on external providers. Capacity constraints or service interruptions affecting large language models can disrupt customer-facing and operational workflows. Maintaining

BACKUP IS VALUABLE ONLY IF IT REMAINS ACCESSIBLE AND USABLE WHEN INFRASTRUCTURE IS UNDER PRESSURE.

ZIAD NASR, GENERAL MANAGER, ACRONIS MIDDLE EAST.

a selective on-premise AI inference infrastructure enhances operational continuity while supporting privacy and low-latency processing requirements.

Cloud delivers scale and efficiency. Long-term resilience requires architectural flexibility across multiple infrastructure models.

Immutable Foundations for Business Continuity

Immutable backup anchors recovery integrity. When data is written in a format that cannot be altered or deleted, even elevated threat activity cannot compromise the recovery point. Destructive malware frequently attempts to target backup repositories directly. Immutability ensures a verified, trustworthy restoration baseline.

“When data is written in an immutable format, it cannot be altered or deleted even if administrative credentials are compromised. During periods of elevated threat activity, destructive malware and ransomware attempts often increase, including attempts to target backup repositories directly,” said Hassellöf.

“Immutable storage ensures that organisations retain a verified recovery point. It anchors restoration processes and restores confidence in system integrity. In an AI-accelerated threat environment, trusted recovery mechanisms form the foundation of business continuity,” added Hassellöf.

Comprehensive resilience planning integrates:

- Hybrid infrastructure models



**Andreas Hassellöf,
Chief Executive Officer, Ombori.**

- Regular recovery testing under realistic scenarios
- Immutable backup strategies
- Clearly defined recovery time objectives (RTOs) and recovery point objectives (RPOs)
- Cross-region or cross-cloud failover options
- Segregated identity and administrative controls

WHEN DATA IS WRITTEN IN AN IMMUTABLE FORMAT, IT CANNOT BE ALTERED OR DELETED EVEN IF ADMINISTRATIVE CREDENTIALS ARE COMPROMISED.

ANDREAS HASSELLÖF, CHIEF EXECUTIVE OFFICER, OMBORI.

Prepared organisations design continuity across multiple disruption scenarios — cyber, infrastructural and regulatory.

In an AI-accelerated threat landscape, recovery integrity is no longer optional. Trusted backup, rapid restoration and architectural flexibility form the foundation of enterprise resilience. **i**



عالم الذكاء الاصطناعي
EVERYTHING
 -ABU DHABI-
 ADNEC CENTRE

11 MAY
 — 2026
SUMMIT

12/13 MAY
 — 2026
EXPO



Ai Semi**con**
 EVERYTHING



PHYSICAL
 AI
 EVERYTHING



AI DIGI HEALTH
 & BIOTECH
 EVERYTHING

AI
 GOVERNMENT
 EVERYTHING



WHERE THE WORLD CONVENES IN NEW INTELLIGENCE

The world's biggest showcase of AI solutions ready to transform every industry bringing together global leaders, startups and the world economy for the most ambitious showcase of applied AI innovation, alongside bold debates shaping the future of intelligent societies.

25,000⁺
 VISITORS

850⁺
 AI COMPANIES

150⁺
 COUNTRIES

\$60K⁺
 Prize Pool

\$50B⁺
 AUM

250⁺
 INVESTORS



GET INVOLVED

aieverythingabudhabi.com

sales@aieverythingabudhabi.com



#AIEverythingAbuDhabi

COMMVault URGES REGIONAL ENTERPRISES TO REDEFINE RESILIENCE AMID RISING CYBER RISK

COMMVault EXECUTIVES RAVI BALDEV SINGH AND HAZEM ABUSHABAN OUTLINE WHY MINIMUM VIABILITY, CLEAN RECOVERY, AND AIR-GAPPED PROTECTION ARE BECOMING CRITICAL FOR ENTERPRISES NAVIGATING CYBER RISK AND OPERATIONAL DISRUPTION.



Cyber resilience, recovery readiness, and business continuity have become urgent boardroom priorities for enterprises navigating a more volatile threat landscape. CPI Media Group in association with Commvault and MDS, recently hosted 'Save The Day'

webinar where Ravi Baldev Singh, Senior Director Systems Engineering (Emerging Markets), Commvault, and Hazem Abushaban, Cyber Resilience SME and Sr. Systems Engineer (UAE Enterprise), Commvault, outlined why traditional disaster recovery is no longer enough in an environment shaped by ransomware,

destructive malware and cloud outages.

The session focused on total resilience, a more comprehensive approach that combines disaster recovery, cyber recovery, clean data restoration, and operational continuity. The discussion made clear that enterprises can no longer afford to view backup as a

standalone function. Recovery must now be tied directly to business survival.

A key theme running through the webinar was the concept of minimum viability, which raises the ability of an organisation to restore its most critical systems, teams, and processes within a realistic timeframe so it can continue operating, even in a reduced capacity.

Closely linked to this is the concept of survival time objective, which challenges businesses to define how long they can afford to remain disrupted before the operational, financial, and reputational impact becomes unacceptable.

Ravi Baldev Singh, Senior Director Systems Engineering (Emerging Markets), Commvault, said: "Organisations need to move beyond broad conversations around backup and availability and instead define, very clearly, what minimum viability means for their business. Businesses must ask which systems, services, teams, and communication channels must come back first, and within what survival time."

In today's environment, resilience is no longer just about disaster recovery; it is about cyber recovery, business continuity, and the ability to recover cleanly under pressure.

"Boards, business leaders, and technology teams must challenge outdated assumptions now, because those who prepare well will not only survive disruption, but emerge stronger and more trusted in the market," added Singh.

Many organisations are still relying on outdated assumptions about resilience, which include the belief that cloud environments are automatically safe,



**Ravi Baldev Singh,
Senior Director Systems
Engineering (Emerging
Markets), Commvault.**

that backup copies are always clean and recoverable, or that disaster recovery and cyber recovery are effectively the same discipline.

Enterprises now need structured blueprints that align technology recovery with business-critical outcomes.

The blueprint-driven approach formed an important part of Commvault's message during the session. The company positioned resilience as an ongoing operational model rather than an ad hoc emergency response. This includes identifying the applications that

matter most, mapping dependencies, understanding where data resides across on-premises and cloud environments, and creating runbooks that can support recovery under real-world pressure.

The webinar also highlighted how resilience architecture must now extend far beyond traditional infrastructure. Organisations increasingly need to protect a broad mix of workloads, including Microsoft 365, Entra ID, Salesforce, Google Workspace, cloud-native services, and on-premises applications, while maintaining flexibility around data location, compliance, and sovereignty requirements.

A major part of the discussion centred on the role of air-gapped, immutable copies of data. Commvault explained that many customers across the region are looking to establish protected secondary and tertiary copies that sit outside the primary production environment, either in-country or out of country,

BOARDS, BUSINESS LEADERS, AND TECHNOLOGY TEAMS MUST CHALLENGE OUTDATED ASSUMPTIONS NOW.

RAVI BALDEV SINGH, SENIOR DIRECTOR SYSTEMS ENGINEERING (EMERGING MARKETS), COMMVault.

depending on regulatory approvals and organisational policy. This is particularly relevant for businesses seeking to reduce exposure to ransomware, destructive attacks, or cloud-region outages.

Another major focus area discussed in the Webinar was the need for clean recovery. Commvault stressed that it is no longer enough to ask whether data can be recovered. The more important question is whether it can be recovered in a clean and trustworthy state.

Capabilities such as threat scanning, clean room recovery, and cyber recovery testing become crucial, allowing organisations to validate recovery points and restore systems in a controlled and isolated environment before returning to production.

Hazem Abushaban, Cyber Resilience SME and Sr. Systems Engineer (UAE Enterprise), Commvault, said: "What we are seeing across the region is a strong shift from conventional backup thinking towards true operational resilience. Customers want flexibility, speed, and confidence that their data is not only protected, but recoverable in a clean and controlled way. Air-gapped copies, immutable storage, clean room recovery, and extended protection across cloud, SaaS, and on-premises workloads are now essential. The challenge today is not just where data sits, but how quickly and safely organisations can recover it when under pressure. Resilience must now be built as a practical, tested architecture rather than treated as a secondary layer."

Abushaban also underlined the



**Hazem Abushaban,
Cyber Resilience SME and
Sr. Systems Engineer
(UAE Enterprise), Commvault.**

importance of identity recovery as part of any cyber resilience strategy. If Active Directory or Entra ID is compromised, the wider recovery process becomes significantly harder. Identity protection and recovery, therefore, become a foundational requirement rather than a secondary consideration, particularly for enterprises seeking to restore core services quickly after a cyber incident.

Compliance and sovereignty remain

major considerations for many sectors, especially regulated industries and public sector organisations. However, recent events have prompted some businesses to re-examine long-held assumptions around where backup copies can reside and what kind of exceptions may be possible in extraordinary circumstances.

Commvault said its software-defined and storage-agnostic approach is designed to support that flexibility across public cloud, sovereign cloud, national repositories, and on-premises environments.

The wider takeaway from the webinar was clear: cyber resilience in 2026 is no longer just a technical safeguard; it is becoming a core business requirement tied to trust, continuity, and competitive strength. For enterprises across the region, the ability to recover minimum viable operations quickly and cleanly may prove just as important as preventing the breach itself. 🔒

CUSTOMERS WANT FLEXIBILITY, SPEED, AND CONFIDENCE THAT THEIR DATA IS NOT ONLY PROTECTED, BUT RECOVERABLE IN A CLEAN AND CONTROLLED WAY.
HAZEM ABUSHABAN, CYBER RESILIENCE SME AND SR. SYSTEMS ENGINEER (UAE ENTERPRISE), COMMVAULT.

 **tahawultech.com**

KSA FUTURE ENTERPRISE AWARDS 2026



**30th August
2026**



**Radisson Blu Hotel & Convention Center
Riyadh Minhal**



06:30 PM onwards

#KSAFEA2026 | #tahawultech

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

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

GOLD SPONSORS



AHAD
Securely Transform

logitech®

OFFICIAL PUBLICATIONS

cnme
computer news middle east

Reseller
MIDDLE EAST
THE VOICE OF THE CHANNEL

Security
MIDDLE EAST
THE VOICE OF THE CHANNEL

HOSTED BY

 **tahawultech.com**

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

<https://tahawultech.com/ksa-futureenterpriseawards/2026/>

AGENTIC AI POWERS CISO ACCOUNTABILITY AND MANDATE IN AI ERA, SAYS LATEST SPLUNK REPORT

SPLUNK'S 2026 CISO REPORT REVEALS RISING ACCOUNTABILITY, AI-DRIVEN RESILIENCE, AND THE EXPANDING STRATEGIC ROLE OF SECURITY LEADERS.

The release of The CISO Report: From Risk to Resilience in the AI Era by Cisco and Splunk signals a defining moment for global cybersecurity leadership. Based on insights from 650 Chief Information Security Officers worldwide, the report captures a profession undergoing rapid transformation — driven by AI acceleration, rising threat sophistication, and mounting regulatory pressure.

CISOs today are no longer confined to managing security incidents. Nearly all respondents report expanded responsibilities spanning AI governance and enterprise-wide risk management, while more than four in five now oversee secure software development practices. The mandate has broadened — and so have the stakes.

AI has emerged as both a powerful enabler and a formidable threat multiplier. While 92% of CISOs say AI allows their teams to review more security events and 89% report improved data correlation, concerns remain high. Eighty-six percent

fear agentic AI will increase the sophistication of social engineering attacks, and 82% anticipate greater deployment complexity in persistence mechanisms. The message is clear: AI is essential for resilience, but governance must evolve in tandem.

Beyond technology, the human factor remains paramount. Security leaders are prioritising upskilling, talent retention, and cross-functional accountability to combat burnout and close capability gaps. High alert volumes, false positives and tool fatigue continue to strain teams, reinforcing the need for unified platforms and clearer data visibility.

Regional markets such as the UAE offer a compelling lens on digital transformation. Strong governance frameworks, sovereign data mandates and ambitious AI investment are reshaping the cybersecurity agenda across sectors.

The following interview excerpts feature insights from Ahmed El Saadi, Vice President – Middle East, Africa, Turkey, Romania & CIS at Splunk, who shares perspectives on the UAE's

digital evolution, the expanding CISO mandate, AI's growing influence on security strategy and practical guidance for building resilient, cost-efficient data infrastructure.

Interview Excerpts

How do you assess the UAE's progress in positioning itself as a Digital First nation?

The UAE represents a blueprint for strong cybersecurity hygiene. Policy-making, governance frameworks and public-private partnerships are all aligned to support secure digital transformation. Digital investment in the UAE is expected to reach nearly \$20 billion over the next three years across IT, telecoms, and IoT. AI spending alone is forecast to reach \$1.9 billion by 2026. Such ambitious adoption requires cybersecurity to be embedded from the outset — across frameworks, governance, technology and talent. AI expansion further reinforces cybersecurity's importance. As digital adoption grows, security must scale in parallel to maintain resilience and trust.

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



What is the most significant shift highlighted in this year's Splunk CISO Report 2026?

The most significant shift identified in the report is the rapid expansion of the CISO's role. Based on insights from more than 650 CISOs globally, 96% state that their responsibilities now extend far beyond traditional cybersecurity oversight to include AI governance and enterprise-wide risk management. Security leaders are increasingly embedded in strategic business decision-making, as AI adoption for revenue growth, productivity optimisation, and faster go-to-market initiatives requires robust governance frameworks. CISOs are now central to shaping those frameworks. Their remit has also expanded into DevSecOps, ensuring that security is embedded into application development from the earliest stages rather than being addressed retrospectively.

With the rise of agentic AI, does the market have enough skills to support this shift?

AI is expected to augment human expertise rather than replace it, with approximately 60% augmentation anticipated through AI-enabled capabilities. Technologies such as large language models allow professionals to interact with systems using natural language, reducing reliance on deep coding specialisation. However, the rapid pace of AI-driven innovation and the growing volume of use cases mean continuous upskilling and reskilling will be essential. Demand for talent is likely to outpace supply for some time. Vendors, including Splunk, carry a responsibility to support this transition

through enablement programmes, structured adoption tracks and sustained workforce development initiatives.

Why is AI becoming central to cybersecurity strategy?

Threat sophistication is increasing at an unprecedented pace, with 95% of CISOs reporting more advanced cyber threats. At the same time, 92% believe AI enables their teams to review more security events, while 60% say it improves and augments cybersecurity operations. Attackers are leveraging AI techniques to accelerate and refine their methods, compelling defenders to adopt AI-driven capabilities in response. AI allows security teams to correlate data more effectively, prioritise high-risk incidents and reduce detection and response times. The shift moves cybersecurity from a volume-based model to a quality-driven strategy, delivering deeper insights and more precise threat mitigation.

Are CISOs facing increased pressure due to this expanded role?

The role has become significantly more demanding, bringing greater personal liability and regulatory accountability. CISOs are now responsible not only for cybersecurity posture but also for AI governance and broader risk oversight, adding to operational complexity. Burnout remains a pressing issue, with 98% citing high alert volumes as a primary stressor, 94% pointing to false positives and many highlighting tool fatigue from managing multiple disconnected systems. While AI can help reduce noise and streamline workflows, it does not eliminate the

accountability and personal risk associated with the role. The CISO position has evolved into one of the most strategically important and high-pressure roles within the organisation.

Is upskilling becoming a priority for CISOs?

Upskilling has become a strategic imperative. Focus areas include AI governance frameworks, advanced risk mitigation strategies, AI-enabled security operations and embedding governance directly into operational processes. Continuous education is critical to remain effective in a rapidly evolving threat environment, and organisations are increasingly investing in both structured training and practical capability development to ensure their security leaders and teams remain ahead of emerging risks.

What advice would you give organisations seeking a strong data infrastructure with controlled investment?

Organisations should prioritise breaking down operational silos, as multiple departments often rely on separate tools and fragmented datasets, slowing detection and response. A unified data platform can reduce duplication, streamline workflows, and improve overall efficiency. Centralising data visibility is equally important, since resilience begins with a comprehensive view of security, IT operations, and DevOps environments within a single ecosystem. Finally, a cross-functional partnership is essential. Modern CISOs must operate as business collaborators rather than purely policy enforcers, fostering open communication across the C-suite to support AI governance, risk management and shared accountability. Unified platforms combined with collaborative governance models help reduce complexity, accelerate response times and deliver sustainable operational value. 📌

THE SHIFT MOVES CYBERSECURITY FROM A VOLUME-BASED MODEL TO A QUALITY-DRIVEN STRATEGY, DELIVERING DEEPER INSIGHTS AND MORE PRECISE THREAT MITIGATION.

 tahawultech.com

Women in TECHNOLOGY FORUM AND AWARDS

Give to gain. Powering women in tech

Gala Dinner Event



29th April 2026



Dubai



6:00 PM onwards

#WomenInTech2026 | #IWD2026 | #tahawultech

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

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

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

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

OFFICIAL PUBLICATIONS

cnme
computer news middle east

Reseller MIDDLE EAST
THE VOICE OF THE CHANNEL

Security ADVISOR
MIDDLE EAST

HOSTED BY

 tahawultech.com

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

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

AI, CYBER RISK, DIGITAL SOVEREIGNTY RESHAPE SECURITY PRIORITIES IN MIDEAST, SAYS RAPID7

I GOPAN SIVASANKARAN, REGIONAL DIRECTOR, MEA, RAPID7, DISCUSSES HOW THE REGION'S FAST-MOVING AI AMBITIONS ARE RAISING THE STAKES FOR CYBER RESILIENCE, GOVERNANCE, AND TRUST.

A I is rapidly reshaping the Middle East's digital landscape, with national strategies such as Saudi Vision 2030 and the UAE's innovation agenda accelerating adoption across government, critical infrastructure, and enterprise operations. Cyber adversaries are also harnessing AI to sharpen reconnaissance, automate attack pathways and make phishing and social engineering campaigns more targeted and convincing.

Gopan Sivasankaran, Regional Director, MEA, Rapid7, shared his perspective with Tahawultech.com on why governance, data protection, and digital sovereignty must now sit at the heart of regional cyber strategy.

Interview Excerpts

How is AI-driven transformation reshaping cyber risk across the Middle East as governments and enterprises accelerate digital adoption?

AI is accelerating digital transformation across the Middle East, with initiatives such as Saudi Vision 2030 and the UAE's innovation strategies driving adoption across government, critical infrastructure, and enterprise operations.



**Gopan Sivasankaran,
Regional Director,
MEA, Rapid7.**

However, Rapid7's 2026 Global Threat Landscape Report shows that threat actors are also using AI to scale reconnaissance, automate decision-making, and make phishing and social engineering attacks more convincing and

harder to detect. The UAE Cybersecurity Council has similarly warned of rising AI-driven threats, including deepfakes, advanced phishing, and automated malware. Governance will also be critical. Data privacy, model security, and

responsible AI use will become central to strategy. In this region, cyber risk is no longer just an IT issue; it is increasingly tied to digital sovereignty, making security and governance essential to sustaining digital ambition.

With identity-led attacks and AI-enabled social engineering on the rise, which threats should regional organisations prioritise in 2026?

Identity must be the top cybersecurity priority for 2026, as it has become the new control plane in modern digital environments. Compromised credentials, session hijacking, and privilege abuse remain some of the most effective attack paths, especially as organisations expand across cloud, SaaS, and hybrid infrastructure. Insider risk and third-party access also add to the challenge. While AI is increasing the speed and scale of attacks, core issues such as misconfigurations, weak access controls, and poor prioritisation still drive many breaches. Strengthening identity governance, improving visibility across access pathways, and reducing unnecessary exposure will be critical in 2026.

As attack surfaces expand across cloud, smart infrastructure, and IT/OT environments, how should CISOs shift from reactive defence to proactive risk reduction?

The expansion of cloud, SaaS, smart infrastructure, and converged IT and OT environments has dramatically increased complexity. A reactive, alert-driven approach is no longer sufficient. CISOs need to move from measuring alert volume to measuring exposure reduction. Visibility alone does not create resilience.



What matters is understanding which vulnerabilities are truly exploitable and which assets represent the highest business impact. Proactive risk reduction requires correlating live threat telemetry with validated exposure data. Instead of responding to alerts in isolation, security teams must prioritise weaknesses that adversaries are most likely to operationalise. In regions like the Middle East, where IT and OT environments increasingly intersect, preventing lateral movement across these domains is critical. A breach in IT can have real-world operational consequences. Unified visibility and prioritisation across the attack surface is essential.

What does Rapid7's expansion into the UAE signal about your long-term commitment and growth strategy in the Middle East?

Our expansion into the UAE reflects a clear long-term commitment to the region. Rapid7 has been supporting organisations across the Middle East for more than a decade, working with hundreds of customers across government, financial services, energy

and enterprise sectors. What you are seeing now is the next phase of that journey as we deepen our investment and expand our regional presence. We have strengthened our physical presence with a new office in Dubai Internet City, which serves as a regional hub for our operations. In addition, Rapid7 has achieved certification from the Dubai Electronic Security Center (DESC), allowing us to support government and regulated sectors while aligning with the UAE's cybersecurity framework.

You joined Rapid7 recently — what motivated the move, and where do you see the biggest opportunity for the company in the region?

I was motivated by the opportunity to help shape the next phase of cybersecurity in one of the world's most dynamic digital regions. Rapid7 stood out for its leadership in both exposure management and MDR, a combination that is critical to shifting security operations from reactive response to a more pre-emptive model. Many organisations across the Middle East are still managing fragmented security environments while accelerating investments in cloud, AI and digital transformation. This creates a major opportunity to simplify operations, reduce exploitable risk and strengthen resilience. For me, the role brought together strong technology, a clear market direction and the chance to drive this vision in a region moving at remarkable speed. 🚀

STRENGTHENING IDENTITY GOVERNANCE, IMPROVING VISIBILITY ACROSS ACCESS PATHWAYS, AND REDUCING UNNECESSARY EXPOSURE WILL BE CRITICAL IN 2026.

F5 AND FORCEPOINT TO SECURE ENTERPRISE AI FROM DATA CREATION TO RUNTIME OPERATIONS

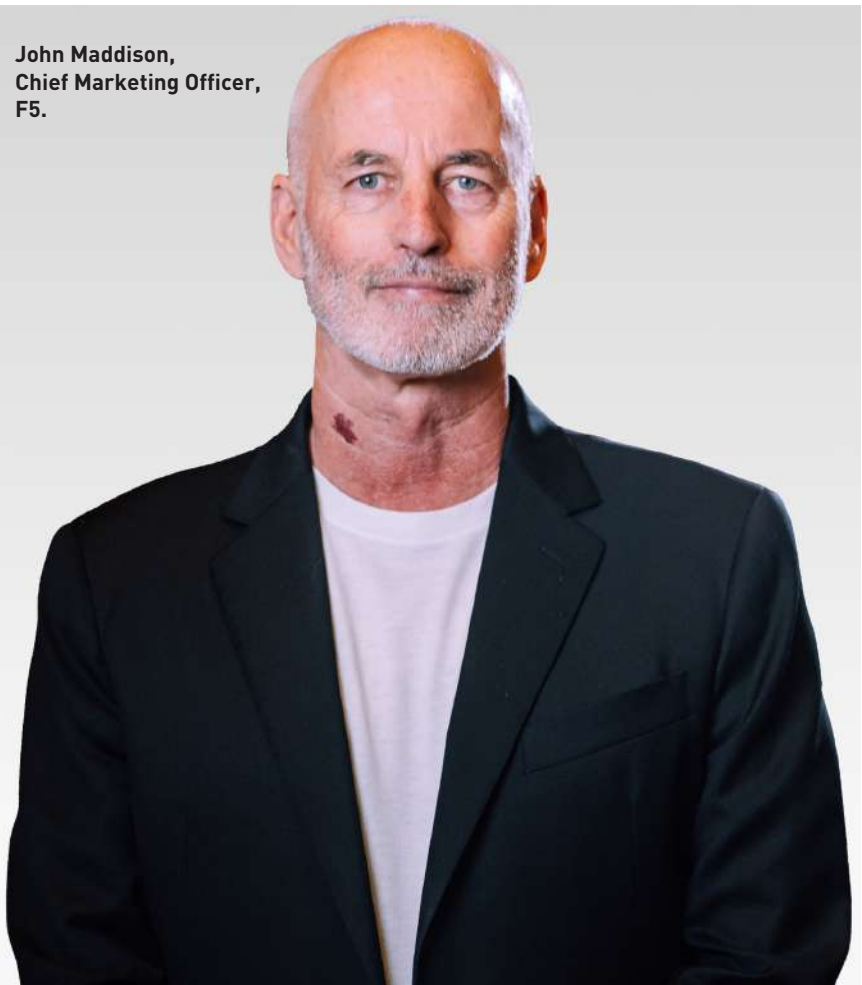
I COLLABORATION CONNECTS DATA DISCOVERY AND CLASSIFICATION WITH RUNTIME PROTECTION AND CONTINUOUS ASSURANCE TO HELP ORGANISATIONS SECURELY OPERATIONALISE AI.

F5, the global leader in delivering and securing every app and API, and Forcepoint, a global leader in data security, today announced a new alliance to help enterprises secure AI across its lifecycle—from foundational data discovery and classification through runtime protection and continuous assurance.

As organisations rapidly deploy AI across copilots, assistants, and automated workflows, security practices are struggling to keep pace. Many enterprises face complex challenges in identifying where sensitive data resides, how it flows through AI systems, and the potential risks introduced during production. While data governance, application security, and runtime protections remain crucial, they commonly operate in silos, creating gaps between security policy and AI behaviour in practice.

To solve this problem, Forcepoint's AI-native Data Security Posture Management (DSPM) data discovery and classification capabilities combine with F5's red teaming and AI guardrails functionality in the F5 Application

**John Maddison,
Chief Marketing Officer,
F5.**



Delivery and Security Platform (ADSP). This approach provides runtime protections for AI applications, APIs, models, and agents to help organisations operationalise AI safely while maintaining control and visibility over sensitive enterprise data.

The combined capabilities help security teams identify and address data vulnerabilities in real time, prioritise AI use cases based on risk, enforce runtime controls over AI interactions, and monitor systems for misuse or abnormal behavior. Continuous telemetry and policy validation provide ongoing assurance that AI systems are operating securely and in line with enterprise governance requirements.

“Enterprises are moving AI initiatives from experimentation to production faster than most security programs can adapt,” said John Maddison, Chief Marketing Officer, F5. “By combining Forcepoint’s deep data intelligence and contextual awareness with F5’s advanced application security and runtime protections, organisations eliminate operational security gaps with unmatched confidence and control in their AI operations. As AI’s threat surface continues to expand, the combined power of DSPM technologies with F5’s AI Red Team and AI Guardrails equips enterprises with proactive tools to securely scale and govern AI at every stage of its lifecycle.”

“AI has fundamentally redefined data security, exposing static policies for what they are: inadequate,” said Naveen Palavalli, Chief Product and Marketing Officer, Forcepoint. “F5 and Forcepoint are establishing a new standard of continuous, adaptive protection that follows data from the moment of creation through every stage of its lifecycle, including the runtime layer where AI systems operate, evolve, and expand risk vectors. The threats AI brings require a new category for proactive data and AI risk mitigation, and our partnership is delivering on this today.”



**Naveen Palavalli,
Chief Product and
Marketing Officer,
Forcepoint.**

Connecting data intelligence with runtime AI protection

Organisations adopting AI must determine which data should be accessible to AI systems, which use cases present the greatest risk, and how to enforce policies once AI applications are in production. The F5-Forcepoint partnership addresses these challenges by treating AI security as a continuous lifecycle, connecting data understanding with runtime enforcement.

At the foundation, Forcepoint enables organisations to discover, classify, prioritise, and govern sensitive and business-critical data across cloud, SaaS, endpoint, and enterprise data environments. This AI-powered visibility helps determine which data is appropriate for AI use and which initiatives require the highest level of scrutiny.

F5 then secures AI systems at runtime by enforcing policies across

APIs, gateways, applications, and AI agents. The F5 AI Red Team and F5 AI Guardrails functionality within F5 ADSP enables customers to secure AI models through its monitoring and adversarial testing capabilities. By leveraging the solution, customers will defend against threat actors by detecting prompt abuse, preventing data exfiltration, and protecting AI models and workloads from emerging threats.

Together, the companies enable organisations to move from data reality to runtime trust, ensuring AI systems are grounded in trusted data while continuously protected as they operate in production.

By aligning data security with application and API protection, the F5-Forcepoint partnership provides a pragmatic path for enterprises to adopt AI without rebuilding their security architecture or waiting for fully integrated platforms to mature. **i**

WHAT GULF GOVERNMENTS' PUSH FOR QUANTUM READINESS MEANS FOR PRIVATE SECTOR

I BY TAKING A NATIONAL-LEVEL APPROACH, GULF NATIONS ARE NOT SIMPLY UPGRADING CRYPTOGRAPHY, BUT ARE BUILDING THE ARCHITECTURE OF A QUANTUM-SAFE ECONOMY.

Across the Gulf, a decisive shift is taking place, one that will define the region's economic competitiveness for the next decade. In 2025, we saw Gulf governments take bold, strategic steps to prepare for a world where quantum computers can break today's encryption. The UAE's National Encryption Policy, now in development, is one of the most forward-leaning national initiatives anywhere in the world. And Bahrain's landmark agreement with SandboxAQ to deploy our cryptography and identity-management platform across more than 60 government agencies marks one of the first sovereign-level commitments to building a quantum-safe digital infrastructure.

These are not symbolic moves. They reflect a clear regional intent to establish the Gulf as one of the world's first quantum-safe economies. And the implications for the private sector are profound.

Why This, Why Now

For many years, quantum computing has existed in the realm of theoretical physics and long-term speculation. That changed this year. IBM's demonstration of the Loon chip provided the clearest engineering pathway yet to fault-tolerant quantum computers by 2029. With this, "Q-Day" (the moment at which quantum machines can break current encryption)



Mohammed Aboul-Magd,
 VP of Product, Cybersecurity
 Group, SandboxAQ.

has also shifted from an abstract concern to an imminent operational deadline. Boards can no longer treat this as a long term threat; the window is now three to four years.

And while quantum decryption may still be several development cycles away, the threat is already active. “Harvest Now, Decrypt Later” attacks are taking place today, with hostile actors stealing encrypted data in anticipation of future quantum breakthroughs. That means critical data stolen this year could be decrypted in 2029. For governments and enterprises alike, that four-year horizon is no longer distant, it is barely sufficient.

The Criticality of a Quantum-Safe Economy

One of the reasons Gulf governments are acting early is their recognition that encryption is not a technical detail. It is the foundation of national security, digital transactions, healthcare records, aviation, communications, and every critical infrastructure sector. The quantum threat strikes at the very heart of digital trust.

By taking a national-level approach, Gulf nations are not simply upgrading cryptography, but are building the architecture of a quantum-safe economy. This carries enormous advantages. Every nation will eventually have to transition to post-quantum cryptography (PQC), but those who move first enjoy outsized benefits. These would include strengthened digital sovereignty, reduced long-term remediation costs, enhanced attractiveness to foreign investors, and the ability to set the standards others follow. In this respect, the Gulf is on track to become a global reference model for quantum-safe transformation.

Government Leads, Private Sector Follows

One of the defining features of digital transformation in the Gulf is the way governments set the pace and the

COMPANIES THAT ACT NOW, WELL AHEAD OF REGULATION, WILL GAIN A CLEAR COMPETITIVE ADVANTAGE.

private sector rapidly aligns. We saw this in cloud adoption, where national cloud strategies accelerated enterprise migration. We saw it in blockchain, in the early embrace of cryptocurrency regulation, and again in the region’s rapid, coordinated mobilisation around artificial intelligence.

Post-quantum cryptography will follow the same pattern. Gulf governments are not merely signalling intent, but are putting structure, policy and timelines behind it. Drawing on global best practice, the UAE’s upcoming National Encryption Policy, is likely to include mandatory automated inventory of cryptographic assets, phased timelines for retiring vulnerable algorithms such as RSA and ECC, and requirements for crypto-agility i.e. the ability to rotate keys or change algorithms without rewriting code or disrupting operations.

These same principles will inevitably cascade into the private sector. Financial services firms, healthcare providers, telecom operators and operators of critical infrastructure will be the first to feel the regulatory impact, especially those handling government data or operating long-lived assets where “identity debt” has accumulated for years. Government contractors will likely need to produce software bills of materials proving their cryptographic hygiene.

Companies that act now, well ahead of regulation, will gain a clear competitive advantage. They will be easier to partner with, faster to certify, and better

protected against real-world threats already unfolding today.

From Compliance to Collaboration

Yet the greatest opportunity for the private sector lies not in meeting compliance deadlines but in shaping the infrastructure of a quantum-safe economy. Transitioning a nation from classical to quantum-resistant cryptography requires immense “plumbing”—scalable automation, legacy system integration, cryptographic orchestration and talent development.

This cannot be achieved by governments alone. The private sector will be instrumental in deploying the tooling, solving the last-mile integration challenges, modernising identity systems and ensuring that quantum-safe standards are deeply embedded into the region’s digital backbone.

Don’t Wait for Q-Day

The Gulf is entering a defining moment in its technological trajectory. Quantum computing is no longer a distant scientific aspiration and governments across the region have rightly signalled their intent to lead the world in quantum-safe security.

But national ambition alone is not enough. The success of a quantum-safe economy depends on the leadership of its private sector, its banks, hospitals, telcos, manufacturers, energy giants and contractors, who collectively operate the systems that keep societies moving.

For private-sector leaders, this is not merely a compliance exercise. It is a strategic inflection point. Acting now transforms cryptography from a hidden technical concern into a source of competitive advantage. It positions organisations as trusted partners to the government. It strengthens resilience against adversaries who are already collecting encrypted data. And it opens the door to deeper public-private collaboration in building the digital foundations of the region. 📌

GROWING THREAT OF IDENTITY FRAUD IN GCC: A WAKE-UP CALL FOR HR TEAMS

ORGANISATIONS ARE INCREASINGLY RELY ON DIGITAL RECRUITMENT PROCESSES AND IT IS ESSENTIAL TO CONFIRM THAT CANDIDATES ARE WHO THEY CLAIM TO BE.

HR teams and recruiters across the Gulf Cooperation Council are facing rising cases of identity fraud in the region, largely supported by the rapid evolution and increasing adoption of sophisticated AI tools according to Deloitte Middle East.

Organisations are increasingly rely on digital recruitment processes and it is essential to confirm that candidates are who they claim to be.

Identity Fraud in the GCC

Identity fraud is becoming a growing concern across the GCC, particularly as forged, stolen, or duplicated identity documents are increasingly being used to attempt to gain employment, access financial services, or to travel.

In the UAE, there have been many reported cases of fraudulent use of Emirates IDs, passports, and residency permits. In one example, between January and March 2024, 366 forgery cases involving fake passports or travel documents were identified at Dubai Airport.

Saudi Arabia has also seen

significant growth in forged ID cases, with a report by Saudi Arabia’s Digital Government Authority (DGA) warning that “the Kingdom of Saudi Arabia, and its government agencies, are facing increasingly sophisticated digital fraud-related risks.” Additionally, a recent report by IMARC Group states that the expected value of the identity verification market in Saudi Arabia will soar to around \$430 million by 2033, up from \$128 million in 2024, suggesting that concerns about identity fraud and theft are expected to grow significantly in the Kingdom in the coming years.

These figures underline how identity fraud is not just a global issue but a pressing local concern in the GCC, creating compliance, security, and reputational risks for HR teams tasked with verifying talent.

Why Identity Verification Matters

HR teams need to confirm that a candidate has the necessary skills and experience for the role and determine if they are a good fit with their company culture. While interviews, CVs, and covering letters provide some insights,

one assumption must always be verified before a job offer is made: that the person being interviewed is the same individual whose credentials have been presented.

In cases of identity theft, if the ID being presented does not belong to the candidate, the organisation risks hiring someone unsuitable for the position. This could reduce productivity, damage the brand’s reputation, or even lead to legal consequences for the business.

The Challenge of Verifying International Candidates

For companies in the GCC—many of which frequently hire international talent—understanding the various forms of government-issued ID is crucial. Beyond the typical passport or driver’s license, many countries have their own widely used forms of identification—their equivalent of an Emirates ID, Saudi National ID, or Qatari ID. The rise of generative AI has further complicated matters, making it easier for individuals to create realistic forged documents or even synthetic identities using widely available technology. With candidates applying to work in the GCC from all around the world, HR professionals that are verifying their candidates’ IDs in-house will need to be familiar with a wide range of legitimate global forms of ID and also be confident in spotting inconsistencies or potential fraud.

BY IMPLEMENTING ROBUST DIGITAL IDENTITY VERIFICATION SOLUTIONS, EMPLOYERS CAN HELP PROTECT THEIR ORGANISATIONS



James Randall,
Sales Director, Middle East, HireRight.

Remote Hiring and the Risks Involved


With remote work becoming increasingly common in the GCC, verifying a candidate's identity without physical presence can be another challenge. Asking candidates to send physical IDs via tracked delivery is an option, but it comes with risks of loss or theft, particularly for international hires. Alternatively, digital scans or photographs are often requested, but these too can be manipulated, for example by replacing the original photo with the candidate's own. Even video calls, once considered a secure way to

validate identity, can be undermined by AI-generated masks or screens.

Identity Verification

A company's HR team cannot reasonably be expected to have an encyclopaedic knowledge of international identity documents. Nor would they be likely to have the expertise needed to confidently identify forged or fraudulent versions of the myriad types of ID that their global candidates may present during the background screening process. Conducting identity verification in-house can also be time-consuming and

stressful, with the risk of errors and potential exposure to fraud being major concerns for many businesses.

As identity fraud continues to grow across the GCC, HR teams must adapt to address increasingly complex threats. To combat this ever-evolving risk, many businesses are relying on advanced digital verification technologies to strengthen their operations. By implementing robust digital identity verification solutions, employers can help protect their organisations, maintain candidate trust, and make more confident hiring decisions in a digital-first, high-risk environment. 

THE DATA SOVEREIGNTY GAP IN MIDDLE EAST

TWO-THIRDS OF ORGANISATIONS SPEND OVER \$1 MILLION ANNUALLY ON SOVEREIGNTY COMPLIANCE. THE INCIDENT RATE IS 44%. FOR CHANNEL PARTNERS, THE GAP BETWEEN INVESTMENT AND ENFORCEMENT ARCHITECTURE IS THE MOST URGENT — AND MOST VALUABLE — CONVERSATION IN THE GCC RIGHT NOW.

Here's the paradox that should define every channel conversation in the Middle East this year. The Kiteworks 2026 Data Sovereignty Report found that 93% of Middle Eastern respondents say PDPL and SDAIA regulations directly impact their operations. Awareness is strong: 44% describe themselves as "very well informed." And two-thirds spend more than \$1 million annually on sovereignty compliance, with 28% exceeding \$5 million. And yet 44% experienced a sovereignty-related incident in the past 12 months, well above Europe's 32%. The region that's moving fastest on sovereignty is getting hit the hardest. That's not a knowledge problem. It's an architecture problem. And architecture problems are channel problems.

Why speed alone isn't enough

Three factors converge to explain the gap. First, PDPL and SDAIA are relatively new frameworks. Organisations understand the rules but haven't fully built the enforcement infrastructure around them. Second, 30% of Middle Eastern respondents work at organisations with 10,000 to 19,999 employees, creating large attack surfaces and complex compliance footprints. Third, 33% cite geopolitical

instability as a top concern, introducing a risk layer that is structurally different from anything in Canada or Europe. The incident profile tells the story. Regulatory investigations lead at 22% meaning regulators are actively probing. Data breaches with sovereignty

implications hit 20%. Third-party compliance failures reach 19%. And 15% report government data access requests. These aren't theoretical risks. They're operational disruptions happening right now, at scale, to organisations that are spending millions to prevent them.



David Byrnes,
VP of Global Channels,
Kiteworks.

The channel opportunity is architectural

Here's the reality I see across our partner ecosystem in the region: Middle Eastern organisations are not short on budget or intent. They're short on the operational infrastructure that turns policy into enforceable control. That's the gap the channel exists to fill.

Technical infrastructure changes are the number one resource drain, cited by 59% of respondents. Legal and compliance expertise follows at 52%. Cross-border transfer assessments (at 41%) are the highest of any region, reflecting the complexity of managing data flows across the GCC's multi-jurisdictional operating environment. These are services-intensive, advisory-rich requirements. They are, by definition, partner territory.

The organisations that need the most help are the ones building new infrastructure rather than retrofitting legacy systems. That's a fundamentally different engagement from the European market, where partners are layering sovereignty onto mature IT estates. In the Middle East, partners have the opportunity to build sovereignty in from the start, and that's a far more valuable, far more sticky engagement.

What provable sovereignty requires

The shift is from stated compliance to sovereignty you can prove. In a region where regulators are actively investigating the ability to produce evidence on demand is not a differentiator. It's a survival requirement. Three architectural capabilities separate the organisations that avoid incidents from those that become the statistic.

Data residency enforced at the infrastructure level. Not a vendor promise, but a technical control ensuring sensitive content stays within the region. Deployment options that keep data exclusively on Middle

Eastern infrastructure, with geofencing enforced through configurable IP controls, are the baseline.

Encryption key custody retained in-jurisdiction. If the provider retains the ability to decrypt customer data, even under legal compulsion from a foreign government, sovereignty is decorative. Sole key ownership within the customer's environment makes foreign access requests a cryptographic impossibility, not a legal negotiation.

Exportable evidence that proves it all. Immutable audit trails, data residency logs, and compliance documentation that satisfy PDPL, SDAIA, and enterprise customer requirements on demand. 46% of Middle Eastern organisations plan to invest in compliance automation over the next two years. Forty-eight percent plan enhanced technical controls. That's budgeted demand looking for the right partner.

AI Governance Is the Next Battleground

The Middle East's AI governance posture is distinctive and it's where channel partners can establish early authority. 39% of respondents keep all AI training data within the region, and another 39% use a mixed approach based on data sensitivity. Safeguard adoption is strong: regular AI audits lead, followed by impact assessments for high-risk AI, consent management, and transparency documentation.

Unlike Europe's top-down AI Act, the Middle East is building AI governance through SDAIA oversight and active regulatory engagement. The organisations that get the balance right of enabling cross-border collaboration where permitted while maintaining provable control where required will set the standard for the GCC. Channel partners who can help operationalise that balance own the advisory relationship.

Sovereignty is already a trust

accelerator

The Middle East's 56% customer trust score was the highest in the entire survey. In a region where organisations are actively building credibility with regulators, partners, and customers under new frameworks, sovereignty compliance is functioning as a trust signal, not just a legal obligation. 69% cite improved security posture. 35% identify competitive advantage. 15% cite geopolitical protection.

For channel partners, this reframes the commercial conversation entirely. You're not selling a compliance cost. You're selling trust, market access, and competitive positioning in a region where demonstrable sovereignty is becoming a procurement prerequisite.

The conversation to start having

The Middle East doesn't lack awareness, budget, or regulatory motivation. What it lacks is the operational depth to close the gap between what organisations know they should do and what their architecture actually enforces. That gap is 44 percentage points wide, measured in incidents.

The partners winning this market aren't leading with product. They're leading with the question: "You're spending millions on sovereignty. Can you prove it's working?" That question opens an engagement that spans assessment, architecture design, deployment, compliance automation, and ongoing managed sovereignty. Recurring revenue built on a region that's building its digital infrastructure from the ground up and doing it under the most intensive regulatory scrutiny of any market in this survey.

The opportunity is enormous. But only for partners who understand that the Middle East's sovereignty problem isn't awareness. It's the distance between policy and architecture. Close that gap, and you own the most consequential technology conversation in the GCC. 🔑

ENSURING CONTINUITY REMAINS CRITICAL AMID DATA SOVEREIGNTY CHALLENGES

BALANCING BUSINESS CONTINUITY, CLOUD RESILIENCE, AND STRICT DATA-LOCALISATION MANDATES IN THE UAE AND WIDER GCC.

Recent events have shown that even the largest cloud data centers can fail. Recently, a major cloud region in the UAE suffered a serious incident that took down several Availability Zones. Service providers advised customers to activate their disaster recovery plans and fail over to other regions. At the same time, businesses in the UAE and the Gulf are bound by strict data sovereignty rules—many kinds of data must stay onshore by law. This creates a dilemma: How can companies keep running their applications when the local cloud goes dark, without violating localisation mandates?

Modern data-governance platforms can automatically map what data you have, who it belongs to, and where it lives, enabling tailored continuity plans. Finally, we outline practical resilience strategies (multi-site, multi-cloud, hybrid models) that align with these legal constraints.

The goal is an original, actionable roadmap for CIOs: use smart data intelligence and robust architecture so that even if a hyperscaler region fails

again, your key services keep running and your data stays compliant.

Recent Cloud Region Outages

Cloud outages necessitate robust resilience. The recent major physical event in the UAE/Gulf Region caused core services to be unavailable for hours, impacting UAE financial/government systems and prompting clients to restore backups or shift sites. The lesson: design for region-level outages, not just rack failures. A prior internal network/DNS failure in October 2025 in the US East Region left hundreds of global websites/apps inaccessible and blocked enterprise access to key databases/services. This demonstrates that a single-region failure can cascade globally, necessitating geographically distributed workloads or multi-cloud strategies.

UAE and GCC data-localisation laws impose strict rules on where certain data can be stored and processed. The UAE Federal PDPL (2021) regulates cross-border transfers and will soon require Transfer Impact Assessments for high-risk flows, while Central Bank regulations mandate that financial institutions keep all customer and transaction data within

the UAE. Free zones such as DIFC and ADGM allow international transfers with safeguards, but require strict compliance and oversight. In addition, telecom, government, healthcare, and critical infrastructure data are typically required to remain onshore, with regulators enforcing residency through licensing and audits. Across the GCC, similar privacy laws exist, but organisations operating in the region generally treat sensitive citizen, financial, and health data as UAE-only, while limited exports are allowed for anonymised or non-regulated datasets under strict controls.

Classifying and Tagging Cloud Data

The foundation of sovereign resilience is knowing your data. Organisations must conduct a full audit of their cloud footprint. Modern data-governance tools automate this by scanning databases, file shares, SaaS platforms, and messaging systems to locate sensitive information and apply metadata tags linking data to identities, country of origin, and classification (public, confidential, regulated).

Experts stress that effective data sovereignty requires mapping digital assets and data flows, classifying risk levels, and geo-tagging data. Automated discovery tools can identify sensitive records—such as UAE citizen data—and flag them as non-exportable, even alerting teams if restricted information appears in unauthorised storage locations.

USE SMART DATA INTELLIGENCE AND ROBUST ARCHITECTURE SO THAT EVEN IF A HYPERSCALER REGION FAILS AGAIN, YOUR KEY SERVICES KEEP RUNNING AND YOUR DATA STAYS COMPLIANT.

Tahir Latif,
Global Data Privacy & AI Governance
Advisor.



The “privacy engines” provide a live view of who owns the data, where it resides, and how it can move. Policy-driven metadata ensures high-sensitivity data never leaves approved jurisdictions, while automated controls block or quarantine backups that attempt to export restricted datasets.

In essence, organisations must continuously discover, classify, and tag cloud data using AI-driven data-intelligence tools. This creates a clear compliance map, enabling business-continuity teams to determine what data can move and what must remain local.

Architecting Sovereign Resilience

Once data is classified, organisations should deploy layered continuity architectures:

- **Multi-Availability Zone High Availability:** Run critical applications across all datacentres within the local cloud region. While this won’t survive a full regional outage, it protects against common failures and enables seconds-to-minutes recovery.
- **Alternate Region Disaster Recovery:** For exportable data, replicate services to a secondary region where legally permitted. Automated failover can redirect traffic quickly, but only compliant or anonymised data should be replicated.
- **Multi-Cloud Strategy:** Distribute workloads across two cloud providers with local presence to reduce dependency on a single vendor and improve resilience during regional outages.
- **Hybrid Pilot-Light Setup:** Maintain a minimal on-premises or local colocation DR environment within the UAE for critical systems. This provides strong sovereignty control but is typically used only for Tier-1 workloads.
- **Immutable Local Backups:** Always store encrypted backups within the country. Even if recovery takes longer, this guarantees a sovereign fallback and satisfies regulatory requirements.

For all designs, automation and testing are crucial. Use Infrastructure-as-Code (IaC) so you can spin up the alternate environment with a click. Lower DNS TTLs for faster cutover. Practice DR drills where you actually simulate the region-down event and confirm recovery steps.

Coverage of a past outage emphasises that companies must actually fail over during a test, not just hope failover will work. Teams should also be ready to operate in a broken-cloud scenario (for example, having a manual plan to operate core databases if automated failover hangs).

Actionable Recommendations

- **Adopt a Data-Intelligence Platform:** Use a governance tool to automatically discover sensitive data, map identities and locations, and tag datasets that must remain in the UAE.
- **Enforce Policy-as-Code:** Link data tags to automated controls so restricted data cannot be transferred outside approved regions.
- **Create Tiered DR Playbooks:** Define RTO/RPO targets and clear failover procedures for each data category.
- **Strengthen Contracts & Compliance:** Ensure cloud agreements specify data location and integrate DR requirements into governance policies.
- **Train and Test:** Run regular drills and outage simulations to validate failover processes.

ORGANISATIONS MUST CONTINUOUSLY DISCOVER, CLASSIFY, AND TAG CLOUD DATA USING AI-DRIVEN DATA-INTELLIGENCE TOOLS.

- **Use Monitoring Dashboards:** Track where sensitive data resides in real time for faster incident response.
- **Coordinate with Partners:** Align local cloud and colocation partners with your DR and monitoring frameworks.

Checklist for CISOs/BC Leads

- **Inventory Cloud Data:** Run discovery tools to catalog all data, applications, and users in the cloud.
- **Classify by Localisation:** Tag each dataset by its residency requirement (e.g. “UAE-only”, “GCC-only”, “Global”, or “Unrestricted”).
- **Map DR Scenarios:** For each critical system, outline failover procedures for both local-only data and unrestricted data.
- **Prepare Alternate Sites:** Provision backup environments (cloud regions, on-prem, multi-cloud) in compliance with legal limits for each data tier.
- **Automate and Test:** Develop IaC scripts and automation for failover steps; schedule regular DR drills and audits of the process.
- **Review Legal Requirements:** Ensure your data flow design abides by UAE laws (e.g. financial data kept local). Update privacy and continuity policies accordingly.
- **Continuous Monitoring:** Use real-time analytics to monitor data locations and automatic alerts for any policy violations.

The UAE’s recent cloud outage should act as a wake-up call for resilience, not panic. It highlights the need to design continuity into systems, especially when regulations require certain data to remain within the country.

Organisations must combine strong data governance with multi-location architectures, ensuring every dataset is classified, policies are automated, and failover systems are regularly tested. When these measures are in place, businesses can maintain operations even during major outages while keeping sovereign data secure. As one regional CIO noted, business continuity is no longer a document on a shelf—it is a live operational discipline. 🔑

GITEX **AI**
EUROPE
Berlin 2026

30 JUNE
01 JULY
— MESSE BERLIN —

A BOLDER DIGITAL EUROPE IS OPEN.
CHOOSE EUROPE.

Forging an Open, Bold
& Collaborative European
Digital Economy

1,400+

Enterprises &
Startups

100+

Participating
Countries

600+

Global
Investors

200+

Global Speakers

25,000+

Tech Executives

— ENDORSED BY —



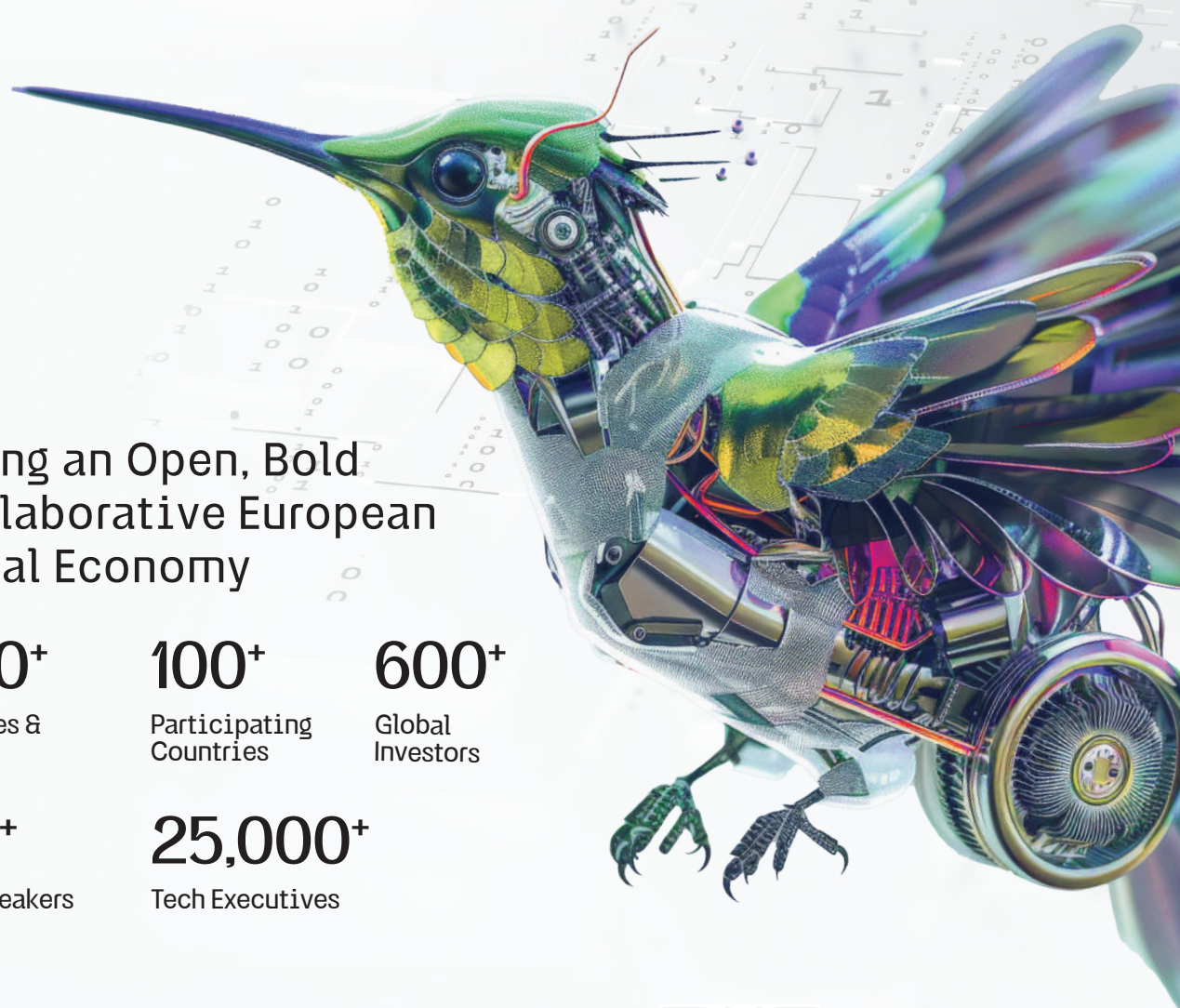
— ORGANISED BY —

KAOUN
INTERNATIONAL



SCAN TO
GET INVOLVED

#GITEXEUROPE
gitexeurope.com



HEIGHTENED CYBER RISK DURING MIDDLE EAST ESCALATION: AN ICS PERSPECTIVE FOR SECURITY LEADERS

I WITH GEOPOLITICAL TENSIONS RAISING CYBER RISK ACROSS THE MIDDLE EAST, CISOS OVERSEEING INDUSTRIAL ENVIRONMENTS MUST PRIORITISE PREPAREDNESS, RESILIENCE, AND DISCIPLINED OPERATIONAL DEFENCE.

As geopolitical tensions intensify, so does cyber risk. Both kinetic and cyber operations are integral to military strategy, and retaliatory cyber actions threaten military and civilian infrastructure. For CISOs overseeing industrial operations, a critical question arises: are we a target, and are we truly prepared?

Asset owners do not determine their status as targets; this is influenced by external factors, whether at war or in peace. CISOs can only control their level of preparation and system resilience.

This begins by maintaining continuous awareness, leveraging OT-focused threat intelligence to shape defenses for their specific sector and systems. Integrating intelligence and lessons from known OT attacks effectively guides security programs.

Recent events in the Middle East have heightened concerns among asset owners and operators. A recent CPX analysis report indicates these crises drive increased hacktivist campaigns, opportunistic breaches, and influence operations against regional organisations.

From an industrial control system (ICS) perspective, however, the situation remains measured. At the time of writing, there are no publicly disclosed cyber operations performing a stage 2 attack, or one that has directly impacted ICS environments. However, this could change at any moment.

This distinction is crucial for security leaders. Disruptive cyber operations targeting industrial environments require extensive planning, access development, and process expertise. Historically, such operations take significant time to mature, but the clock is ticking.

The initial phases of geopolitical cyber escalation almost always involve swift reconnaissance, persistent intrusion attempts, and clear warning signals rather than delayed disruption of industrial systems. Threat actors work urgently to gain footholds in enterprise networks before moving to operational environments.

DISRUPTIVE CYBER OPERATIONS TARGETING INDUSTRIAL ENVIRONMENTS REQUIRE EXTENSIVE PLANNING, ACCESS DEVELOPMENT, AND PROCESS EXPERTISE.

Recent activity aligns with this pattern. Dragos researchers have observed increased operations by MuddyWater, a group linked to Iranian cyber operations. Targeted sectors include aviation, government, healthcare, energy-supporting engineering services, and maritime domains.

Observed tactics mirror typical intrusion campaigns: exploiting known vulnerabilities, harvesting credentials, and abusing legitimate remote management tools. While these activities confirm ongoing interest in industrial control systems (ICS) environments, current evidence does not show successful attempts to manipulate industrial processes.

Geopolitical crises often lead to increased hacktivist messaging and cyberattack claims. These claims frequently exaggerate or fabricate operational impacts to create psychological pressure or signal symbolic retaliation.

A recent example was a claim by the hacktivist persona APT IRAN, linked to the Dragos tracked group BAUXITE, alleging a cyberattack against a Jordanian government-run wheat storage facility. The claim described the manipulation of environmental controls within grain storage systems. However, Jordanian authorities later confirmed the attempted attack was thwarted, and no evidence confirms an industrial control system compromise.

This pattern is common during geopolitical conflicts. Hacktivist groups often claim to have carried out ICS attacks that never occurred. These narratives underscore that critical infrastructure organisations are highly visible targets, and cyber messaging is used to amplify political pressure. They are not directly targeted, but geopolitical events can still produce operational disruption. Recent regional reporting has referenced sustained GPS and GNSS interference affecting maritime traffic across the Arabian Gulf and Red Sea.

This is not industrial control system



Mike Hoffman,
Field CTO and Certified Instructor,
SANS Institute.

manipulation, but it underscores growing operational dependencies. Many industrial operations depend on external services like satellite navigation, telecommunications, and cloud-connected systems. Disruptions can erode situational awareness, logistics, and operational safety.

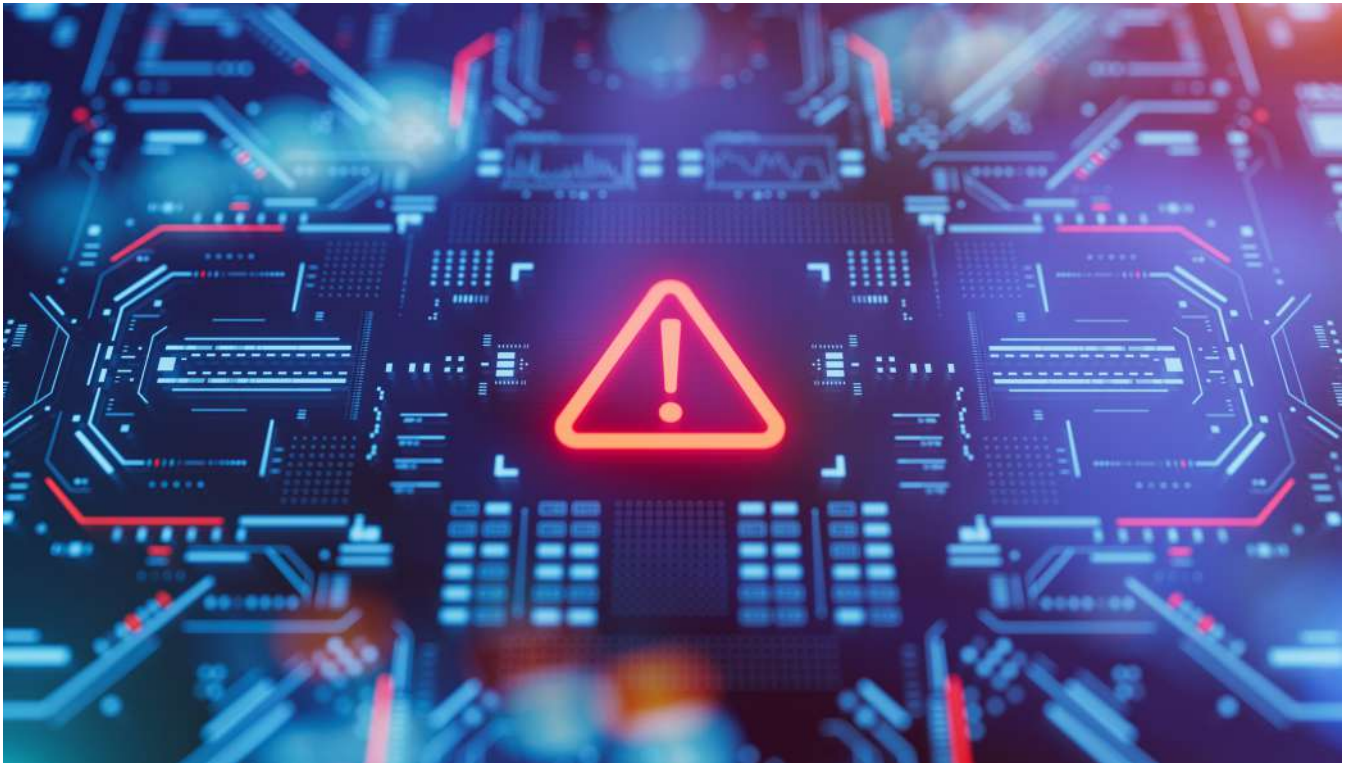
Key takeaways for CISOs and security leaders during geopolitical tension: focus on disciplined risk management and operational readiness. Do not react out of alarm, but adopt proven controls to maximise defense effectiveness.

ICS-Specific Incident Response Plan

Organisations should maintain an incident response capability tailored to industrial environments. Unlike traditional IT plans, ICS response must prioritise safe operations, process stability, and system integrity.

CISOs should ensure cybersecurity teams, engineers, and operations leadership can coordinate effectively during incidents. Regular tabletop exercises and scenario planning align the organisation, from executives to plant operations, around known, realistic cyber incident scenarios.

Defensible Architecture



A defensible architecture lowers risk by design and supports effective monitoring and response. In industrial contexts, this means segmenting enterprise and OT networks, implementing industrial DMZs, and strictly controlling communication between zones of trust within OT networks.

The goal is not a perfectly secure network, but one that limits attacker movement, supports containment actions, and provides a foundation for network visibility into critical operational systems.

ICS Network Visibility and Monitoring

Industrial environments require visibility into system communications to detect behavior that may indicate malicious activity.

Unlike traditional IT monitoring, ICS monitoring focuses on ICS protocols and operational interactions. This capability is essential for detecting threats before they escalate into operational disruption. Host and network monitoring should have a direct tie back to intelligence. Intelligence tracks known adversaries, and network detection tooling should

leverage intelligence to produce low-noise, high-fidelity, and actionable detections that operations and SOC analysis can respond to.

Secure Remote Access

Remote connectivity is essential for many industrial operations, but also presents a significant attack vector. Adversaries increasingly target remote access used by employees, vendors, and service providers.

Security leaders must identify, strictly control, and monitor all remote access routes. Strong authentication, limited entry points, and watched jump hosts reduce the risk of unauthorised network access, but this is only the beginning.

Risk-Based Vulnerability Management

In industrial environments, patching every vulnerability immediately is often unrealistic due to operational and safety constraints. Organisations should focus on vulnerabilities that pose significant operational risk. The 2026 Draogs OT Cybersecurity Year in Review report indicated that 3 percent of reported OT vulnerabilities were labeled as “Now”

and required immediate action, proving that vulnerability mitigation in OT is achievable.

A risk-based approach targets vulnerabilities that permit access to operational environments or manipulation of vital systems. Often, segmentation or enhanced monitoring outperforms immediate patching as a mitigation strategy.

CISOs should treat the current situation as a time for vigilance, not panic. Use this period to assess preventative, detective, and recovery controls.

Remember, destructive industrial cyber operations demand time and meticulous planning. Organisations equipped with strong visibility, enforced boundaries, and recovery readiness create formidable barriers to adversaries.

In summary, the primary takeaway for security leaders is that preparedness before a crisis is essential for resilience during escalating geopolitical threats. Maintain strong visibility, robust boundaries, and readiness to respond; these are the key tenets for effective ICS security. 🔑



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

WHY OT SECURITY HINGES ON A STRONG IDENTITY-MANAGEMENT STRATEGY

The UAE's push towards "We the UAE 2031" will place Operation 300bn firmly at the centre of its industrial growth agenda. This shift also requires security professionals in heavy industrial sectors to confront the inherent risks emerging from the modernisation of Industrial Control Systems (ICS).

To make smart factories and smart plants work, enterprises have merged OT with IT, exposing critical infrastructure to the same connected threat landscape that has plagued more IT-centric sectors. Problems arise because, for such environments to function, machines must be given identities. CISOs across the region have been aware for some time that identities are the new perimeter. According to a May 2025 report from e&'s security arm, Help AG, 45% of cyber-incidents in the UAE involve the compromise of credentials.

As more of the UAE's OT surface becomes exposed, security teams must address the issue of credential sprawl in legacy ICS in ecosystems. Old setups are set up to fail when simple misconfigurations and over-credentialling leave paths to privilege, and consequently success, for adversaries. A new approach to risk management is needed to deal with the difficulties in remediation that are frequently found in heavy industry's always-on environments.

Purdue models, with their iDMZ firewalling and air-gap precautions, do not, on their own, meet the agility requirements of modern businesses when it comes to remote management,

vendor access, and IT integration for systems like DNS and IAM (identity access management). OT security must embrace human and machine identities, the latter of which include AI. To prevent credentials thieves logging in at will, we must look at a futureproof, identity-centric approach to OT security.

OT identity security principles

For this, we turn to Privileged Access Management (PAM), which goes beyond mere account management to the control, monitoring, and auditing of every authentication transaction. Identities of all seniorities and types are placed under 24-7 surveillance for a modern, secure-by-design OT environment that is no longer isolated from the corporate identity estate. This gives security professionals more options for managing OT identity risk. Everything improves – operations, IT, OT, security, compliance – when tackling the risks that identities pose in an ICS-rich business.

Visibility

Every identity – human, machine, and AI – must be cataloged and categorised. Humans include internal employees and external suppliers or partners. The survey must also discover all service accounts, SSH keys, device credentials, and machine-to-machine secrets. Any entity that is given access to any area, sensitive or otherwise, of the IT or OT network, must be subject to scrutiny. There are tools for discovery and visibility that offer operability across IT and OT. These are essential, because any overlooked identity has the potential to

become an attacker's beachhead.

Just enough access

The principle of least privilege gives only those rights needed for a human or machine entity to perform a designated task. Just-in-time (JIT) access bestows these rights for a limited time-window; when the window expires, so do the rights. These practices must be applied to employees, vendors, and the full range of M2M interactions. By narrowing windows of exposure, we choke off opportunities for would-be attackers. The principle of least privilege cuts down the number of paths open to them, and JIT access gives them shortened periods in which to elevate their entitlements.

No more legacy remote access

Security teams must enforce identity-secure remote access. VPNs, remote-desktop, and static vendor access are risky legacies. When moving to a modern OT environment, we must treat all remote sessions as we would any other – as privileged access, subject to standard controls and monitoring. Implement measures such as MFA and watch for behavioral anomalies such as anomalous log-in times.

Network segmentation

Even if the organisation follows all security best practices, perfect identity hygiene may remain evasive. OT solutions that leverage the Purdue model can limit cross-system layered access while isolating vendor sessions. The purpose is to prevent lateral movement and DOS attacks, so architecture must be

designed for micro-segmentation and if necessary, granular controls applied even to the level of individual workloads.

Never stop surveilling

Round-the-clock monitoring is essential. Frequent auditing will allow the business to assess its identity risk. Unfortunately, there is no patch for identity vulnerability. Without constant vigilance, dormant accounts can arise from offboarded employees or expired vendor contracts. Continuous discovery and entitlement analysis will make for a more mature risk posture.

A secure supply chain

Identity-centric PAM is the backbone of modern OT security and yields measurable returns on investment. Businesses reduce risk by eliminating previously unseen pathways to privilege. This is because, under such conditions, a compromised identity has a limited blast radius – a comforting notion for those tasked with protecting critical infrastructure.


As for business continuity, OT environments' high-availability, safety-critical systems are better protected by identity-centric PAM, from nefarious access, so uptime is maximised and the probability of catastrophic failure and subsequent financial loss is vastly reduced. All these measures put the organisation on a strong compliance footing, having put in place robust identity controls and auditable access models.

It is time for the nation's enterprises to move away from OT security as a reactive, patching exercise. Identity now vies for the number-one spot in attack-vector preferences. The way forward is a relentless pursuit of PAM maturity – a journey every OT-centric enterprise must take to face the current threat landscape. A mature identity posture comes through migration from "patch-and-protect" to a proactive, zero-trust culture that allows the organisation to take part in the lucrative future promised by Operation 300bn and "We the UAE 2031". 🧑



Layale Hachem,
Principal Solutions Engineer,
BeyondTrust.

Matthew Prince,
co-founder and CEO, Cloudflare.



**WE'VE BUILT THE LARGEST AND MOST
COMPREHENSIVE GLOBAL SENSOR NETWORK
→ THAT GIVES US A FRONT-ROW SEAT TO THREATS
INVISIBLE TO EVERYONE ELSE.**

NATION-STATE ACTORS AND CYBERCRIMINALS SHIFT FROM 'BREAKING IN' TO 'LOGGING IN', SAYS CLOUDFLARE

NEW INSIGHTS DEMONSTRATE THAT THE BARRIER TO ENTRY FOR SOPHISTICATED CYBERCRIME HAS COLLAPSED.

Cloudflare, Inc., the leading connectivity cloud company, recently published its inaugural 2026 Cloudflare Threat Report reveals that threat actors are using DDoS attacks of unprecedented scale, leveraging AI systems to exploit vulnerabilities, and continuing to strike at traditional weak spots like email to find ways to “log in” versus “break in.”

This report draws on the expertise of the Cloudforce One threat research team and the scale of Cloudflare’s global network to spotlight a fundamental rewiring of the modern cyberattack.

The 2026 report arms security teams against emerging threats, detailing the tactics and trends behind the 230 billion threats Cloudflare blocks on average each day. With AI making it easier for anyone to launch sophisticated attacks, threat actors are moving faster than ever, crashing websites, infiltrating payroll systems and tricking software into trusting them. Security is no longer about keeping strangers out; it’s about proving that the users inside your network are who they say they are.

“Hackers thrive on the gaps left by fragmented, stale threat intelligence. At Cloudflare, we’ve built the largest and most comprehensive global sensor network that gives us a front-row seat to threats invisible to everyone else,” said Matthew Prince, co-founder and CEO of Cloudflare.

“By sharing this intelligence with

the world, we’re plugging the gaps and shifting the advantage back to the defenders. The result is a safer, more reliable Internet, where it is fundamentally more difficult and expensive for hackers to operate.”

Over the past year, Cloudforce One has analysed trillions of network signals and threat actor tactics, techniques, and procedures (TTPs) to uncover the most common attack vectors, nation-state espionage tactics, and the real-world impact of AI on cyberattacks.

Key findings include:

- **AI Erases the Technical Barrier to Entry to Launch Attacks:** Threat actors are using Large Language Models (LLMs) to map networks in real-time, develop new exploits, and create hyper-realistic deepfakes. Cloudforce One tracked a threat actor who leveraged AI to help identify the location of high-value data. This allowed the actor to compromise hundreds of corporate tenants — high-volume SaaS applications that allow multiple organisations to share resources — in one of the most impactful supply chain attacks seen.
- **Chinese Threat Actors Trade Broad Attacks for Precision Strikes:** State-sponsored actors, specifically Salt Typhoon and Linen Typhoon, have shifted focus toward North American telecommunications, government entities, and IT services. These actors are shifting from traditional

espionage to persistent pre-positioning — the act of installing code on the network or system of a rival state to allow for future attacks — within U.S. critical infrastructure.

- **Corporate Identities are Being Hijacked:** North Korean operatives are using AI-generated deepfakes and fraudulent IDs to bypass hiring filters, embedding state-sponsored workers directly into Western corporate payrolls. Using U.S.-based “laptop farms,” these threat actors are masking their true location.
- **DDoS Attacks Surpass Human Response Capabilities:** Large-scale botnets like Aisuru have evolved into nation-state level threats capable of taking down entire country’s networks. With record-breaking attacks reaching 31.4 Tbps, these high-speed strikes now demand fully autonomous defenses.

“Threat actors are constantly changing tactics, finding new vulnerabilities to exploit and ways to overwhelm their victims. To avoid being caught off guard, organisations must shift from a reactive posture to one fuelled by real-time, actionable intelligence,” said Blake Darché, head of threat intelligence, Cloudforce One at Cloudflare. “This report is a North Star for understanding the scale of attacks, and how threat actor aggression and techniques are shifting. The message to defenders is simple: lead with intelligence or risk falling behind in a race where the stakes have never been higher.”



HPE THREAT LABS REVEAL CYBER ADVERSARIES MORPH BUSINESS MODEL TO SCALE AND ACCELERATE ATTACKS

ORGANISATIONS ARE INCREASINGLY RELY ON DIGITAL RECRUITMENT PROCESSES AND IT IS ESSENTIAL TO CONFIRM THAT CANDIDATES ARE WHO THEY CLAIM TO BE.

HPE unveiled the results of its inaugural cyberthreat research report, *In the Wild*, showing a striking shift in how modern cyber adversaries operate at scale across global industries and critical public sectors. Based on HPE's analysis of live threat activity observed globally throughout 2025, the report shows that cybercrime has gone industrial, with attackers using automation and long-standing vulnerabilities to scale campaigns and repeatedly compromise high-value targets faster than defenders

can respond. For enterprises, the ability to overcome these aggressive threat campaigns effectively and retain digital trust within their networks is a fundamental business priority.

The report shows a global cyber threat environment defined by scale, organisation and speed. Based on the cyber analysis of 1,186 active threat campaigns observed worldwide between January 1 and December 31, 2025, the findings reveal a rapidly evolving adversary ecosystem defined by professionalism, automation and strategic targeting, with attackers using

repeatable infrastructure and long-standing vulnerabilities to target high-value sectors with precision.

"*In the Wild* reflects the reality organisations face every day," said Mounir Hahad, Head of HPE Threat Labs, HPE. "Our research is grounded in real-world threat activity, not theoretical tests in controlled lab scenarios. It captures how attackers behave in active campaigns, how they adapt, and where they are finding success. These first-hand observations and insights help sharpen detection, strengthen defenses, and give customers a clearer view of the threats most likely

to impact their data, infrastructure, and operations. That means stronger security, faster response, and greater resilience in the face of increasingly organised and persistent attacks.”

Industrial-scale infrastructure fuels modern threat campaigns

As this inaugural report shows, HPE Threat Labs observed an increase in both the volume of attacks and the sophistication of adversary tactics and techniques. Threat actors, including nation-state-linked espionage groups and organised cybercrime operations, increasingly ran their operations like large enterprises, using hierarchical command structures, specialised teams, rapid coordination to deploy expansive and industrialised attack infrastructures, and a deep understanding of commonly used workforce applications and documents.

Government organisations were the most targeted sector globally, accounting for 274 campaigns spanning federal, state and municipal bodies. The finance and technology sectors followed closely, with 211 and 179 campaigns, respectively, reflecting attackers’ sustained focus on high-value data and financial gain. Defense, manufacturing, telecommunications, healthcare and education organisations were also heavily targeted. Together, these findings underscore that attackers are strategically prioritising sectors tied to national infrastructure, sensitive data and economic stability, but reinforce that no sector is immune.

Over the course of the year, threat actors deployed more than 147,000 malicious domains, nearly 58,000 malware files, and actively exploited 549 vulnerabilities. This professionalisation of cybercrime makes attacks more predictable in execution, yet harder to disrupt, as dismantling one component of an operation rarely stops the broader campaign.

Automation and AI tools accelerate attacker speed and impact

Attackers also adopted new techniques

- Cyber adversaries adopt business-like models to target every major sector, HPE finds
- Generative AI used to produce synthetic voices, images and videos for targeted impersonation fraud campaigns
- World-class network threat research expertise and experience brought together in new HPE Threat Labs

to increase speed and impact. Some operations used automated “assembly line” workflows over platforms like Telegram to exfiltrate stolen data in real time. Others leveraged generative AI to produce synthetic voices and deepfake videos for targeted video-phishing (vishing) and executive impersonation fraud, while an extortion gang did market research on virtual private network (VPN) vulnerabilities to optimise its intrusion strategy.

These tactics allowed threat actors to move faster, reach more targets and concentrate efforts on sectors tied to national infrastructure, critical data and economic stability. By streamlining operations and prioritising high-value targets, threat actors were able to pursue financial gain with greater efficiency by strategically “following the money.”

Practical steps to strengthen cyber resilience

The report underscores that effective defense depends less on adding tools and more on improving coordination, visibility, and response across the network.

Organisations can take the following steps to improve their security posture:

Break down silos by sharing threat intelligence across corporate teams, customers, and industries, while using a secure access service edge (SASE) approach to unify networking and security and surface attack patterns earlier.

Patch common entry points such as VPNs, SharePoint, and edge devices to reduce exposure and shut down

frequently exploited paths into the network.

Apply zero trust principles to strengthen authentication and limit lateral movement, with zero trust network access (ZTNA) continuously verifying users and devices before granting access.

Improve visibility and response with threat intelligence, deception technologies, and AI-native detection, helping organisations detect, analyse, and respond to attacks with greater speed and accuracy.

Extend security beyond the corporate perimeter to home networks, third-party tools, and supply chain environments.

Together, these steps can help organisations move faster, reduce risk, and better defend against increasingly organised and persistent threats.

Combined HPE Threat Labs raises the bar for network defense

Building upon long-standing expertise, HPE has launched HPE Threat Labs to address this evolving threat environment. By uniting the world-class security research talent and intelligence from HPE and Juniper Networks, HPE Threat Labs brings together deep expertise, and creates an even more extensive data pool to identify and track real-world threats and directly inform HPE products with the threat intelligence needed to detect and block malicious attacks efficaciously.

“HPE Threat Labs was created to bridge the gap between cutting-edge research and real-world security outcomes,” said David Hughes, SVP & GM, SASE and Security for Networking, HPE. “The In the Wild report shows that today’s attackers operate with the discipline, scale, and efficiency of global enterprises, and defending against them requires the same level of strategy, integration, and operational rigor. By translating threat intelligence into our products, HPE Threat Labs is helping organisations reduce risk, limit disruption, and protect the systems their businesses depend on.” 📌

UAE PARENTS' SOCIAL SHARING OF CHILDREN RAISES PRIVACY CONCERNS, SAYS KASPERSKY

Kaspersky "Growing up online" survey reveals that almost half (54%) of parents in the United Arab Emirates regularly post photos, videos, or updates about their children on social media platforms. While family content remains popular, privacy settings and motivations behind sharing vary significantly.

Among those who post about their children, 61% limit visibility to friends, friends of friends, or followers. However, more than a quarter (39%) of surveyed parents maintain fully public accounts, making such content accessible to anyone online.

The main reason parents share content featuring their children is to preserve memories (65%), followed by pride in their children's achievements (46%). At the same time, social influence also plays a role: 27% admit they post because others do the same, and 27% say they like how they appear in the photos or videos. Additionally, 11% acknowledge that they share content about their children to attract more followers or increase engagement, believing such posts generate more likes.

Notably, 63% of respondents say they ask their children for permission before publishing content about them. However, one in five parents (19%) admit they proceed with posting regardless of whether the child agrees.

"It can be difficult for parents to distinguish between harmless sharing and content that may unintentionally compromise a child's safety. What feels like a proud family moment today can contribute to a permanent digital

Seifallah Jedidi,
Head of Consumer
Channel in Middle East,
Turkiye and Africa,
Kaspersky.



footprint tomorrow. That is why it is important to pause and reconsider the urge to share – especially when the motivation is popularity or engagement. Online attention is temporary, but the risks can be long-term," said Seifallah Jedidi, Head of Consumer Channel in the Middle East, Turkiye and Africa at Kaspersky.

When parents overshare information about their children online, they may unintentionally expose sensitive details such as full names, dates of birth, school locations or daily routines. This information can be exploited for identity theft, social engineering, fraud, or even physical safety risks. Publicly available photos and videos may also be misused, altered, or redistributed without consent, contributing to long-term digital footprint issues and reputational harm.


To safeguard children's data and share safely, Kaspersky strongly recommends

following this advice:

Limit access to your social media accounts and make them visible to friends only (but always mind that you add to the list of friends the people you know personally). Do not forget about general safety settings such as two-factor authentication and a secure password.

Do not share the materials that may cause any harm to your child, like the contacts of your child, the name of their school, etc.

Maintain open and trusting relationships with your children, talk to them about digital hygiene and online safety, and lead by example by practicing responsible and mindful behavior on social media yourselves.

Consider a reliable security solution with the Safe Kids module, which helps to guard your family and private data, plus protects your kids online and beyond. 



Fortify Your Cybersecurity

Fortinet
Global Cybersecurity Leader

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

Learn more at fortinet.com

IDENTITY CONVERGENCE DRIVES NEW FOCUS ON TRUST, PROTECTION AND USER CHOICE

NEW RESEARCH HIGHLIGHTS FIVE TRENDS SHAPING THE IDENTITY LANDSCAPE, ALONGSIDE RISING ETHICAL AND PRIVACY CONCERNS

HID, a global leader in trusted identity solutions, has released its 2026 State of Security and Identity Report, revealing how organisations in the region and worldwide are reshaping their approach to identity management. Based on insights from more than 1,500 security and IT professionals, end users and industry partners across regional and global markets, the research shows that security leaders are focused on how to manage identities in ways that build trust, strengthen protection and preserve user choice across increasingly converged physical and digital environments.

“Security leaders are clearly under pressure to modernise access and identity infrastructure, but our research shows they’re equally focused on the governance, protection and transparency that build lasting trust,” said Ramesh Songukrishnasamy, Senior Vice President and Chief Technology Officer at HID. “The organisations succeeding in 2026 are those giving stakeholders meaningful solution choice while maintaining robust security.”

Key Findings that Define the Path Forward

1. Identity management now dominates strategic planning (73%) of respondents rank identity management as a top priority, reflecting a shift towards unified identity governance that spans both physical access and digital systems.



Ramesh Songukrishnasamy,
Senior Vice President and
Chief Technology Officer, HID.



2. Mobile credentials have reached critical mass

Mobile credentials adoption is now driven by security improvements (50%) rather than convenience (34%), a notable shift as organisations recognise the many advantages of mobile credentials. Meanwhile, hybrid credential environments remain standard, with 84% of end users maintaining physical credentials within their mobile deployment.

3. Biometrics are expanding beyond MFA into core access control

Biometric technologies continue to gain traction (45% of users view them as strategic), with fingerprint (71%) and facial

recognition (50%) leading adoption. Yet, ethical and privacy concerns more than doubled year-over-year from 31% to 67%.

4. Physical and digital identity convergence is accelerating

(75%) of organisations have either deployed (29%) or are actively evaluating (46%) unified identity solutions. While single credentials spanning buildings, networks and applications deliver efficiency and stronger security, budget constraints (51%), complexity (37%), and expertise gaps (34%) remain persistent barriers.

5. Investment patterns are shifting towards integrated platforms

Organisations are prioritising integrated

identity and security platforms over standalone point solutions to improve visibility, efficiency, and resilience across increasingly complex environments. Yet, integration complexity persists as a primary barrier (52% for identity systems, 37% for physical-digital convergence).

Ethics and privacy concerns are at an all-time high

Beyond technology trends, the 2026 report highlights ethics and privacy as a defining concern, with 67% of end users expressing 'high' or 'moderate' concern about ethical and privacy implications. As a result, organisations are strengthening policies and governance to balance protection with individual rights.

Drawing on diverse perspectives across industries, including healthcare, education, government, finance, manufacturing, and critical infrastructure, the survey offers insight into how strategy aligns with execution and where gaps remain. **i**

THE ORGANISATIONS SUCCEEDING IN 2026 ARE THOSE GIVING STAKEHOLDERS MEANINGFUL SOLUTION CHOICE WHILE MAINTAINING ROBUST SECURITY."

SENTINELONE APPOINTS SONALEE PAREKH AS CHIEF FINANCIAL OFFICER

WORLD'S LEADING AI SECURITY FIRM USHERS IN NEXT CHAPTER OF GROWTH AND PROFITABILITY WITH NEW CFO.

SentinelOne, the leader in AI-native cybersecurity, announced the appointment of Sonalee Parekh as Chief Financial Officer, effective March 24, 2026. Parekh will oversee all aspects of the company's global financial operations, including FP&A, accounting, tax and treasury, internal audit, and investor relations. Barry Padgett will continue to serve as Interim CFO until Parekh's start date, leading the company's upcoming fiscal fourth quarter and full year 2026 earnings report and ensuring a seamless transition.

Bringing more than 25 years of experience across public software and technology companies, Parekh will lead SentinelOne's finance organisation and drive its financial strategy as the company scales while advancing its leadership in AI-native cybersecurity.

Parekh joins SentinelOne with extensive public company experience and a track record of scaling high-growth software platforms. Most recently, as Chief Financial Officer of Asana, she led the global finance organisation and played a key role in advancing the company's multi-product, AI-first strategy, and improving profitability. Previously, she served as CFO of RingCentral, where she helped scale the business to over \$2 billion in annual recurring revenue while significantly improving margins through financial rigor and discipline. She also held senior finance leadership roles at



Hewlett Packard Enterprise, including Divisional CFO and Head of Corporate Development and Investor Relations.

"Sonalee's proven track record of scaling global software organisations and driving financial discipline makes her the perfect fit to lead SentinelOne's next phase of profitable growth," said Tomer Weingarten, CEO of SentinelOne. "Her arrival marks a significant milestone for our leadership team as we capitalise on the surging market demand for AI-native cybersecurity. I also want to thank Barry for his exceptional leadership and steady hand through this transition."

SentinelOne continues to lead the cybersecurity industry with world-class technology, top-tier growth profile, and

impressive margin expansion. As the world's leading AI-native cybersecurity platform, SentinelOne empowers the world to run securely by creating intelligent, data-driven systems that think for themselves, stay ahead of complexity and risk, and evolve on their own.

"SentinelOne is uniquely positioned at the convergence of two powerful secular megatrends, AI and cybersecurity," said Parekh. "The company has built a differentiated AI-native platform and a strong financial foundation. I am excited to partner with Tomer and the leadership team to advance SentinelOne's mission, accelerate growth, expand margins, deepen investor engagement, and deliver sustained long-term value for our shareholders." 📌

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



MIDDLE EAST AND AFRICA'S



SCAN HERE



GET FREE
 VISITOR PASS

#gisecglobal
 gisec@dwtc.com

SPONSORS & PARTNERS

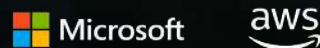
OFFICIAL DISTRIBUTION PARTNER



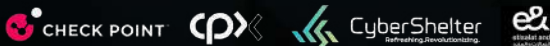
LEAD STRATEGIC PARTNER



STRATEGIC PARTNER



DIAMOND SPONSOR



PLATINUM SPONSOR



GOLD SPONSOR



SILVER SPONSOR



BRONZE SPONSOR





Delinea

Unlock AI's potential, not your defenses.

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

Machine identities now outnumber humans as much as 46:1¹, making them prime targets for attackers seeking to exploit privileged credentials.

Secure AI with Delinea so you can:

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

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

¹Delinea, Cybersecurity and the AI Threat Landscape, 2025