ISSUE 105 | APRIL 2026

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

IDENTITY TURNS NEW SECURITY CONTROL PLANE

AI AGENTS, MACHINE IDENTITIES, AND CREDENTIAL ABUSE ARE FORCING ENTERPRISES TO RETHINK TRUST AND ACCESS CONTROL.

tahawultech.com

cnme computer news middle east SUPPLEMENT

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 SPONSOR

logitech

OFFICIAL PUBLICATIONS

cnme computer news middle east

Reseller MIDDLE EAST

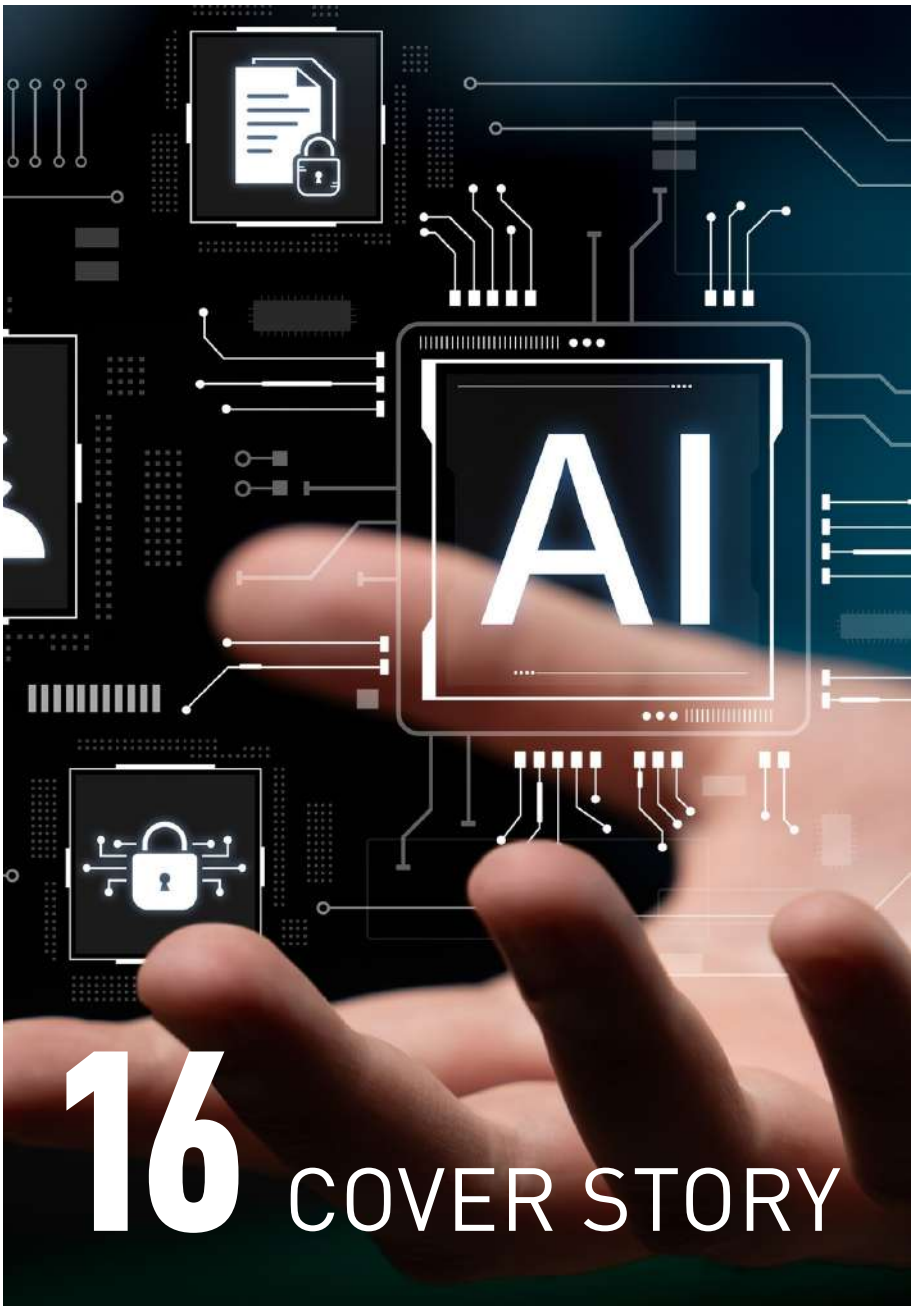
Security MIDDLE EAST

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/

CONTENTS



GITEX AI EUROPE Berlin 2026

30/JUNE
01/JULY
— MESSE BERLIN —

DRIVING A BOLD, OPEN & CONNECTED DIGITAL FUTURE

EUROPE'S MOST GLOBAL TECH, STARTUP & DIGITAL INVESTMENTS EVENT

GET YOUR FREE PASS*

*LIMITED OFFER

SCAN TO REGISTER

Follow Us

#GITEXAIEUROPE

EDITOR'S NOTE

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

Sandhya DMello
Editor

IDENTITY TAKES CONTROL IN THE AGE OF AI

April's edition of Security Advisor Middle East places identity firmly at the centre of the cybersecurity conversation. Our cover story explores how identity has evolved into the primary control plane of modern enterprise security, driven by the rapid rise of AI agents, machine identities, and credential-based attacks. Insights from industry leaders at BeyondTrust, Delinea, Trellix, Acronis, ManageEngine and Sophos underline a defining shift: attackers are no longer breaking in—they are logging in.

IDENTITY DEFINES SECURITY NOW

Across the issue, this identity-first narrative extends into enterprise security strategies and platform innovation. ServiceNow strengthens cyber asset intelligence through its Armis acquisition, while Cloudflare and Wiz address the growing AI attack surface. Meanwhile, Rubrik and Dell Technologies reinforce the importance of resilience, performance, and recovery in a threat landscape increasingly shaped by AI.

Our research section reveals a sobering reality. Studies from Sophos, Veeam, and SAS highlight gaps in trust, recovery readiness, and preparedness against AI-driven fraud, signalling that confidence often outpaces capability.

In opinion, voices from Cloudera, ManageEngine and SANS Institute examine resilience, cyber warfare, and industrial control system risks in an increasingly volatile geopolitical landscape.

Finally, our appointments section reflects a market in motion, with leadership moves at Delinea, TrendAI, SentinelOne and WatchGuard Technologies signalling continued investment in growth, partnerships, and AI-led transformation.

The message is clear. Identity is no longer a feature of security; it is its foundation.

EVENTS

tahawultech.com FUTURE SECURITY AWARDS

tahawultech.com CISO50 AWARDS & FORUM

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

BEYONDTRUST DELIVERS INDUSTRY'S FIRST UNIFIED PRIVILEGED IDENTITY SOLUTION FOR AI AGENT COWORKERS AND WORKLOADS

BeyondTrust, the global leader in privilege-centric identity security protecting Paths to Privilege, has announced expanded capabilities across its Pathfinder Platform that deliver the industry's first unified approach to securing AI agent coworkers that operate alongside users and autonomous AI workloads executing at scale across cloud and SaaS environments. The announcement is backed by new threat research from BeyondTrust Phantom Labs, which found that the majority of enterprises are running shadow AI agents with privileged access that security teams cannot see or govern.

AI agents are no longer experimental. They are production workloads, initiating API calls, using credentials, deploying code, and accessing sensitive data. Many are deployed in minutes on low-code platforms, often with privileges that rival or exceed those of human administrators. In many enterprise environments, machine and AI identities already far outweigh human identities, dramatically expanding the privileged-identity attack surface. Yet most organisations lack any visibility into how many AI agents are operating in their environments, what those agents can access, or what happens when one of those agents is compromised. These trends underscore the need for a unified approach to securing AI, human, and machine identities across environments.

"Agentic AI is not an isolated problem. It's a subset of the broader non-human identity landscape," said Marc Maiffret, Chief Technology Officer at BeyondTrust. "Organisations cannot secure agentic identities in a silo. These agents are interconnected with human identities, machine accounts, secrets, and entitlements across every environment. You need a platform that sees and secures the full spectrum, and that's what Pathfinder delivers. Simply put, to get agentic AI right, you need to get privileged identity right."

Marc Maiffret, Chief Technology Officer at BeyondTrust.

Securing AI Identities Across Coworkers and Workloads

Unlike most AI security solutions, the Pathfinder Platform addresses both sides of the agentic AI challenge, providing defense for AI coworkers and local agents on endpoints, as well as for AI workloads running autonomously across cloud infrastructure and SaaS platforms.

New capabilities include:

- Endpoint Privilege Enforcement for AI Coworkers: BeyondTrust Endpoint Privilege Management (EPM) enforces least privilege and application control for AI clients operating on endpoints, such as Claude, ChatGPT, etc., ensuring AI tools can only execute actions permitted by policy—a critical enforcement plane that no other agentic AI security vendor delivers.
- AI Agent Discovery and Risk Analysis: Identity Security Insights® delivers comprehensive agentic AI discovery, classification, and posture auditing with connector coverage spanning major enterprise AI platforms, including OpenAI (Admin, Projects, and ChatGPT Enterprise), Google Vertex AI and Discovery Engine, Salesforce Agentforce, ServiceNow AI agents, and AWS Bedrock. Organisations gain automatic discovery, privilege path mapping, risk scoring, and shadow AI detection wherever they deploy agents.
- Secrets Management for Autonomous Agents: BeyondTrust Password

Safe® vaults, rotates, and enforces just-in-time access for the secrets and API keys that power agentic workloads. Combined with Insights, organisations gain end-to-end visibility from agent discovery through credential management, eliminating the static credential exposure that creates persistent attack surfaces.

Managing the Explosion of Non-Human Identities

Telemetry surfaced through BeyondTrust's Identity Security Insights, operating within the Pathfinder Platform, indicates AI agent growth is accelerating rapidly across enterprise environments. Over the past year, organisations analysed through the Pathfinder Platform experienced a 466.7% increase in enterprise AI agents, many deployed through low-code platforms and automation frameworks that operate across endpoints, cloud infrastructure, and SaaS applications.

"The question security teams should be asking isn't 'do we have AI agents?' You do," Maiffret continued. "The question is: what can they access, what secrets are they using, and what happens if one gets compromised? A single AI agent's blast radius can span your identity providers, cloud infrastructure, SaaS platforms, and on-prem directories all at once. Pathfinder maps those cross-domain privilege paths so you can see exactly how a compromised agent could escalate access across your entire environment."

Free AI Security Posture Assessment

BeyondTrust's Identity Security Risk Assessment (ISRA) now provides organisations with immediate visibility into AI agent risk as part of a comprehensive identity security posture analysis. The assessment connects across enterprise identity and AI agent infrastructure in under an hour and delivers findings within 24 hours, including discovery and inventory of all AI agents, shadow AI detection, cross-domain privilege path analysis, and risk scoring aligned to MITRE ATT&CK with prescriptive remediation guidance.

SERVICENOW COMPLETES ARMIS ACQUISITION, CLOSING GAP BETWEEN ASSET VISIBILITY AND CYBER RISK

ServiceNow expands its security platform into physical and operational environments, strengthening cyber asset intelligence for trusted agentic AI at scale.

ServiceNow, the AI control tower for business reinvention, has completed its acquisition of Armis. Armis, a leading cyber exposure management and security company, delivers a comprehensive AI-powered solution that sees, protects, and manages cyber risk across every connected asset — from OT, IoT, medical devices, physical AI to code and cloud — in real time. The acquisition extends ServiceNow's security platform into the physical and operational layers of the enterprise, adding the cyber asset intelligence foundation and business context that enterprises need to deploy agentic AI with trust and control at scale.

The close follows ServiceNow's completion of the Veza acquisition in March 2026. Veza brought AI-native identity intelligence to the ServiceNow AI Platform, giving enterprises continuous visibility into who and what has access to every digital, connected resource. With the Armis acquisition, ServiceNow's identity intelligence and cyber exposure management capabilities distinctively power critical pre-breach and post-breach security outcomes as enterprises deploy agentic AI at scale. Together, Armis delivers real-time visibility and protection across every connected cyber asset, while Veza maps every permission and access path across human, machine, and AI agent identities.

Closing the gap between visibility and cyber risk

Security teams operating across fragmented, point solution stacks have long faced a structural challenge. Historically, the tools that manage risk cannot execute on remediation actions, and the tools that remediate cyber risk cannot see the full picture. The result is a widening gap between detection and response, a gap that exponentially increases the risk of security incidents in the agentic AI era.

Stolen credentials remain the dominant entry point for attackers[1] and this problem is accelerating. Machine identities now outnumber human identities by more than 80 to one, and nearly half carry sensitive or privileged access rights that most organisations cannot fully see or control, leading to lateral movement attacks. As enterprises accelerate agentic AI, their attack surface has expanded further to encompass autonomous agents, unmanaged OT devices, and other connected systems across manufacturing, healthcare, and critical infrastructure that conventional security tools were never built to handle.

ServiceNow's advantage is architectural. Armis provides continuous, real-time visibility, management, and security across every connected cyber asset through non-invasive discovery, tracking nearly 7 billion devices in real time, including OT, IoT, medical devices and physical AI, code, and cloud. Veza's Access Graph provides cross-system visibility into every permission held by every human, machine, and AI agent identity. Both graphs power ServiceNow's Context Engine — the organisational

of every connected asset, including the devices and systems that conventional tools were never built to see. Combined with Veza's identity intelligence, that signal flows into ServiceNow's Context Engine and AI Control Tower, turning exposure into automated remediation with governance and a full audit trail built in at every step."

"We built Armis to solve the toughest cybersecurity challenges of organisations globally, protecting all their assets across IT, OT, IoT, medical devices, code, and cloud that are at the heart of manufacturing, healthcare, and critical infrastructure," said Yevgeny Dibrov, co-founder and CEO, Armis. "Joining ServiceNow, with Veza already on the platform, enables us to address this mission tenfold to keep the world's largest and most complex enterprise environments safe and secure."

Amit Zavery, president, chief operating officer, and chief product officer at ServiceNow.

What this means for customers and partners

For current Armis customers, Armis Centrix now operates with the full support of ServiceNow's product, engineering, and global go-to-market organisation. It is integrated with the ServiceNow AI Platform today and remains available as a standalone solution, with deeper integration expected over time.

Customers of both ServiceNow and Armis can immediately begin leveraging their combined capabilities, with broader availability coming soon. Partners of ServiceNow and Armis can immediately accelerate revenue by tapping into growing customer demand from organisations looking to deploy agentic AI with trust and control at scale.

ServiceNow establishes global hub to pioneer autonomous cyber defense

ServiceNow is establishing an AI Center for Cyber Defense — a global hub dedicated to building the next generation AI security stack and pioneering the transition from reactive security to autonomous, agentic cyber defense. The center will bridge the gap between AI research and practical cybersecurity solutions, serve as a definitive resource for enterprise security leaders transitioning from legacy frameworks to AI-native security postures, and develop the expertise needed to anticipate and neutralise AI-driven attacks before they occur.

Strength building on strength

In the four months since the acquisition was announced, Armis has continued to operate as an independent company, consistently being recognised as a Leader. Armis was recently named a Leader in the 2026 Gartner Magic Quadrant for CPS Protection Platforms for the second consecutive year. Armis was also named a Leader in The Forrester Wave: IoT Security Solutions, Q3 2025 and The Forrester Wave: Unified Vulnerability Management Solutions, Q3 2025. Armis Centrix was named "Best Solution" for Cyber Exposure Management in The Global InfoSec Awards at RSAC 2026 Conference.

The companies already maintain multiple integrations connecting Armis' asset intelligence to ServiceNow workflow action, making this integration acceleration, not initiation. Armis is trusted by nine of the Fortune 10 and more than 35% of the Fortune 100, as well as by public sector organisations and government agencies globally. Many of these organisations are already ServiceNow customers, reinforcing the complementary nature of both companies' capabilities and the demand that already exists for their combined capabilities.

"Stronger cyber resilience starts with visibility across the entire network," said Rex Thexton, chief technology officer, Accenture Cybersecurity. "At Accenture, we help clients align this critical security foundation with real business outcomes. By leveraging solutions like ServiceNow and Armis, organisations can accelerate automated asset protection so they can scale securely, build the visibility needed to be resilient, and stay ahead of cyber threats."

"As the attack surface expands, real-time visibility and control over every asset is non-negotiable," said John Whittle, chief operating officer, Fortinet. "ServiceNow's acquisition of Armis enables a powerful three-way partnership with Fortinet, advancing cybersecurity into an AI-driven, autonomous system that helps organisations continuously understand assets, prioritise threats, and execute response in real time. With Fortinet's industry-leading AI-driven innovation at scale, combined with our long-standing relationships and deep integrations across both platforms, we can drive ServiceNow security workflows with precision — delivering faster, closed-loop protection and more consistent, accurate response for our customers."

With Armis employees joining ServiceNow, the combined organisation brings deep expertise in cyber-physical security and risk to the ServiceNow AI Platform, accelerating its roadmap for autonomous, proactive cybersecurity. ServiceNow closed its largest quarter ever for OT in Q4 2025 and its security and risk business crossed $1 billion in annual contract value in Q3 — organic growth that established the foundation Armis now extends.

Armis, together with Veza, is expected to more than triple ServiceNow's addressable market for security and risk solutions.

CLOUDFLARE, WIZ PARTNER TO SECURE GLOBAL AI ATTACK SURFACE, ELIMINATE BLIND SPOTS CAUSED BY SHADOW AI

New integration gives organizations a clear path from identifying AI risks to stopping attacks in real-time

Tom Evans, Chief Partner Officer at Cloudflare.

Cloudflare, Inc., the leading connectivity cloud company, today announced a partnership with cloud and AI security leader Wiz, now part of Google Cloud, to give security teams a unified way to analyze and protect AI-powered applications across their entire environment. By integrating the power of Cloudflare's AI Security for Apps directly into the Wiz Security Graph, organisations will gain access to the most comprehensive map of their entire AI footprint, and the tools needed to secure it.

Organisations are shipping AI-powered features faster than security teams can track them. Every new chatbot, copilot, or AI-powered search endpoint is a potential attack surface vulnerable to prompt injection, sensitive data exfiltration, and abuse. The challenge is knowing which ones exist across your web properties, whether they have security guardrails in place, and whether those guardrails are actually working. To help organisations understand their AI footprint and whether they have the necessary guardrails in place, CISOs need a single source of truth where they can better understand and secure their AI and cloud infrastructure.

The integration helps customers autonomously eliminate AI blind spots across their infrastructure, allowing security teams to safely accelerate AI adoption. Cloudflare's AI Security for Apps equips organisations with guardrails at the edge to secure AI endpoints from risks such as prompt injection and unsafe topics, while Wiz's AI Application Protection Platform (AI-APP) simultaneously maps the complete AI application and surfaces the security gaps. By integrating Cloudflare's security rules into the Wiz Security Graph, security teams can prioritise risks based on exploitability. As a result, CISOs gain visibility into the LLMs operating across their web properties and runtime controls to enforce policies. Cloudflare and Wiz are model and host-agnostic, protecting endpoints regardless of the LLM or cloud provider.

"AI is the most transformative technology we've seen in a generation, powering countless capabilities. But for a majority of businesses, it can be a black box. When talking with CISOs today, they are struggling with the balance of being an enabler of innovation with AI, while combating uncontrolled shadow AI across their organisation because their legacy security tools are effectively useless at this level," said Tom Evans, Chief Partner Officer at Cloudflare. "The Cloudflare and Wiz partnership helps tackle this trade-off. Now, we are delivering a solution to allow innovation with AI at speed, without the worry that their most sensitive data will be exposed."

"Security alignment isn't just about reducing risk, it's an enabler of AI application development," said Oron Noah, VP of Product, Extensibility & Partnerships at Wiz. "By combining Wiz's end-to-end visibility with Cloudflare's edge protections, we close a critical gap in how AI risk is managed. This partnership gives organisations a unified view of AI application endpoints and shared risk context, helping them stop threats like prompt injection and shadow AI before they start."

Cloudflare's partnership with Wiz empowers customers to:

- Discover Shadow AI: identify all LLM endpoints across your web properties, including ones deployed without security team involvement, and understand which are protected and which are exposed.

- Inspect AI Traffic In Real Time: Cloudflare AI Security for Apps runs detections on every request to LLM endpoints to identify and mitigate PII leakage, prompt injection, and custom-defined topics. These detections run in parallel across Cloudflare's global network, without adding latency to AI traffic.
- Map Sensitive Data Flows: Wiz maps data flows between AI applications, models, and data stores onto its Security Graph, giving security teams visibility into where sensitive data interacts with AI workloads to help teams prioritise remediation.
- Verify Guardrails: Wiz verifies that AI deployments are protected by Cloudflare's AI Security for Apps. If guardrails are missing or misconfigured, Wiz alerts teams for direct remediation within the Cloudflare platform.
- Prioritise Remediation: The integration surfaces which unprotected AI endpoints have access to sensitive data or production systems, so security teams fix the highest-risk gaps first.

The partnership delivers a seamless integration without needing custom workflows or additional agents to deploy. Cloudflare's detections run inline on its global network, one of the largest and most interconnected in the world, so organisations gain AI security without architectural changes or performance trade-offs.

CIS, ASTRIX, AND CEQUENCE RELEASE NEW AI SECURITY COMPANION GUIDES

Partnership delivers practical guidance for securing LLMs, agents, and MCP environments

The Center for Internet Security, Inc. (CIS), Astrix Security, and Cequence Security today announced the release of three new CIS Critical Security Controls (CIS Controls) Companion Guides designed to help enterprises secure rapidly evolving AI environments.

Co authored by experts across all three organisations, the guides extend the CIS Critical Security Controls into AI systems where large language models (LLMs), autonomous agents, and Model Context Protocol (MCP) integrations introduce new and unique risks. Each guide focuses on a distinct layer of the AI ecosystem, offering targeted guidance aligned with how modern AI systems operate:

- AI LLM Companion Guide: Provides guidance for securing large language models, including risks related to prompts, context handling, and exposure of sensitive information.
- AI Agent Companion Guide: Outlines controls for managing autonomous and semi-autonomous agents, focusing on safe tool execution, governed autonomy, and appropriate access to enterprise systems.
- MCP Companion Guide: Details protections for Model Context Protocol environments, emphasising secure tool access, management of Non-Human Identities (NHIs), and auditable interactions across the protocol layer.

Shreyans Mehta, CTO and Co-Founder of Cequence Security.

As AI becomes deeply embedded in production workflows – from copilots to autonomous task execution to tool-integrated systems – security teams are confronting risks that traditional controls were never built to address. These include data leakage, unbounded agent autonomy, credential misuse, and unsafe or inappropriate execution of tools. The new Companion Guides offer practical, prioritised guidance that reflects how AI is actually deployed in modern enterprises.

"These guides reflect a shared effort to bring clarity to an area where organisations are seeking direction," said Curtis Dukes, Executive Vice President and General Manager of Security Best Practices at CIS. "By combining our collective expertise, we translated the CIS Controls into concrete steps that help teams secure AI systems

across the model, agent, and protocol layers."

Astrix contributed deep expertise in securing AI agents, MCP servers, and NHIs, including API keys, service accounts, and OAuth tokens that connect AI systems to enterprise resources.

"AI agents introduce a new operational surface that organisations must understand before they scale," said Jonathan Sander, Field CTO of Astrix Security. "Collaborating with CIS and Cequence allowed us to build guidance that addresses identity, authorisation, and execution risks in a way that's both actionable and aligned with how enterprises work today."

Cequence brought extensive experience in securing enterprise applications, data, and APIs, shaping guidance around visibility, governance, and control over what AI systems can access and execute.

"As AI systems interact more directly with applications and APIs, the security implications become increasingly critical," said Shreyans Mehta, CTO and Co-Founder of Cequence Security. "This partnership enabled us to create guidelines that codify what we've learned about deploying agentic AI at the world's largest enterprises without sacrificing security, governance, or scale, giving organisations a framework for enabling agentic AI safely."

How the Companion Guides Support Organisations

Together, the three Companion Guides give security and IT teams a unified way to apply the CIS Controls to AI systems that behave and evolve differently from traditional software. By extending the Controls into environments powered by LLMs, autonomous agents, and MCP-based integrations, the guidance helps organisations understand where risks emerge and how to address them with guidance that reflects real-world deployment patterns.

The guides:

- Adapt the CIS Controls to AI-driven architectures, helping teams secure LLMs, agentic systems, and MCP interfaces without adopting a new framework.
- Provide clear, prioritised recommendations that support responsible AI adoption across development, deployment, and operational phases.
- Blend the strengths of all three organisations by combining standards leadership with deep expertise in agentic AI and API-centric security.
- Cover the full AI security stack, from model inputs and context handling to agent reasoning, tool execution, and protocol-level access.

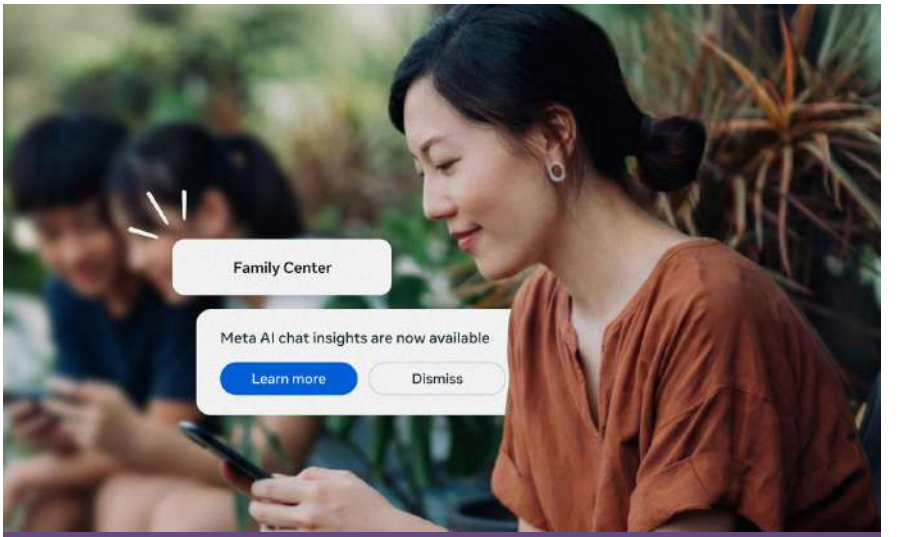
META ROLLS OUT AI CONVERSATION INSIGHTS FOR PARENTS SUPERVISING TEEN ACCOUNTS

New supervision tools allow parents to view the topics teens discuss with Meta AI, alongside expert-led conversation guides and wellbeing oversight.

Meta has introduced new parental supervision tools designed to help parents better understand how their teens are engaging with AI across its platforms.

Parents supervising Teen Accounts on Facebook, Messenger and Instagram can now access an Insights tab that shows the topics their teen has asked Meta AI about over the past seven days. The feature is currently available in the US, UK, Australia, Canada and Brazil, with a global rollout planned in the coming weeks.

The topics may include school, entertainment, lifestyle, travel, writing, health and wellbeing. Parents can also view broader categories within each



Meta's new AI insights aim to help parents better understand how teens engage with AI across Facebook, Messenger and Instagram.

topic, such as fitness, physical health and mental health under health and wellbeing.

Meta said the feature is designed to provide parents with greater visibility into general AI interactions, while maintaining safeguards for teen users. The company also said it is developing alerts for parents if a teen attempts to engage Meta AI in conversations related to suicide or self-harm.

The new tools complement existing Teen Account protections, including time limits, scheduled breaks and visibility into who teens have chatted with over the past seven days.

Meta has also worked with the Cyberbullying Research Center to develop AI conversation starters that help parents discuss AI use with teens in a non-judgmental way.

The company has also launched an AI Wellbeing Expert Council, comprising experts in youth safety, mental health, body image, suicide prevention and responsible AI, to provide ongoing input on age-appropriate AI experiences for teens.

RUBRIK ANNOUNCES CYBER RESILIENCE FOR GOOGLE CLOUD SQL

Rubrik Security Cloud provides enterprise security and recovery for PostgreSQL databases.

Rubrik, the Security and AI Operations Company, announced today it is now offering cyber resilience capabilities to organisations running Google Cloud SQL. The integration enables Cloud SQL customers to leverage Rubrik Security Cloud to protect their managed PostgreSQL databases with immutable, automated backups that add Rubrik's enterprise-grade cyber resilience without disrupting their current database operations or recovery strategy.

Cloud SQL has become a foundational database service for enterprise applications, housing some of organisations' most critical production workloads. As these databases grow, so do customer requirements for comprehensive cyber resilience. The new integration delivers Rubrik's enterprise-grade protection for Cloud SQL, helping joint customers defend against ransomware with air-gapped backups and rapid cross-region recovery at scale.

"Organisations shouldn't have to choose between cyber resilience and disaster recovery," said Anneka Gupta, Chief Product Officer at Rubrik. "With Google Cloud, we're giving our joint customers immutable backups that work alongside their existing disaster recovery strategy, so they can meet compliance requirements, protect against threats, and recover fast, all without changing their architecture."

Anneka Gupta, Chief Product Officer at Rubrik.

Key Features with Rubrik Security Cloud for Google Cloud SQL:

- Unified cyber resilience: Manage Cloud SQL protection alongside Google Workspace, Google Compute Engine, and Google Kubernetes Engine from a single, intuitive interface.
- Automated discovery and protection: Automatically discover new Cloud SQL instances and apply global policies.
- Backup without tradeoffs: Delivers immutable backups that add enterprise-grade cyber resilience without disrupting existing database operations or disaster recovery strategies, and with no limit on retention periods.
- Storage class flexibility: Choose Google Cloud Storage Archive, Coldline, or Nearline for backups to align cost with actual usage.
- Meet compliance objectives: Use tag-based SLA policies to enforce consistent retention across every instance to meet compliance requirements automatically.

Rubrik Zero Labs found that organisations are facing an increased wave of cyberattacks, with 90% of IT and security leaders reporting cyberattacks in the previous year. The study also revealed that 35% of IT leaders cite securing data across varied ecosystems as their top challenge, followed closely by a lack of centralised management and visibility over cloud-based data. Rubrik Security Cloud for Cloud SQL provides resilience with a unified, automated approach for PostgreSQL databases, and addresses a growing need for protection in regulated industries that are scaling managed databases.

DELL TECHNOLOGIES ENHANCES MISSION-CRITICAL STORAGE WITH POWERMAXOS 10.4

Dell Technologies announced PowerMaxOS 10.4, a major software update for its industry-leading mission-critical storage. The release introduces faster performance, enhanced cyber resilience and deeper ecosystem integration, to help business stays ahead of the curve.

Unlocking New Levels of Performance and Efficiency

PowerMax is trusted by enterprises to handle the most demanding workloads like large-scale Oracle, SAP, Salesforce and Epic deployments. PowerMaxOS 10.4 takes this performance to the next level, delivering up to 25% faster read response times for SRDF-protected workloads1. Real-time decision-making and high-performance applications now have the speed that they need to excel with the leading cyber resilience.

Efficiency is equally critical, especially when balancing innovation with budget constraints. PowerMaxOS 10.4 accelerates performance while lowering the total cost of ownership for the new PowerMax 2500 and 8500 arrays. This allows organisations to achieve outstanding IOPs performance with reduced costs, thanks to the newest PowerMax node-pair configuration.

Fortifying Cyber Resilience

PowerMaxOS 10.4 introduces Advanced Ransomware Detection to identify risks early and protect businesses before attacks occur. With Single Sign-in (SSO) support for Okta, PingFederate and Entra ID, access management is simple, while private-key support for SSO OIDC strengthens security. Together, these features help customers accelerate Zero Trust deployments that safeguard vital data without disrupting productivity.

Supporting automated failover, load balancing and full-scale recovery, PowerMax uses secure snapshots and flexible data protection to keep businesses running through any challenge.

Bridging the Gap to Modern Applications

Modernising applications is a top priority for large enterprises, but the shift from virtual machines to container platforms can be complex. PowerMaxOS 10.4 simplifies this journey through seamless integrations with both VMware and Red Hat OpenShift. Customers can now migrate VMware virtual machines up to 10 times faster2 through array-based XCOPY and the Red Hat Migration Toolkit for Virtualization (MTV). Additionally, enhanced REST API support enables up to 7 times faster storage cluster provisioning for OpenShift Container Platforms3 (OCP). These advancements help IT professionals and developers focus on creating value. PowerMaxOS 10.4 represents the future of mission-critical storage, combining performance, security and deep ecosystem integration to help businesses thrive.

"From a storage point of view, the bank's critical workloads and applications run on PowerMax due to its performance, reliability and flexibility. PowerMax very much runs the bank."

Ali Rey, Group Head of Technology Platforms, Emirates NBD.

ACRONIS LAUNCHES GENAI PROTECTION, ENABLING MSPS TO SECURE AND GOVERN AI USAGE

New solution provides visibility, control, and protection for generative AI adoption, designed for MSPs

Acronis, a global leader in cyber protection, has announced the launch of Acronis GenAI Protection, a monitoring and security solution that enables managed service providers (MSPs) to control generative AI usage across client environments, preventing sensitive data exposure and protecting against malicious prompt manipulation. Acronis GenAI Protection represents the initial phase of Acronis Cyber Workspace, with additional capabilities planned for release to deliver a protected AI workspace, natively integrated into the Acronis platform.

As organizations rapidly adopt generative AI tools, businesses face growing risks related to data leakage, shadow AI usage, and malicious prompt manipulation. Many consumer-grade AI tools lack enterprise visibility, while enterprise solutions are not designed to be delivered and managed through MSPs. Acronis GenAI Protection addresses this gap by providing partners with a purpose-built solution to monitor and secure generative AI usage across SMB environments.

AI Monitoring and Security Delivered Through MSPs

Acronis GenAI Protection is designed to be provisioned, managed, and monetized by MSPs. Through a centralized console integrated into the Acronis platform, service providers can monitor AI usage across customer environments, including policy enforcement, reporting, and risk mitigation, while protecting generative AI interactions alongside data, applications, and endpoints.

"Generative AI adoption is accelerating, but it introduces new risks that businesses are not fully equipped to manage," said Gaidar Magdanurov, President at Acronis. "MSPs are uniquely positioned to help businesses adopt AI securely, but until now they haven't had the right tools to monitor and manage it effectively. GenAI Protection enables MSPs to turn AI security into a managed service, creating new revenue opportunities while protecting their customers from emerging risks."

Built-In Protection for Generative AI Usage

Acronis GenAI Protection provides visibility and security for AI usage without requiring additional point solutions or enterprise-grade complexity.

Key capabilities include:

- Shadow AI usage and visibility: Discover and monitor generative AI applications used across client environments to understand adoption and risk exposure.
- Sensitive data protection for AI interactions: Inspect prompts for sensitive data such as PII or PHI and prevent unauthorized transmission to public or unsanctioned AI tools.
- Prompt injection and AI abuse prevention: Detect and block malicious prompts designed to manipulate AI behavior or compromise workflows.

"AI is now mainstream for SMBs, with over half using AI tools, led by marketing and sales seeking scale, productivity, and efficiency," said Matthew Ball, Chief Analyst at Omdia. "While most adoption runs through SaaS, growing use of consumer AI, sanctioned or not, generates new security risks that create new requirements for MSPs to actively manage."

As AI continues to evolve, Acronis plans to introduce additional AI-powered capabilities to protect, manage, and automate AI services and tools within its broader Cyber Workspace offering. These enhancements are designed to boost productivity and automation, enabling MSPs to streamline day-to-day operations while strengthening data and asset protection.

LEAP

INTO NEW WORLDS

YOU'RE ONE LEAP AWAY

From 31 Aug - 3 Sept 2026

Riyadh Exhibition and Convention Center - Malham, Saudi Arabia

SECURE YOUR PASS NOW

IDENTITY TAKES CENTRE STAGE AS AI, MACHINE IDENTITIES REDEFINE SECURITY

IDENTITY MANAGEMENT HIGHLIGHTS HOW CREDENTIAL ABUSE, AI AGENTS, AND NON-HUMAN IDENTITIES ARE RESHAPING CYBER RISK AND FORCING ORGANISATIONS TO RETHINK ACCESS CONTROL.

Identity Management Day, observed annually on April 14, has evolved into a critical moment for organisations to reassess how they secure the very foundation of digital trust: identity. Originally launched to raise awareness around identity governance, access control, and cybersecurity best practices, the day was established by industry leaders to address one of the most persistent gaps in enterprise security: mismanaged identities and excessive access privileges.

In 2026, its relevance has expanded significantly. Identity is no longer limited to human users; it now encompasses a rapidly growing universe of machine identities, AI agents, and autonomous systems that operate continuously and at scale. This shift has transformed identity into the central control plane of modern enterprises—linking users, applications, data, and infrastructure across cloud, SaaS, and hybrid environments.

Industry consensus underscores a clear reality: attackers are no longer primarily breaking into systems—they are logging in. Credential abuse, phishing, and the exploitation of privileged access have become dominant attack vectors, often enabling large-scale breaches from a single compromised identity. At the same time, organisations are accelerating AI adoption faster than they can govern access, creating what experts describe as an "AI identity paradox."

Identity Management Day serves as a vital reminder that security must move beyond static, human-centric models. Principles such as least privilege, just-in-time access, continuous verification, and behavioural context are no longer optional—they are essential. More importantly, they must be extended to non-human identities with the same rigour as human users.

Ultimately, Identity Management Day 2026 is not just about awareness—it is about redefining accountability in a digital world where trust is constantly tested. In an era where identities outnumber humans exponentially and operate at machine speed, securing identity is no longer a function of IT—it is the cornerstone of resilience, continuity, and business survival.

Sandhya D'Mello, Technology Editor, CPI Media Group, spoke with leading industry experts across cybersecurity and identity management, capturing insights from organisations at the forefront of securing digital ecosystems. The collective views highlight a clear and urgent shift: identity is no longer just an IT function, but the core control layer of modern enterprise security. From the rise of AI-driven identities and autonomous agents to the growing sophistication of credential-based attacks, these experts underscore the need for organisations to rethink how identity is governed, monitored, and protected in an increasingly complex threat environment.

Morey Haber, Chief Security Advisor, BeyondTrust

Identity Management Day is no longer solely about humans and the accounts that represent our digital personas. It has evolved into managing identities that do not sleep, have no morals, ethics, or understand risk in the form of fear, pain, or anxiety. AI agents, and complete systems that form Agentic AI, introduce autonomous decision making tied directly to privilege identities and accounts operating on behalf of human users. Without privileged centric identity controls, these AI agents represent an emerging risk surface that can be operated and compromised at machine speed. Least privilege, just in time access, ephemeral secrets, and continuous verification are no longer just best practices for humans; they must be incorporated into the workflows for every agentic AI implementation. They are absolutely essential requirements, based on secure by design principles. Identity Management Day gives us a perfect opportunity to raise awareness of this and ensure that every organisation considers AI agent identity security as a part of current and future deployments. If you do not govern non-human identities, including agentic AI, with the same rigour as human privileged users, you are not managing identities. You are delegating trust without accountability, and the risks will become breaches if not managed from the start.

Santiago Pontiroli, Lead TRU Researcher at Acronis

Identity has quietly become the easiest way in for attackers. In 2025, more than half of attacks against service providers started with phishing, and instead of breaking systems, attackers are increasingly logging in using stolen or bought access. This shift is visible across major campaigns where ransomware groups combined vulnerabilities with credential abuse to steal data at scale.

At the same time, a full underground economy has formed around identity. Access brokers are selling VPN, RDP, and corporate credentials harvested by information stealers such as Lumma and RedLine. These stealers quietly collect passwords, cookies, and session tokens, which are then resold to ransomware groups as ready-made entry points. Incidents like the Handala hack show how identity compromise is no longer just the first step, but the core of the attack itself.

As we continue through 2026, this trend is accelerating, with attackers targeting SaaS admin accounts and even machine identities, while using AI to scale phishing and impersonation.

Identity has become the primary attack surface, and defending today is no longer about protecting the perimeter alone, but continuously verifying who and what is accessing your systems.

Vibin Shaju, Vice President, EMEA Solutions Engineering, Trellix

Identity has become the defining control point of the cloud era. As organisations expand across cloud, SaaS, and hybrid environments, identity is now what connects people, applications, and data, making it central to how modern businesses operate and scale. Insights from Trellix Threat Research show that attackers are increasingly targeting this layer, not by breaking systems, but by exploiting trust, focusing on credentials, access pathways, and high-value cloud accounts. Identity-based incidents can scale massively from a single user compromise, exposing millions of records. This reflects a broader shift in which the misuse of legitimate access can be just as impactful as traditional breaches, and are often harder to detect. At the same time, leaders are being asked to balance speed, openness, and security in environments where identity is constantly in motion. A proactive cybersecurity strategy is successful here. Trellix brings together identity signals across endpoint, cloud, email, and network for a unified view of risk, applying AI and threat intelligence across the dataset, so organisations can better identify abnormal behaviour, detect misuse of access, and respond faster when trust is compromised.

On Identity Security Day, the message is clear: identity is no longer just about managing access; it is fundamental to trust, resilience, and continuity.

Ezzeldin Hussein, Regional Senior Director, Solution Engineering, META, SentinelOne

We keep in mind that identity is the fundamental perimeter that needs to be safeguarded on Identity Management Day. It is now more than just a defensive layer. As the region undergoes escalations, the attack surface has expanded to digital environments, making both machine and human identities targets for rapid disruption. Attackers take advantage of hurry, worry, and attention. They log in rather than breaking in. Our ideas should grow as the attack surface does, which means that simply protecting infrastructure alone is insufficient. To preserve identity protection, we must continuously verify who has access to what, why, and under what circumstances. This requires AI security, which can adapt and identify even slight changes in behavior before they become security breaches.

This is more about accountability than technology. Every identity represents a person, a purpose, or the continuity of a country. During uncertain times, protecting one's identity becomes a resilient act that guarantees the continuation of daily activities, vital infrastructure, and services. In this field where real-world conflicts are driving change, identity security is important for stability, trust, and sovereignty. Protecting identity now, particularly during tense times, ensures continuity and, ultimately, safeguards the future.

Jay Reddy, Head of growth, ManageEngine

The identity landscape has outgrown what static models were built to secure. Identity risk is now continuous, expanding and increasingly autonomous. It sits at the center of every security decision an organisation makes. The way we manage identities has evolved from a perimeter-bound discipline into an intelligent, context-aware fabric that must synthesise risk signals, behavioral patterns, and business context in real time.

Non-human identities (NHIs) and AI agents proliferating across organisations faster than governance models can account for, has led to the rise of ungoverned identities with legitimate credentials, operating at machine speed inside the environment. The identity intelligence deficit we face today is not just a shortage of skilled professionals. It is the growing gap between the pace at which AI agents operate autonomously and governance frameworks that were built around human behavior.

Every AI agent must be treated as a distinct identity and tied to an accountable human. The principles that define mature identity programs, least privilege, just-in-time access, and zero trust remain the foundation. But they must now extend systematically beyond human identities to every service account, certificate, token and API in the environment, subject to continuous monitoring, access reviews, and time-bound credentials. The questions of "Where are my identities? What can they access? What should they be permitted to do?" remain unchanged. The ability to answer that continuously, across every identity in the environment, is now a defining capability for resilience.

Mortada Ayad, VP – META, Delinea

Identity Management Day is a timely moment to reflect on a space that is at a critical inflection point. Today's enterprise environments are awash with AI agents and other non-human identities. These entities are always on, highly capable, and deeply embedded in critical workflows. Yet despite this, they continue to be treated as tools, rather than the privileged identities they effectively are. This is the 'AI security paradox': organisations are scaling AI adoption faster than they can govern who, or what, has access to what. We cannot, and should not, put AI back in the bottle. But we must evolve identity management beyond static, standing access models towards approaches that are dynamic, contextual, and responsive. Access decisions must account not just for identity, but for behaviour. If we continue to rely on frameworks designed for humans alone, they will increasingly fail in the reality where machines outnumber humans by over 40,000 to 1.

Victor Garcia, Field CISO Associate, Sophos

The key takeaway is clear: identity is now the primary security perimeter. Attackers are no longer breaking in—they are logging in, as mentioned in the report "who needs CVEs and exploits to get in when you have got passwords?". When identity is compromised, trust is automatically granted, making identity protection the foundation of modern cybersecurity. During reported breaches due to credential compromise, credentials were not stolen once they were reused everywhere

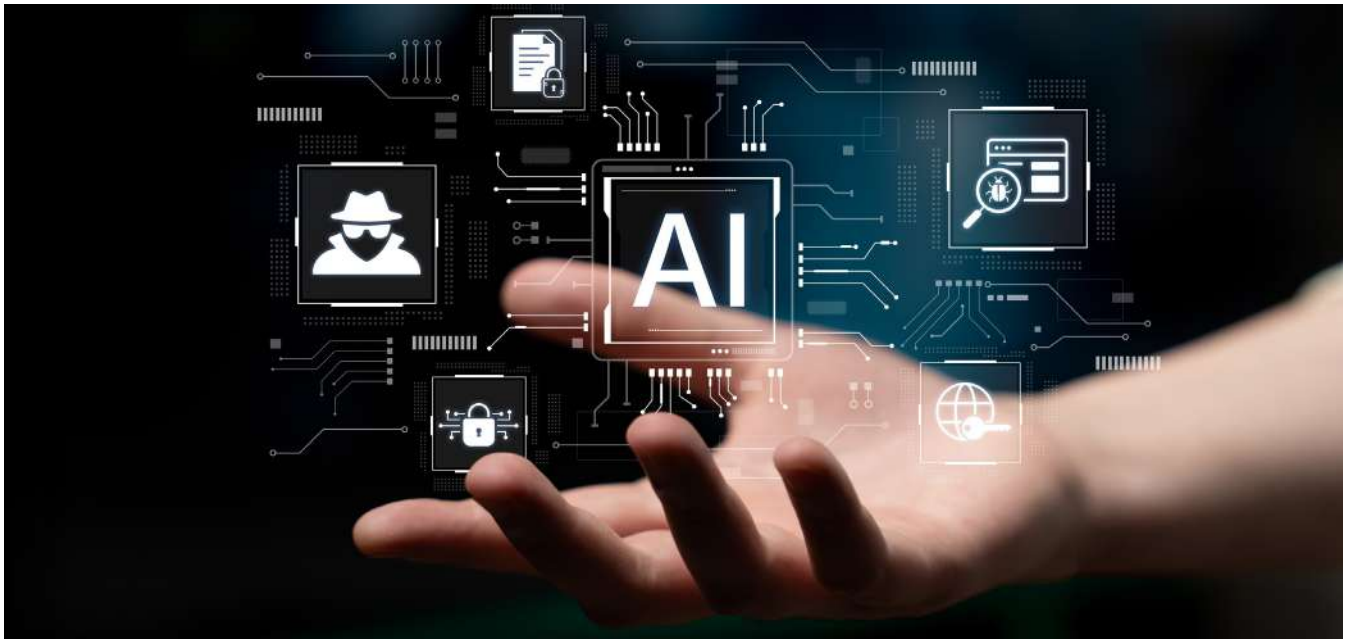
What makes this shift more critical is how invisible these attacks have become. With stolen credentials and authentication abuse, malicious activity often looks like normal user behavior. This means organisations must move beyond basic login controls and adopt continuous identity verification based on context, behavior, and risk, moving toward a more preventive approach: monitoring user fingerprints, removing dormant accounts, conducting posture checks, and monitoring for leaked credentials on the deep web and dark web.

Speed is also a defining factor. Attackers can escalate privileges and target core identity systems within hours, leaving little room for delayed response.

Strong identity controls—like least privilege, rapid session revocation, and tight access governance—are essential to contain threats before they spread.

Identity Management Day also highlights a persistent gap: identity controls are often deployed but not fully enforced. Inconsistent MFA and weak privileged access management continue to create avoidable risk. Effective identity security requires full coverage, strong authentication methods, and disciplined execution.

Ultimately, identity is the control plane of cybersecurity. Organisations that prioritize resilient identity systems and real-time visibility will lead in defense. Those that don't will continue to face breaches that are quiet, fast, and difficult to detect.



tahawultech.com

Women in TECHNOLOGY FORUM AND AWARDS

Give to gain. Powering women in tech

Gala Dinner Event

May 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/

BACKUP AND SECURITY ARE POWERING BUSINESS RESILIENCE IN MIDDLE EAST

ORGANISATIONS NEED CLARITY ON WHAT DATA EXISTS, HOW IT IS USED, AND WHAT RECOVERY EXPECTATIONS APPLY.

IDC's Global DataSphere Forecast estimates that global data volume will surge to 393.9 zettabytes by 2028. This growth puts business continuity, data protection, governance, and the cost of sustaining them under greater pressure. This turns resilience into an AI economics issue, where every additional dataset retained and protected compounds spend across storage, backup operations, compliance overhead, and downstream AI quality and remediation. In the UAE, this challenge is driving both government and enterprise efforts to harness data growth for AI innovation, while strengthening data sovereignty and secure digital infrastructure.

The World Backup Day reminds us that the real question is not whether organisations are backing up more data or adding more cloud security controls. It is whether those investments are improving business resilience in a way that is economically sustainable. Backup cannot be treated as an insurance policy that simply expands indefinitely. Without clear retention policies and strong governance, data resilience programs become financially draining, operationally burdensome, and harder to justify. The priority should be protecting the right data, at the right level, for the right recovery outcomes when disruption hits.

Carolyn Duby, Field CTO and Cyber Security GTM Lead, Cloudera.

Governance is what makes resilience targeted, not indiscriminate

According to a report by PwC, 55% of respondents in the Middle East prioritise digital and technology risk mitigation over the next 12 months, compared to 53% globally.

Understanding the data estate is where effective data resilience begins. Organisations need clarity on what data exists, how it is used, and what recovery expectations apply. Without that visibility, everything tends to be treated as equally critical, which quickly leads to oversized backup environments and unclear recovery priorities.

Governance provides the structure that allows organisations to prioritise protection. When datasets are classified according to business impact, protection levels can be tiered accordingly. Other datasets may be protected through lower-cost approaches or retained for shorter periods.

Determining what is critical is not purely a technical exercise. It depends on business commitments and the consequences of disruption, such as regulatory penalties, contractual obligations, operational risk or reputational damage. When organisations frame resilience decisions through the lens of governance, protection and retention become deliberate choices aligned to business risk rather than default IT configurations.

Stop paying twice for bad data

When governance priorities are unclear, many organisations default to keeping and backing up data "just in case." Over time, that approach creates large volumes of information that provide little operational value.

Research from the Veritas Global Databerg Report suggests that up to 85 percent of stored data may be dark or redundant, obsolete or trivial (ROT). Yet organisations still store and protect this data, expanding backup sets and increasing recovery complexity. Larger backup environments require more data to be validated and restored before trusted operations can resume. The impact extends beyond infrastructure costs.

In organisations adopting AI-driven workflows, the consequences may be magnified. Poorly governed data often flows directly into analytics pipelines and AI models, introducing noise and reducing reliability in the insights. The result is a cycle where organisations "pay twice" by investing resources to store and protect low-value data, and then investing again to correct the problems that data creates in downstream systems.

Recovery testing proves governance decisions work in production

Governance strategies only matter if they produce reliable recovery outcomes. Regular restore and disaster recovery testing validates whether protection tiers actually match business priorities. These tests often surface critical insights, such as data that was backed up but did not contribute to recovery, or systems that require stronger protection than originally assumed. They can also expose hidden dependencies across data pipelines, where data lineage helps teams restore in the right order to resume trusted operations without restoring everything.

Leaders can track a small set of indicators to maintain focus. These include whether disaster recovery plans are tested regularly, whether recovery time objectives are clearly defined, whether tests consistently meet those objectives, and what improvements are implemented after each cycle.

Over time, this creates a feedback loop that strengthens governance. Insights from recovery testing inform cleanup efforts, policy updates, and operational improvements, helping organisations keep backup environments efficient and aligned with business needs.

Reducing data sprawl prevents resilience costs from compounding

In hybrid and multi-cloud environments, uncontrolled replication increases the volume of data that is secured, governed, and backed up. This adds to the total cost of AI adoption when data spreads across too many systems, copies, and unmanaged pathways.

That is why data movement into third-party SaaS platforms and external services should be treated as a deliberate governance decision, not a convenience. Once data leaves managed environments, visibility drops, controls become harder to enforce, and recovery becomes more difficult to coordinate.

Consistency across environments matters just as much. On-premises and cloud platforms need to be governed in the same manner to avoid managing and protecting data in fragmented ways that may encourage duplicate datasets and bloated backup environments. Open standards such as the Iceberg REST Catalog protocol can help by improving interoperability across engines and catalogs, reducing the need to create extra copies simply to make data usable across platforms.

The result is fewer duplicates, clearer ownership and retention, and a smaller, cleaner backup footprint that is easier to govern and manage, and costs less to maintain.

What leaders should take away

World Backup Day should be a reminder for businesses in the UAE that resilience in modern enterprises is not about creating more copies of everything or piling on controls. It is about making intentional, governed decisions so organisations avoid carrying an ever-expanding bill for data that is redundant, obsolete, trivial, or simply unknown.

Governance is the mechanism that optimises backup spend, shortens recovery, and improves AI reliability. With this, companies will stop paying premium prices to protect data they did not understand, did not need, or should not have kept in the first place.

CYBERWAR AT FRONT LINE: WHY ENTERPRISES MUST PREPARE FOR DIGITAL CONFLICT

ORGANISATIONS THAT RUN CLOUD PLATFORMS, DIGITAL SERVICES, SUPPLY CHAINS, AND COMMUNICATION INFRASTRUCTURE SIT AT THE CORE OF MODERN ECONOMIES.

Geopolitical conflict is no longer confined to land, sea, or air. Today, it unfolds silently across networks, servers, and endpoints. Governments, critical infrastructure operators, and private enterprises are increasingly targeted by cyber operations designed to disrupt services, steal sensitive data, or undermine national stability.

Unlike traditional warfare, cyberwarfare does not require armies crossing borders. A coordinated attack launched from anywhere in the world can disrupt supply chains, shut down utilities, or expose millions of customer records within minutes. From ransomware attacks on healthcare systems to disruptions in logistics and satellite communications, organisations across sectors have faced outages, financial loss, and reputational damage. As organisations digitise operations and connect critical systems to the internet, the line between national security and enterprise cybersecurity continues to blur.

Rise of cyberwarfare

According to the European Union Agency for Cybersecurity's 2025 Threat Landscape report, the global cyberthreat environment is shaped primarily by state-nexus actors and organised cybercriminal groups, with increasing convergence in their tools, tactics, and objectives alongside the growing professionalisation of cybercrime and its alignment with geopolitical dynamics.

Critical infrastructure sectors, such as energy, transportation, finance, and telecommunications, have emerged as primary targets for these attacks. Disruptions in these areas can trigger significant economic damage and widespread societal impact, making them especially attractive to threat actors.

In 2026, geopolitical dynamics continue to be the leading influence on cyber risk strategies. According to the World Economic Forum, 64% of organisations now factor geopolitically driven cyberthreats into their security strategies, while 23% of public sector organisations report insufficient cyber resilience capabilities.

THE USE OF DISRUPTIVE MALWARE IN ENTERPRISE ENVIRONMENTS HIGHLIGHTS THE POTENTIAL FOR EVEN BROADER OPERATIONAL FALLOUT.

Why enterprises are in the crosshairs

Enterprises are no longer incidental casualties; they are deliberate targets in cyberwarfare. Organisations that run cloud platforms, digital services, supply chains, and communication infrastructure sit at the core of modern economies, making them high-impact points of disruption.

Recent developments have already validated this shift toward physical targeting of enterprise infrastructure. In early 2026, drone strikes on commercial cloud data centers in the Middle East caused structural damage and triggered widespread service disruptions across dependent digital services. These incidents marked one of the first clear instances of data centers being directly targeted in kinetic conflict, highlighting their growing role as strategic assets. The outages extended beyond the immediate blast radius, affecting critical sectors reliant on cloud infrastructure and exposing how modern conflict increasingly focuses on the core infrastructure of the digital economy.

This strategy is not limited to physical attacks. Supply chain compromises further amplify impact by exploiting trust at scale. By infiltrating a trusted enterprise platform, attackers can scale their reach exponentially across downstream organisations. Incidents such as the Sunburst supply chain attack demonstrated how deeply embedded

trust relationships can be exploited, turning widely used software into vectors for national security compromise.

The use of disruptive malware in enterprise environments highlights the potential for even broader operational fallout. Wiper malware outbreaks mimicking NotPetya have crippled global shipping, manufacturing, and commerce, disrupting essential supplies and proving that the consequences extend far beyond the initial target.

What makes these attacks particularly effective is the structure of modern enterprises themselves. Deep interdependencies, reliance on shared platforms, legacy systems, and limited visibility across complex environments create ideal conditions for attackers to move quickly, amplify impact, and align cyber operations with broader geopolitical objectives.

Cybersecurity priorities in a geopolitically volatile time

As cyberwarfare becomes a permanent feature of the geopolitical landscape, organisations must rethink how they approach security. Cybersecurity can no longer be treated solely as an IT function; it must be embedded into enterprise risk management and business strategy.

Adopt a risk-based security approach: Align cybersecurity priorities with business-critical assets and evolving threat landscapes to focus efforts where impact is highest.

Ensure leadership and board-level alignment: Make cybersecurity a strategic priority with clear governance, executive ownership, and regular oversight at the leadership level.

Strengthen identity, endpoints, and visibility: Enforce least-privilege access, strong authentication, and continuous monitoring while securing endpoints and leveraging threat logs for faster detection and response.

Promote a security-first culture: Build organisation-wide awareness through regular training, ensuring employees act as the first line of defense.

Shobana Sruthi Mohan, Enterprise Analyst, ManageEngine.

Enhance resilience through testing and response readiness: Continuously test defenses, maintain robust incident response plans, and ensure rapid recovery to minimise disruption.

Preparing for sustained digital conflict

Cyberwar is no longer a distant, theoretical threat; it is an active and evolving reality shaping how nations and businesses operate. In a world where attacks can be swift, borderless, and strategically motivated, preparedness becomes a competitive advantage. Organisations that embed security into their core strategy by anticipating risks, strengthening resilience, and fostering a culture of vigilance will be far better positioned to withstand and recover from disruption.

Ultimately, the question is no longer if enterprises will be impacted by cyber conflict but when. Those that act now will not only defend against emerging threats but also build the trust and reliability required to thrive in an increasingly volatile digital landscape.

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

UNLIKE TRADITIONAL IT MONITORING, ICS MONITORING FOCUSES ON ICS PROTOCOLS AND OPERATIONAL INTERACTIONS.

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.

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

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.

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 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.

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

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.

ONLY 5% OF ORGANISATIONS HAVE FULL TRUST IN THEIR CYBERSECURITY VENDORS

LACK OF VERIFIABLE TRANSPARENCY UNDERMINES CYBERSECURITY DECISION MAKING, ACCORDING TO SOPHOS-BACKED RESEARCH.

Sophos, a global leader of innovative security solutions for defeating cyberattacks, today released findings from a global, vendor-agnostic study (based on responses from 5,000 organisations across 17 countries), examining one of cybersecurity's most urgent and overlooked necessities: trust.

The Cybersecurity Trust Reality 2026 report is one of the most comprehensive studies of trust in cybersecurity and the impact on operational risk and board-level decision making. It reveals a critical challenge facing CISOs: Trust in cybersecurity vendors is fragile, difficult to measure, and increasingly shaping risk posture at both operational and board levels.

At a time of relentless cyber threats, heightened regulatory scrutiny, and accelerating AI adoption, trust has become a defining factor in cybersecurity decision-making. Yet new research reveals that nearly all organisations report lacking full confidence in their cybersecurity vendors, and many struggle to assess vendor trustworthiness in the first place.

The independent study found that:

- 95% of respondents said they do not have full trust in their cybersecurity vendors
- 79% struggle to assess the trustworthiness of new cybersecurity partners, and over six in ten (62%) even find it challenging for their existing vendors
- More than half (51%) report increased anxiety about the likelihood of a significant cyber incident as a direct result of lack of trust

These findings underscore a critical reality: cybersecurity effectiveness cannot be measured by technological performance alone, but also by the confidence that organisations have in the partners defending their business.

TRUST IS NOT AN ABSTRACT CONCEPT IN CYBERSECURITY, IT'S A MEASURABLE RISK FACTOR.

For CISOs, trust gaps create operational friction, slower decision-making, and higher vendor turnover. Trusted cybersecurity partners reduce risk and build more resilient organisations.

"Trust is not an abstract concept in cybersecurity, it's a measurable risk factor," said Ross McKerchar, CISO at Sophos. "When organisations can't independently verify a vendor's security maturity, transparency, and incident handling practices, that uncertainty flows directly into boardrooms and security strategies."

The survey identifies verifiable security artifacts, including independent assessments, certifications, and demonstrated operational maturity, as the single greatest driver of vendor trust. CISOs prioritise transparency during incidents and consistent technical performance, while boards and senior leadership place greater weight on independent validation, certifications, and analyst performance.

The common thread is clear. Organisations want transparency backed by evidence, not blanket assurances.

"With regulatory pressure increasing globally, organisations must be able to

Ross McKerchar, CISO, Sophos.

demonstrate due diligence in vendor selection — especially where AI is involved," said Phil Harris, Research Director, Governance, Risk and Compliance Solutions at IDC. "Trust is shifting from a marketing message to a defensible compliance requirement."

As artificial intelligence becomes embedded in cybersecurity tools, services, and workflows, organisations are not only evaluating whether security solutions are effective, but whether AI is deployed responsibly, transparently, and with appropriate governance. Trust is no longer optional. It is foundational.

"CISOs are being asked to prove trust, not assume it," added McKerchar. "Cybersecurity providers must do the same. Respondents to the survey cited a lack of accessible, sufficiently detailed information as the primary barrier to making confident trust assessments. Trust must be earned continuously through transparency, accountability, and independent validation."

These findings elevate trust from a brand attribute to a strategic imperative.

At Sophos, building and maintain that trust is foundational. Through the company's Trust Center, Sophos aims to help security leaders make faster, more defensible decisions in an increasingly hostile threat landscape.

VEEAM REPORT HIGHLIGHTS SHIFT TO PROVEN DATA RESILIENCE AMID RANSOMWARE AND AI RISKS

NEW VEEAM DATA TRUST AND RESILIENCE REPORT FINDS 90% OF SECURITY LEADERS BELIEVE THEY CAN RECOVER QUICKLY BUT ONLY 28% FULLY RESTORE DATA AFTER A RANSOMWARE ATTACK.

Veeam Software recently released the Data Trust and Resilience Report 2026, revealing a growing disconnect between how confident organisations feel about cyber resilience and the reality of recovery outcomes. As ransomware, regulatory pressure, and AI-driven data risk grow, even mature organisations are finding that confidence in recovery and proof of recovery are fundamentally different capabilities.

The Veeam Data Trust and Resilience Report 2026, based on insights from more than 900 senior IT, security and risk leaders worldwide, found that while 90% of organisations express confidence in their ability to recover from a cyber incident, fewer than one in three ransomware victims fully recovered their data. On average, organisations recovered just 72% of affected data following a ransomware attack.

"Confidence in recovery from a ransomware attack is high, but the data tells a different story – and AI is only widening that gap," said Anand Eswaran, Chief Executive Officer (CEO) at Veeam. "Even the most sophisticated organisations are discovering that confidence in recovery and proof of recovery are fundamentally different capabilities. Data resilience is still the hard requirement: knowing what data you have, where it lives, who can access it, and proving you can restore clean, trusted data fast when attackers – or operational failures – put the business under pressure. The infrastructure for deploying AI has rapidly outpaced the ability to secure it. Organisations need end-to-end capabilities to understand, secure, protect, govern and ensure their data is resilient at machine speed."

"Veeam is redefining data resilience for the agentic era, where AI agents, apps, and data move faster than traditional controls. Our unified trusted platform, strengthened by our recent acquisition of Securiti AI, delivers the visibility, precision, and trust required to operationalise resilience so businesses can adopt AI safely without compromising recovery, compliance, or continuity. The organisations that will lead tomorrow are those proving trust, not just believing in it – and this is the new standard Veeam is setting for the industry."

EVEN THE MOST SOPHISTICATED ORGANISATIONS ARE DISCOVERING THAT CONFIDENCE IN RECOVERY AND PROOF OF RECOVERY ARE FUNDAMENTALLY DIFFERENT CAPABILITIES.

Key Findings: Confidence Is High, But There's a Critical Shift from Confidence to Proven Recovery

The 2026 report highlights why "recovery confidence" must be paired with validated recovery capabilities and measurable outcomes:

- 90% say they're confident they can recover from a cyber incident within RTOs yet only 69% say RTOs are fully aligned with business continuity goals.
- Among organisations hit by ransomware where operations or data were affected, only 28% fully recovered all affected data; 44% recovered less than 75%.
- Among organisations that experienced a cyber incident, 42%

reported customer/constituent disruption, 41% reported financial loss or revenue impact, and 38% reported extended downtime of critical systems.
- Regulation is becoming a core resilience driver as 33% cite regulatory shifts as a top emerging threat—nearly matching cyberattacks (36%).

AI Is Moving Faster Than Governance – and Increasing Data Exposure

As AI shifts from experimentation to execution, the report shows many organisations are struggling to maintain visibility and control over data flows across apps, clouds, and third party services.

- 43% say AI adoption is outpacing their ability to secure data and models.
- 42% report limited visibility into all AI tools or models used across the organisation.
- 40% say security policies have not yet been updated to address AI specific risks.
- 25% say shadow IT and unauthorised AI tool usage are a primary concern related to employee AI tool use and data security.

What Separates Stronger Recoveries: Four Practices That Matter

Across industries and maturity levels, the report identifies four capabilities consistently linked to stronger outcomes:

1. Clear visibility into enterprise data and AI risk in production and in backup data.
2. Enforced security controls (not policy alone).
3. Proven recovery through realistic testing and validation.
4. Executive alignment on ownership, reporting, and "what recovered means."

One clear signal of moving from intent to execution: organisations with enforceable controls such as data loss prevention (DLP) reported measurably better visibility and less security lag as AI usage expands.

Anand Eswaran, Chief Executive Officer (CEO) at Veeam.

Budgets, Metrics and Measured Readiness Drive Better Outcomes

The report also finds that resilience improves when readiness becomes measurable, and leadership sees risk in business terms:

- 49% increased cybersecurity budgets year-over-year.
- Organisations with budget increases were more likely to invest in resilience fundamentals like immutable storage and automated backup – and reported better ransomware outcomes.
- Full recovery was significantly higher among organisations reporting increased budgets (40% vs. 16%).

The report underscores a pivotal reality for business leaders: AI is amplifying both opportunity and operational exposure, and recovery plans must evolve beyond assumptions. Data trust isn't a statement – it's a capability proven through controls, clarity, and clean recovery.

BEYONDTRUST'S 13TH ANNUAL MICROSOFT VULNERABILITIES REPORT REVEALS DROP IN TOTAL VOLUME, BUT SURGE IN CRITICAL RISK

BeyondTrust, the global leader in privilege-centric identity security protecting Paths to Privilege, has released the 13th edition of its annual Microsoft Vulnerabilities Report, revealing a critical shift in the vulnerability landscape: while total vulnerability volume appears to be stabilising, critical vulnerabilities have surged, indicating severity and exploitability of vulnerabilities are rapidly increasing.

The report, which provides an in-depth analysis of data from publicly issued Microsoft security bulletins published throughout 2025, highlights a shifting risk profile driven by AI-accelerated vulnerability discovery, expanding cloud adoption, and increasingly sophisticated attacker strategies targeting identity and privilege.

"Don't be distracted by the dip in total vulnerabilities. Critical vulnerabilities doubled. This is a warning that risk is not decreasing, it is concentrating, and it is concentrating around privilege. Elevation of Privilege made up 40% of all vulnerabilities again this year because that is exactly what attackers need to reach critical systems." said James Maude, Field CTO at BeyondTrust.

"A ninefold increase in Azure and Dynamics 365 critical vulnerabilities shows where that concentration is happening.

James Maude, Field CTO at BeyondTrust.

Combined with the rising tide of identity compromise attacks that exploit standing privilege, patching alone will not close this gap. The organisations that weather this are the ones treating every vulnerability and identity, human or machine, as a potential path to privilege in their most critical systems, and shrinking those paths before an attacker reaches them."

Key Highlights from the Report: A Surface-Level Decline Masks a Deeper Shift in Risk

Microsoft reported 1,273 total vulnerabilities, a 6% decrease from 1,360 in 2024

At first glance, this decline suggests improvement, potentially reflecting Microsoft's continued investment in

security is maintaining control, despite a rapidly expanding attack surface. However, it may also indicate that traditional vulnerability tracking is no longer capturing the full picture, particularly as AI-driven systems, non-human identities (NHIs), and complex cloud architectures introduce risks that don't always map cleanly to CVEs.

At the same time:

- Critical vulnerabilities doubled year-over-year, rising from 78 to 157, reversing a multi-year downward trend.
- Elevation of Privilege (EoP) vulnerabilities accounted for 40% (509) of all reported vulnerabilities, reinforcing their role as the most direct path for attackers to escalate access, move laterally, and compromise critical systems, and underscoring the continued importance of identity and privilege in modern attack chains.

Cloud and Enterprise Platforms Drive Critical Risk Expansion

The report found sharp increases in critical vulnerabilities across key Microsoft platforms that had previously seen declining vulnerability activity:

- Microsoft Azure and Dynamics 365 experienced a 9x increase in critical vulnerabilities, rising from 4 to 37
- Microsoft Office vulnerabilities surged to 157, more than tripling year-over-year
- Critical vulnerabilities in Office increased 10x, signaling heightened risk in widely used productivity tools

While critical risk surged across cloud and enterprise platforms, other areas showed signs of improvement:

- Microsoft Edge vulnerabilities dropped significantly to 50 in 2025, an 83% decrease year-over-year

Security Takeaways:

- AI is changing the vulnerability equation — AI is accelerating discovery for defenders, while also enabling attackers to analyse patches, reverse engineer fixes, and operationalise exploits faster than ever. This creates a widening gap between vulnerability disclosure and exploitation, where organisations may be exposed before traditional defenses can respond.
- Hear from experts why CVE counts no longer tell the full story — Emerging risks, such as over-privileged AI agents, long-lived machine credentials, and identity misconfigurations, often do not appear in CVE counts, despite carrying significant impact, meaning traditional vulnerability tracking is no longer capturing the full picture.

Key Priorities for Organisations:

- Patch faster—but assume compromise is still possible
- Apply least privilege to limit the blast radius of an attack and create opportunities for detection and response
- Adopt identity-first security strategies that secure all identities, human and non-human
- Focus on paths to privilege, not just individual vulnerabilities

ELEVATION OF PRIVILEGE MADE UP 40% OF ALL VULNERABILITIES AGAIN THIS YEAR BECAUSE THAT IS EXACTLY WHAT ATTACKERS NEED TO REACH CRITICAL SYSTEMS.

DEEPFAKE FRAUD SURGES AND ONLY 7% OF ORGANISATIONS ARE FIRMLY READY

GLOBAL SURVEY FINDS ORGANISATIONS UNDER-EQUIPPED AS AI-CHARGED THREATS ESCALATE ACROSS INDUSTRIES

Abed Hamandi, Senior Director, EMEA Consulting, Fraud and Security Intelligence Practice, SAS.

Fraudsters are rapidly weaponising AI, while organisations are struggling to keep pace. New fraud research by the Association of Certified Fraud Examiners (ACFE) and data and AI leader SAS reveals that only 7% of anti-fraud professionals believe their organisations are more than moderately prepared to detect or prevent AI-fuelled fraud. The findings come as criminals exploit inexpensive and widely available AI tools to scale social engineering schemes, digital forgery and consumer scams to record highs.

The 2026 Anti-Fraud Technology Benchmarking Report – the fourth installment in a research series debuted by the ACFE and SAS in 2019 – is based on a survey of 713 fraud fighters across eight regions worldwide.

"The data paints a worrisome picture: fraud is evolving faster than most organisations can defend against it," said John Gill, J.D., CFE, President of the ACFE. "AI-powered threats aren't on the horizon – they're already here, and they're accelerating quickly. The profession has made real strides in adopting AI, but this report is a wake-up call. Organisations that don't strengthen their defenses against AI-charged fraud risk as others do will become bigger targets."

As fraud risk rises globally, the UAE and Saudi Arabia are uniquely positioned to lead the next generation of fraud prevention. Strong regulatory alignment, government-led digital transformation, and modern financial infrastructure give both markets a structural advantage. With central banks CBUAE and SAMA acting as ecosystem orchestrators, the region has a rare opportunity to leapfrog legacy approaches and move directly to supporting a secure, seamless, and future-ready financial ecosystem.

"Few regions combine high

growth with such strong regulatory leadership," said Abed Hamandi, Senior Director, EMEA Consulting, Fraud and Security Intelligence Practice, SAS. "The UAE and Saudi Arabia are not constrained by legacy in the same way as many mature markets. By embracing real-time, AI-driven, and identity-centric fraud prevention, they can stop fraud before it happens, while delivering the low-friction customer experiences that modern digital economies demand."

Industries at a crossroads – and in the crosshairs

Respondents represent more than a dozen industries, most prominently government and public sector (26%) and banking and financial services (23%), alongside meaningful participation from professional services, manufacturing, insurance, technology, education, energy and health care. Survey insights reveal that:

- Fraudsters are winning the AI race. Every AI-powered fraud modality examined has risen over the past two years, according to the anti-fraud professionals surveyed. Deepfake social engineering saw the sharpest surge, with 77% of respondents reporting a slight-to-significant increase – followed closely by consumer fraud/scams (75%), generative AI document fraud/forgery (75%) and deepfake digital injection (72%). Looking ahead, 55% expect deepfake social engineering and GenAI document fraud/forgery to increase significantly over the next 24 months.
- AI and machine learning (ML) adoption are accelerating but remain far from ideal. One-quarter of organisations (exactly 25%) now use AI/ML in their anti-fraud programs, according to respondents, up from 18% in 2024. Another 28% expect to adopt it by 2028. For organisations still on the sidelines, the window to build AI competency before competitors and criminals widen the gap is narrowing fast.
- Governance lags dangerously behind AI adoption. Nearly nine in 10 (86%) organisations rate accuracy of results as important or very important in adopting GenAI, yet less than one in five (18%) respondents say their organisation tests AI models for bias or fairness. Similarly, 82% say explainability is important, but just 6% feel completely confident explaining how their AI/ML models make anti-fraud decisions. For banks, insurers and other regulated entities in particular, deploying AI in this manner risks regulatory consequences and legal liability on top of reputational damage.
- Budgets are growing – but so are constraints. More than half of respondents (55%) expect their organisations to increase their anti-fraud technology budgets over the next two years. Even so, budgetary and financial restrictions remain the leading barrier to implementation, cited as a major or moderate challenge by 84% of respondents.

Emerging tech: Promise, progress and the cost of waiting

Physical biometrics, agentic and generative AI – and yes, even quantum AI – the technologies transforming the war on fraud are maturing rapidly. But fraudsters' readiness to exploit them is advancing in parallel, and bad actors have a tremendous advantage.

"Cybercriminals don't have governance committees, and they don't wait for budget cycles or regulatory clarity – they just act," said Stu Bradley, Senior Vice President of Risk, Fraud and Compliance Solutions at SAS. "Every quarter business leaders spend evaluating a technology is another quarter lawbreakers get to weaponise it and find organisations underprepared."

The question isn't whether to adopt anti-fraud innovations, but rather, can organisations afford to wait? The study revealed these trends in value-proven, emerging technologies:

- GenAI is moving from aspiration to application. Although only 16% of respondents indicate their organisations currently use generative AI as an anti-fraud tool, another 58% plan to in the future. Among those already using GenAI, top applications are phishing and scam detection (49%), risk identification/assessment (46%) and report writing (45%).
- AI agents are hotter still. Nearly one in 10 (8%) of respondents say their organisations use agentic AI for fraud fighting, and nearly one-third (31%) more expect to deploy it by 2028 – the highest near-term adoption expectation of any emerging technology category examined.
- Physical biometrics leads emerging tech adoption – while many neglect the benefits of automation and the cloud. The use of physical biometrics is now the most widely adopted emerging technology in anti-fraud programs gauged in the study, used by nearly half of organisations (45%) surveyed – up from roughly one-third (34%) in 2022. In contrast, cloud-native fraud detection platforms and automation remain significantly underutilised, used by only 10% and 29% of organisations, respectively.
- Quantum computing's impact on the anti-fraud battlefield is closer than most expect. Most respondents (62%) expect quantum computing and quantum AI to materially impact fraud detection and prevention by 2030 – and a surprising 11% say it already is.

Ready or not...

Whatever their level of preparedness, organisations across sectors face the same AI-accelerated fraud threats. The differentiator? Their ability to fight back. Fraud fighters must be equipped with the right data and technology – and also the appropriate speed, scale and governance – to combat modern-day risks.

DELINEA APPOINTS SCOTT GOREE TO LEAD NEXT PHASE OF STRATEGY AND PARTNER-LED GROWTH

GLOBAL CHANNEL LEADER TO SCALE PARTNER ECOSYSTEM AND HELP CUSTOMERS ADOPT MODERN IDENTITY SECURITY FOR THE AI ERA

Delinea, the identity security control plane that secures access across human, machine, and AI identities, has appointed Scott Goree as Senior Vice President of Channel and Alliances. In this role, Goree will lead Delinea's global partner and alliance strategy, including launching the company's next-generation partner program, expanding its ecosystem, and accelerating partner-led growth worldwide.

Goree brings two decades of experience building and scaling high-impact partner ecosystems across the security and infrastructure industry. Most recently, he served as Senior Vice President of Partners and Commercial Sales at Optiv, where he helped modernise channel strategy and accelerate partner-driven growth. Prior to that, he was the first global channel chief at Skyhigh Security, where he reinvented the partner program and significantly increased channel-sourced revenue.

"Identity security has become a board-level priority for organisations navigating cloud, hybrid, and AI-driven environments," said Chris Kelly, President at Delinea. "Partners are essential to helping customers modernise securely and deliver measurable outcomes. Scott has a proven track record of building strong partner ecosystems and driving growth, and his leadership will be instrumental as we scale our partner strategy for the AI era."

Goree will focus on building a more unified, scalable partner model designed for how customers buy and deploy identity security today. The SVP's priorities include strengthening enablement, simplifying engagement, and ensuring partners are equipped to support customers as they modernise privileged access, secure cloud entitlements, and reduce identity-based risk.

CUSTOMERS ARE LOOKING FOR TRUSTED ADVISORS WHO UNDERSTAND THEIR ENVIRONMENTS AND CAN DELIVER RESULTS

"Customers are looking for trusted advisors who understand their environments and can deliver results," said Goree. "I'm excited to work with our partners to build a program that supports long-term growth, accelerates time to value, and helps organisations adopt modern identity security with confidence."

Before joining Optiv and Skyhigh Security, Goree held senior channel leadership roles at Nutanix, Pure Storage, and Cisco, where he consistently built high-performing teams and delivered growth that exceeded corporate goals. He has been recognised as a CRN Channel Chief and a Top 50 Channel Influencer by Channel Futures.


Scott Goree

SOPHOS APPOINTS HUSSAIN SALMAN AS ENTERPRISE SERVICES DIRECTOR FOR GULF REGION

HUSSAIN WILL LEAD ENTERPRISE SERVICES DELIVERY ACROSS THE GULF, WORKING CLOSELY WITH ORGANISATIONS TO STRENGTHEN THEIR CYBER RESILIENCE AND SECURE HYBRID ENVIRONMENTS.

Sophos, a global leader of innovative security solutions for defeating cyberattacks, today announced the appointment of Hussain Salman as Enterprise Services Director for the Gulf Region, where he will lead across the UAE, Bahrain, Kuwait, Oman and Qatar.

With the region consistently ranking among the world's most targeted regions for cyberattacks, cybersecurity has evolved from priority to an urgent business need. This shift is driven by rapid digital transformation, the rise in state-sponsored threats, and the growing impact of AI-powered attacks, fueling a cybersecurity market that is expected to nearly double from $20.55 billion in 2025 to $40.97 billion by 2030. In this environment, the need for extensive regional expertise continues to grow.

Hussain has decades of experience in IT services, cybersecurity, and digital transformation, with strong expertise in the Gulf market. After long years at Dell Technologies, he went on to lead cybersecurity business development at Secureworks, driving regional growth and supporting major organisations with practical, business-focused security strategies.

In his new role, Hussain will lead enterprise services delivery across the Gulf, working closely with organisations to strengthen their cyber resilience and secure hybrid environments. By leveraging Sophos' AI-driven cybersecurity solutions and 24/7 threat monitoring, prevention, detection, and response, he will also guide customers in accelerating their digital transformation journeys with greater assurance.

"Cybersecurity in the Middle East has entered a new strategic era," said Harish Chib, Vice President, Emerging Markets, Sophos. "The organisations that will lead in this region are those that move from reactive defence to proactive, intelligence-led security, integrating resilience into every layer of their business. Hussain brings decades of experience at this level, advising some of the region's most complex enterprises and helping align security with business outcomes. His appointment reflects Sophos' focus in the region, and our commitment to going beyond the traditional vendor role, working as a trusted, long-term partner in our customers' success."

"The threat landscape is evolving faster than ever, and the pressure on enterprises in the Gulf region continues to grow," said Hussain Salman, Enterprise Services Director, Gulf Region, Sophos. "With AI accelerating both the scale and sophistication of cyber threats, organisations need more than just technology. They need a partner who truly understands their business, their risks, and where they want to go. I'm excited to step into this role and work closely with our customers to build security strategies that are proactive, resilient, not only protect their operations, but also give them the confidence to grow and lead in an increasingly digital world."

As Sophos continues to invest in the region, the company remains focused on supporting customers with the right expertise and capabilities to navigate today's increasingly complex threat landscape and stay ahead of what's next.

WITH AI ACCELERATING BOTH THE SCALE AND SOPHISTICATION OF CYBER THREATS, ORGANISATIONS NEED MORE THAN JUST TECHNOLOGY.

Hussain Salman.

CLOUD BOX TECHNOLOGIES STRENGTHENS AI LEADERSHIP WITH THREE-PILLAR STRATEGY AND APPOINTMENT OF CAIO

THE NEW ROLE OF CHIEF AI OFFICER ESTABLISHES THAT CLOUD BOX TECHNOLOGIES IS INCORPORATING AI INTO THE CORE OF ITS OFFERINGS

Cloud Box Technologies, a leading systems integrator and IT services specialist in the Middle East, announces its AI-first strategy with the introduction of a focused three-pillar framework led by Laxmi Nageswari as the Chief AI Officer (CAIO). This highlights how the company has evolved from a traditional IT infrastructure provider into a full spectrum digital transformation partner including AI, automation and cybersecurity.

The new role of Chief AI Officer establishes that Cloud Box Technologies is incorporating AI into the core of its offerings. Laxmi will guide the strategy, innovation, partnerships and capability development where AI is an integrated layer in all its offerings and not just a standalone service.

The company's AI strategy is anchored on three pillars. Firstly, it covers AI-based cybersecurity, data analytics, automation and cloud integrated intelligence, making sure that AI is included in all its services. Next is the Algo-as-a-Service (AaaS) model, which helps to deploy scalable, reusable AI models, speeding up time-to-market with consistency and accessibility for customers. At the heart of this strategy and supporting the other pillars is its Centre of Excellence (CoE). This serves as the hub for governance, innovation, and developing talent by providing best practices, helping with research and making sure that AI is adopted responsibly.

Together, they reshape AI from individual initiatives into a combined capability that is available across the whole company. It improves scalability, speeds delivery and strengthens the company's long-term competitive positioning. Designed as an integrated innovation ecosystem, the strategy connects hardware, applications, and talent to create a cohesive platform for AI adoption.

Ranjith Kaippada, Managing Director at Cloud Box Technologies, said, "The introduction of the three-pillar framework, and the strategic move to appointing Laxmi Nageswari to lead it strengthens our ability to deliver scalable AI-driven solutions and aligns our vision with the UAE's National Strategy for Artificial Intelligence 2031. This will have a significant impact on how Cloud Box Technologies transforms into an all-encompassing digital transformation partner and harness AI effectively."

Laxmi Nageswari, Chief AI Officer of Cloud Box Technologies, says, "Our approach is centred on delivering end-to-end guidance from strategy formulation to execution, grounded in a deep understanding of both advanced technologies and the operational realities our clients face every day. Our mission is to bridge business

OUR MISSION IS TO BRIDGE BUSINESS AND TECHNOLOGY TO DRIVE INNOVATION AND DELIVER MEASURABLE OUTCOMES.

and technology to drive innovation and deliver measurable outcomes. We focus on translating strategy into execution, turning emerging technologies into scalable, production-ready AI solutions that unlock efficiency and new opportunities. I'm excited to lead this journey and contribute to both the company's growth and the UAE's broader AI ambitions."

In her role, Laxmi will oversee how this framework is integrated and executed end-to-end. Her responsibilities include ensuring that AI investments meet with business priorities, actioning scalable AI solutions through AaaS and driving governance and innovation through the CoE. She will also play a major role in making sure that there is a smooth collaboration across teams. Consequently, high-impact AI use cases will be of priority, business outcomes will be measurable and refining of the AI roadmap will be ongoing.

In the short term, Laxmi will focus on translating strategy into execution by operationalizing the AI pillars and strengthening their integration. This approach will enable CoE-led innovation to serve as the foundation for delivering production-ready AaaS solutions, creating a structured and scalable AI delivery model. Her leadership will be significant in systematizing AI delivery, showing tangible value and building a strong foundation for scalable growth.

Laxmi brings strategic vision, technical depth, and ecosystem leadership and her experience in AI initiatives, industry academia collaborations and innovation programs provide high value to the company's AI capabilities. She also brings prior experience from Boston Limited, where she contributed to large-scale transformation initiatives, further strengthening her ability to align AI strategy with business outcomes. Her career spans leadership roles across diverse regions and industries, where she has successfully led strategy through execution. This involves implementing new technologies into practical solutions that help with smarter decision-making and creating tangible business impact.

With this announcement, Cloud Box Technologies makes its commitment more solid in the UAE market, further positioning itself at the forefront of AI-based transformation in the region.

Laxmi Nageswari.

Girard Moussa.

SENTINELONE APPOINTS GIRARD MOUSSA AS AREA VICE PRESIDENT FOR META TO DRIVE EXPANSION STRATEGY

INDUSTRY VETERAN TO LEAD SALES STRATEGY AND STRENGTHEN GROWTH ACROSS ENTERPRISE AND PUBLIC SECTOR MARKETS

SentinelOne, the AI Security leader, has appointed Girard Moussa as Area Vice President (AVP) of Sales for the Middle East, Turkey, and Africa (META) region. In this role, Moussa will oversee the company's regional sales strategy, facilitating growth across enterprise and public sector markets along with the adoption of the Singularity Platform.

With over 25 years of experience in the field of technology, including over two decades in the META region, Moussa will expand SentinelOne's growth in key markets. His responsibilities also include increasing customer and partner engagement, creating high-performance teams, and actioning go-to-market strategies aligned with regional priorities. He holds a Bachelor of Science in Computer Science from the American University of Beirut.

"Companies are facing a fast transformation, with AI and cloud reshaping their processes and scale," said Girard Moussa, Area Vice President, META, SentinelOne. "SentinelOne is at the forefront of change in cybersecurity, where autonomous, AI-based capabilities are needed to keep up with the speed and complexity of modern threats. I look forward to collaborating with our teams, customers, and partners to support this transition, expand our regional footprint, and deliver measurable outcomes at scale."

Moussa held senior leadership positions at Microsoft, Google Cloud, SAP, Cisco, and Splunk. Recently, he was the Senior Sales Director at Microsoft UAE, where he led interactions across the public sector and higher education institutions. Earlier, he led Microsoft's Enterprise Cybersecurity Group for the MEA region, setting the practice and the company as a trusted advisor to CXOs across the region. He also played a key role in launching and growing Splunk's regional presence, with significant growth and market expansion.

COMPANIES ARE FACING A FAST TRANSFORMATION, WITH AI AND CLOUD RESHAPING THEIR PROCESSES AND SCALE.

SentinelOne is broadening its presence within META to support businesses facing the complex threat landscape by adopting generative AI and cloud technologies. The company is focused on advancing the use of its AI-based Singularity Platform, which provides autonomous, machine-speed protection against modern threats. Additionally, it is strengthening the capacity to support secure AI adoption, including protections against manipulation of models, leakage of data and prompt injection.

"Girard's appointment comes at a defining moment for our region. As AI accelerates both innovation and threat sophistication, organizations can no longer rely on traditional security models. The shift toward autonomous, AI-driven security is not optional - it's inevitable," says Ezzeldin Hussein, Regional Senior Director, Solution Engineering, META at SentinelOne. "Girard brings the leadership, regional depth, and execution mindset needed to help our customers navigate this transformation with confidence. Together, we are not just scaling our presence in META; we are reshaping how security is delivered, moving from reactive defense to real-time, intelligent resilience."

WATCHGUARD APPOINTS RABIH ITANI AS REGIONAL DIRECTOR, EXPANDS MEA FOOTPRINT

MIDDLE EAST CYBERSECURITY MARKET SET TO SURPASS $ 37 BILLION BY 2034, DRIVEN BY RAPID DIGITAL TRANSFORMATION.

WatchGuard Technologies, a global leader in unified cybersecurity, has announced the appointment of Rabih Itani as Regional Director for the Middle East and Africa (MEA). The appointment comes at a time of significant growth across the region, with the Middle East cybersecurity market projected to more than double from $16.72 billion in 2025 to $37.22 billion by 2034 (Market Data Forecast), driven by digital transformation across finance, healthcare, energy, and government sectors.

In this newly created role, Rabih will report to Frederic Saint-Joigny, Vice President EMEA, and will lead WatchGuard's go-to-market strategy across MEA, focusing on driving revenue growth, expanding the company's direct presence, and strengthening its channel ecosystem of distributors, MSPs, and resellers. He will also accelerate adoption of WatchGuard's Unified Security Platform across the region.

"Rabih brings the perfect combination of regional expertise and industry experience to drive WatchGuard's growth in the Middle East and Africa," said Fred Saint-Joigny, Vice President EMEA. "MEA is one of our most significant growth markets. His deep knowledge of the local landscape and proven leadership across the ICT and cybersecurity ecosystem will be invaluable as we expand our operations, engage partners more directly, and support customers at scale."

Rabih is a veteran of the ICT and cybersecurity industry with a pioneering role in helping the MEA region embrace disruptive technologies. Having worked across the full ecosystem — as a customer, integrator, and technology provider — he brings a uniquely well-rounded perspective on the region's digital transformation and cyber resilience journeys.

Previously, Rabih served as Regional Director at VAD CyberKnight and held pivotal leadership roles at Vectra AI. He spent nearly a decade at Aruba, a Hewlett Packard Enterprise company, leading Security, SD-WAN, and Telco sector initiatives across METNA, including work with MSSPs. Earlier in his career, he spent 13 years at the American University of Beirut directing data communications, security, and operations, followed by technical roles at Extreme Networks and Computer Network Systems UAE — building a deep foundation in ICT and cybersecurity.

"I'm excited to join WatchGuard at a time when cybersecurity and digital transformation are top priorities for businesses across MEA," said Rabih Itani. "There is tremendous potential to help organisations adopt innovative security solutions while empowering the channel ecosystem to deliver real value. I look forward to leading this expansion and supporting our partners and customers with WatchGuard's industry-leading Unified Security Platform."

I'M EXCITED TO JOIN WATCHGUARD AT A TIME WHEN CYBERSECURITY AND DIGITAL TRANSFORMATION ARE TOP PRIORITIES FOR BUSINESSES ACROSS MEA

Rabih Itani.

TRENDAI APPOINTS IBRAHIM ELKABANY TO DRIVE PARTNER STRATEGY ACROSS MMEA AND INDIA

ELKABANY BRINGS MORE THAN 20 YEARS OF LEADERSHIP EXPERIENCE ACROSS ENTERPRISE TECHNOLOGY, CLOUD TRANSFORMATION, AND STRATEGIC ALLIANCES.

Ibrahim ElKabany.

I'M EXCITED TO JOIN TRENDAI AT A TIME WHEN ORGANISATIONS ARE PRIORITISING RESILIENCE, PLATFORM SECURITY, AND TRUSTED ECOSYSTEM PARTNERSHIPS.

TrendAI has appointed Ibrahim ElKabany as Director, Global Partner Office, Alliances & Go-To-Market for Mediterranean, Middle East & Africa (MMEA) and India, reinforcing its strategic focus on accelerating ecosystem-led growth, strengthening partner alliances, and expanding market presence across key high-growth regions.

Based in Dubai, ElKabany brings more than 20 years of leadership experience across enterprise technology, cloud transformation, and strategic alliances, with a strong track record of driving revenue growth and building high-impact partner ecosystems across Europe, the Middle East, Levant, and Africa.

Throughout his career, he has held senior leadership roles with global technology organisations, including Oracle, Microsoft, IBM, SAP, Wipro, and Commvault, where he led high-performing teams, multimillion-dollar growth initiatives, hyperscaler partnerships, and large-scale enterprise transformation programs.

"I'm excited to join TrendAI at a time when organisations are prioritising resilience, platform security, and trusted ecosystem partnerships," said Ibrahim ElKabany.

"I look forward to working closely with our teams, partners, and customers to unlock growth and deliver meaningful impact across the region."

In his new role, ElKabany will focus on scaling alliance ecosystems, driving partner-led go-to-market execution, and accelerating strategic growth initiatives across the Mediterranean, Middle East & Africa (MMEA), and India, enabling stronger collaboration across hyperscalers, strategic partners, and enterprise customers.

Delinea

Unlock AI's potential, not your defenses.

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

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

Secure AI with Delinea so you can:

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

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

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

delinea.com


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