@entitworldmea @enterpriseitworldmea @enterpriseitworldmea

PAGES 40 | VOLUME 04 | ISSUE 04

WWW.ENTERPRISEITWORLDMEA.COM

Enterprise IT WORLD MEA

FOR THE CIOs. BY THE CIOs.

DECEMBER 2025

MIM BURT
VP, Gartner

2026: AI, Cloud, and Cybersecurity Reshape Global Enterprise—Middle East Leads the Leap

From Riyadh to Silicon Valley, enterprises are racing to turn ambition into architecture.... Page no. 16

MIKE CAPONE
CEO, Qlik

ANAND ESWARAN
CEO, Veeam

https://enterpriseitworldmea.com/

infoblox®

Infoblox unites networking, security and cloud to create a foundation for operations that is as resilient as it is agile.

Learn more

infoblox.com

THE TECH FORCES REDEFINING THE MIDDLE EAST IN 2026

The Middle East is entering 2026 as a digital powerhouse, driven by ambitious national visions and unprecedented investment in transformative technologies. Governments across the Gulf Cooperation Council (GCC) are steering economies away from hydrocarbons toward hyper-scale digital ecosystems, creating fertile ground for innovation and global partnerships.

Artificial Intelligence (AI) and Generative AI

AI adoption is no longer aspirational—it's foundational. From predictive analytics in finance to autonomous logistics in energy, AI is embedded in every sector. Generative AI (GenAI) is accelerating software spending, projected to hit $20.4 billion in 2026, as enterprises integrate AI-driven automation into workflows. Saudi Arabia's $40 billion AI fund and UAE's Stargate data center initiative underscore the region's intent to dominate the AI stack.

Cloud and Edge Computing

Cloud computing is surging, with the Middle East public cloud market expected to grow nearly 20% annually through 2033. Multi-cloud strategies and sovereign cloud models are critical as nations prioritize data residency and compliance. Edge computing complements this shift, enabling real-time processing for smart cities, autonomous vehicles, and industrial IoT—key pillars of Vision 2030 and similar programs.

Cybersecurity as a Strategic Imperative

Cyber resilience is evolving from a defensive posture to a growth enabler. With cyberattacks on critical infrastructure rising, GCC nations are embedding zero-trust architectures and AI-driven threat detection into national agendas. The regional cybersecurity market is forecast to double by 2030, fueled by cloud adoption and AI-powered security frameworks.

IoT and Smart Cities

IoT integration is transforming urban life and industrial operations. Mega-projects like NEOM and Msheireb Downtown Doha are deploying IoT sensors for energy optimization, predictive maintenance, and intelligent mobility. Digital twins—virtual replicas of physical assets—are becoming standard for infrastructure planning and operational excellence.

Emerging Horizons: Blockchain, Quantum, and AR/VR

Blockchain is gaining traction in finance and supply chain transparency, while quantum computing research is laying the groundwork for breakthroughs in cryptography and optimization. AR and VR are redefining customer engagement and workforce training, signaling a shift toward immersive digital experiences.

The Bottom Line

2026 will mark a turning point where AI, cloud, cybersecurity, IoT, and immersive technologies converge to reshape economies. For businesses, the message is clear: adapt to this tech-driven reality or risk irrelevance. The Middle East isn't just catching up—it's setting the pace for global digital transformation. MEA

SANJAY MOHAPATRA
SANJAY@ACCENTINFOMEDIA.COM

NEXT MONTH SPECIAL

COVER STORY

REVEIEW 2025 TECHNOLOGY GROWTH

The next issue is dedicated to the Reveiew 2025 Technology Growth. We would like to take feedback from the CIOs and OEMs and create our judgement on the same.

SUPPLEMENT

QUOTES FROM TOP CIOS

The supplement story of the magazine would have relevant quotes from the top CIOs in India.

PLUS

Interviews and Case Studies

Catch interviews, guest articles and case studies of recent applications from the Industry stakeholders, IT/ITES Vendors and IT leaders and CIOs from the Enterprise IT World CIO Community.

Send in your inputs to sanjay@accentinfomedia.com

CONTENTS

VOLUME 04 | ISSUE 04 | DECEMBER 2025 | WWW.ENTERPRISEITWORLDMEA.COM

COVER STORY

MORE INSIDE

Enterprise IT WORLD MEA

FOR THE CIOs. BY THE CIOs.

Publisher: Sanjib Mohapatra
Chief Editor: Sanjay Mohapatra
Managing Editor: Anisha Nayar Dhawan
Associate Editor: Balaka Baruah Agarwal
Designer: Deepak kumar
Web Designer: Sangeet Kumar
Technical Writer: Manas Ranjan

MARKETING
Marketing Manager: Sangram Barpanda
Events Marketing: Sanjib M

SALES CONTACTS
Accent Infotech Media FZC.
Business Center
Sharjah Publishing City, Free Zone
Sharjah United Arab Emirates

EDITORIAL OFFICE
Accent Infotech Media FZC.
Business Center
Sharjah Publishing City, Free Zone
Sharjah United Arab Emirates

EMAIL CONTACTS
Group Editor: sanjay@accentinfomedia.com
Editorial Query: balaka@accentinfomedia.com
Video Interview Query: sanjay@accentinfomedia.com
Advertisement Query: sanjib@accentinfomedia.com

ADVERTISE WITH US
Advertisement Query
For Print Magazine / Online Magazine / Social Media – lagan@accentinfomedia.com
For Events / Seminar / Webinar / Round table – Sanjib@accentinfomedia.com
For CIOTV.LIVE – sanjay@accentinfomedia.com

IT WORLD MEA
ROUND UP

Confluent Debuts Real-Time AI Platform **in Middle East**

Confluent has launched Confluent Intelligence in the Middle East during its Data Streaming World Tour in Dubai, introducing a fully managed platform designed to accelerate enterprise AI adoption. Built on Confluent Cloud, the solution enables organisations to stream and process historical and real-time data, delivering the context AI systems need for accurate, adaptive decision-making.

The timing is critical. While global AI investments exceed $30–$40 billion, 95% of generative AI projects fail to deliver ROI, largely due to the absence of context-rich data. Confluent Intelligence addresses this gap by providing an always-on data foundation that evaluates past events, adapts to current conditions, and instantly supplies context to AI agents.

"Across the Middle East, organisations are rapidly progressing from experimentation to real, production-grade AI," said Karim Azar, AVP and GM – Middle East, Confluent. "With Confluent Intelligence, we're enabling them to harness the full potential of their data to power adaptive, context-aware AI applications."

Key features include:

Real-Time Context Engine: Streams structured context to AI agents via Model Context Protocol (MCP).

Streaming Agents: Event-driven agents built on Apache Flink® for real-time automation.

Built-in ML Functions: Anomaly detection, forecasting, and inference directly in Flink SQL.

Confluent also strengthened its AI ecosystem through a deeper partnership with Anthropic, making Claude the default LLM for Streaming Agents. This integration enables advanced anomaly detection, real-time personalization, and other high-value use cases.

"Without continuous data flow, even the best models can't deliver timely, business-critical decisions," said Jay Kreps, CEO, Confluent.

DATA BRIEF

Only 20% of Customer Service Leaders Report AI-Driven Headcount Reduction: Gartner Survey

Commvault Launches Cloud Unity to Reinforce **Enterprise Resilience**

Commvault has unveiled Commvault Cloud Unity, an AI-powered platform designed to unify data security, cyber recovery, and identity resilience across multi-cloud, SaaS, on-premises, and edge environments. This marks a major leap in enterprise continuity amid escalating cyber threats and AI-driven attacks.

Why It Matters:
Businesses today face relentless cyber risks and identity system compromises that threaten revenue and reputation. Cloud Unity consolidates fragmented tools into a single console, delivering visibility and control across 160+ cloud regions and 200+ services.

Three Pillars of Resilience:
Data Security: AI-driven discovery, classification, and automated protection policies with full workload visibility. Customers gain cost insights comparing Commvault Cloud versus native services.

Cyber Recovery: Features include Threat Scan for detecting IoCs, patent-pending Synthetic Recovery to surgically remove threats, and Cleanroom Recovery with automated runbooks for secure testing.

Identity Resilience: Enhanced protection for Active Directory with vulnerability assessments, anomaly detection, and instant reversal of suspicious changes. Integrated AD forest recovery ensures safe testing without disrupting production.

AI at the Core:
Cloud Unity leverages AI insights combining threat intelligence and recovery readiness to enable rapid, clean recoveries and enforce centralized policies.

Availability:
Select features roll out later this year, with full.

Endava Launches Dava.Rise to Accelerate **Enterprise Innovation**

Endava has introduced Dava.Rise, a global programme designed to bridge the gap between scale-ups and enterprises, enabling faster innovation and commercial success. The initiative aims to transform breakthrough ideas into scalable solutions by pairing high-potential innovators with large organisations seeking rapid transformation.

Dava.Rise leverages Endava's extensive industry network to identify enterprise challenges and match them with scale-ups offering cutting-edge technologies. Beyond introductions, the programme provides structured support to move concepts from pilot to market-ready solutions. "Enterprises want to innovate at speed, while scale-ups seek guidance and infrastructure to succeed," said John Cotterell, CEO of Endava. "Dava.Rise brings entrepreneurial creativity together with enterprise-grade execution."

For scale-ups, the programme offers mentorship, technical guidance, and go-to-market support to accelerate growth and prove product-market fit. Enterprises gain access to a curated pipeline of innovation-ready ventures, reducing risk and time-to-adoption. Industry leaders have praised the initiative.

CIO **EVENTS**

09-10 DEC, 2025

World Summit AI Qatar
Global AI ecosystem, enterprise and academia collaboration, cutting-edge AI innovations.

PLACE: **DOHA EXHIBITION & CONVENTION CENTER, QATAR**

09-10 DEC, 2025

I.S.E.S. Middle East 2025
Semiconductor industry leadership, collaborative ecosystem building in MENA.

PLACE: **ST. REGIS AL MOUJ MUSCAT RESORT, OMAN**

10 DEC, 2025

#RISK Dubai 2025
Governance, risk, and compliance (GRC), cybersecurity strategies, and regulatory insights.

PLACE: **DUBAI, UAE**

11-12 NOV, 2025

BTOPEX Middle East Summit
Business transformation, operational excellence, and IT innovation.

PLACE: **RIYADH, SAUDI ARABIA**

eventus™

www.eventussecurity.com
hello@eventussecurity.com

EMPOWERING BUSINESSES
with Award-winning
MANAGED SECURITY SERVICES

Enterprise-Grade Security:

- AI-driven SOC as a Service
- Managed XDR
- Incident Response & Digital Forensics
- Continuous Automated Red Teaming(CART)
- Breach & Attack Simulation (BAS)
- DevSecOps and Application Security
- Ransomware Emergency Response

Ranked #82
Globally Among Top 250 MSSPs

Why Eventus?

Technology:

- XDR-powered Next-gen **SecOps Platform**
- Eventus Threat Labs - **4500+** Threat Advisories issued
- **40000+** IOCs blocked

Experience:

- **1000+** manhours of Incident Response experience.
- **40+** team for Threat Research and R&D.
- **70+** successful SOC projects.
- **100+** successful Cyber Resilience projects.

Expertise:

- **150+** certified SOC analysts, incident responders, threat hunters with international accreditations.

Our Global Awards

Head Office

Kesar Solitaire | 604, 605, 606, 6th Floor Palm Beach Rd, Sector 19, Sanpada, Navi Mumbai 400705

India | SEA | Middle East | USA

FOMO at Work: Women in Tech Urge **More Female Leaders**

Acronis has released its 2025 Women in Tech Report, "FOMO at Work: The Opportunity Gap Between Men and Women in Tech," revealing persistent gender perception gaps and the urgent need for leadership-focused initiatives. The global survey of over 650 IT professionals shows stark differences in how men and women view career opportunities and workplace equity. While men largely see the industry as fair, women report systemic barriers tied to bias, work-life balance, and limited access to leadership roles—despite making up 29% of the global tech workforce.

"Closing the gender gap requires more than good intentions—it demands action," said Alona Geckler, SVP Business Operations & Chief of Staff at Acronis. Key findings highlight the disparity: only 60% of women believe men and women share equal career opportunities compared to 75% of men; 63% of women cite work-life balance as a major hurdle versus 49% of men; and 70% of women want tailored leadership programs, while just 56% of men agree. Over half of women fear missing career-defining opportunities due to family responsibilities.

Industry leaders echo the call for change. Melyssa Banda of Seagate noted, "Highlighting women role models and fostering inclusive cultures can benefit the entire industry." The report urges companies to move beyond intent and implement targeted initiatives—mentorship, leadership development, and bias training—to unlock innovation and create workplaces where diverse talent thrives.

S/HE SAID IT

DAVE WILSON
DIRECTOR OF GLOBAL HYBRID SOLUTIONS AT VERTIV.

"The world expects energy efficiency and flexibility with the growth of communications, such as 5G and edge connectivity."

"As organizations grow ever more dependent on data and the DBAs who manage that data, it is imperative for us to create a corporate culture that removes complexities and misalignments, setting the stage for true team success."

Kevin Kline, Database Management Systems Expert at SolarWinds

QUICK BYTE ON SECURITY

Cloudflare Acquires Replicate to Simplify AI **Development**

Cloudflare has announced its acquisition of Replicate, a strategic move aimed at democratizing AI development by eliminating infrastructure complexity for developers worldwide. In an era of rapid AI innovation, the biggest challenge for startups and independent creators remains managing GPUs, fragmented tools, and deployment hurdles. Cloudflare's vision is clear: make AI development as simple as writing an idea. By integrating Replicate's catalog of over 50,000 production-ready AI models with its Workers AI platform, Cloudflare is creating a unified environment for model discovery, instant deployment, and global execution. Developers will no longer need to configure infrastructure or worry about scalability—they'll have a seamless, code-first platform that accelerates the journey from concept to application.

Cybersecurity's Next Frontier: AI, Identity, and Geopolitics **Redefine Defense**

The cybersecurity landscape is entering a transformative era where identities, AI-driven decisions, and geopolitical forces take center stage. BeyondTrust's latest predictions for 2026 reveal a future where convenience and intelligence collide with complex vulnerabilities, reshaping security strategies worldwide.

Agentic AI—autonomous software capable of making independent decisions—is emerging as a game-changer. While it promises efficiency and smarter automation, it also introduces AI-driven breaches that are faster, adaptive, and unpredictable. The attack surface is shifting from systems to decision-making logic, making identity visibility and access control more critical than traditional firewalls.

Geopolitics adds another layer of complexity with the rise of digital tariffs—cross-border taxes on data flows and digital services. This move toward digital sovereignty will challenge multinational enterprises with new compliance demands and fragmented cloud ecosystems.

Legacy tools are fading fast. VPNs, long a staple of remote work, are expected to disappear, replaced by identity-based zero-trust models. Cybercriminals are also evolving tactics, with account poisoning—manipulating trusted financial identities to divert payments—signaling a shift from disruption to direct financial exploitation.

Looking ahead, biological computing powered by living neurons and companion AI will raise ethical and security dilemmas far beyond privacy. Even MITRE's threat classification framework may need reinvention to keep pace.

BMC Helix Named Leader in Forrester Wave 2025 for Enterprise **Service Management**

BMC Helix has been recognized as a Leader in The Forrester Wave: Enterprise Service Management Platforms, Q4 2025, earning top scores in 17 evaluation criteria including vision, roadmap, innovation, agentic AI orchestration, analytics, and enterprise workflow management. This achievement positions BMC Helix at the forefront of redefining ServiceOps for the AI era.

Forrester's report highlights how AI is transforming the enterprise service management market, with platforms like BMC Helix enabling intelligent service orchestration, proactive management, and enhanced employee experiences across IT and business operations. "For organizations seeking a unified, AI-driven platform to manage complex IT operations, BMC Helix offers powerful enterprise workflow and task management, monitoring, and proactive management," wrote Julie Mohr, Principal Analyst at Forrester.

Ryan Manning, Chief Product Officer at BMC Helix, emphasized that the recognition validates the company's bold vision. "Being named a leader isn't just recognition—it's proof that playing it safe isn't in our DNA. Our mission is to reset the economics of IT with the anti-platform for agentic AI in ServiceOps, turning the department of 'No' into the department of 'Let's go!'"

The Helix platform enables enterprises to deploy dynamic fleets of AI agents that augment human work, automate solutions, and predict operational challenges before they impact business.

EXECUTIVE MOVEMENT

OPSWAT Appoints Veteran Cybersecurity Leader Hussam Sidani to Accelerate MENA Growth

WSO2 Strengthens Global Growth Strategy with Appointment of Sudesh Vasudevan as VP & Head of Corporate Development

Veeam Appoints Allison Cerra as Chief Marketing Officer to Drive Global Brand Transformation for the AI Era

IFS Appoints Robi Gone as CIO to Drive Global Technology Transformation

Confluent Strengthens Regional Leadership with Appointment of Karim Azar as AVP and GM for the Middle East

GLOBAL UPDATE

Logitech Spot Named TIME Best **Invention of 2025**

Logitech Spot, a radar-based workplace occupancy and environmental sensor, has been recognized by TIME as one of the Best Inventions of 2025 in the Productivity category. This accolade highlights Spot's role in transforming workplace efficiency by making the invisible visible.

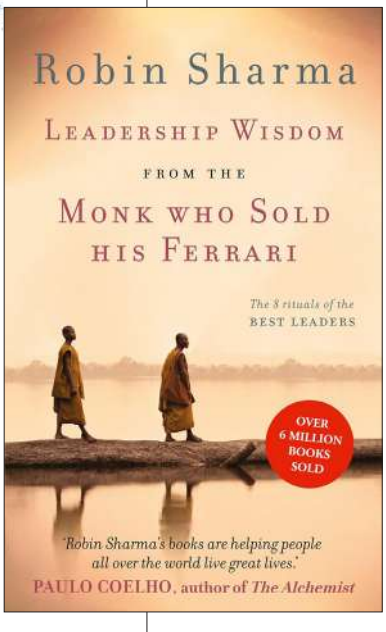
Designed to address hidden barriers to productivity and office health, Logitech Spot functions like a fitness tracker for the workplace. The compact, peel-and-stick device monitors room occupancy, air quality, temperature, and humidity—without wiring or user interaction. By turning unseen inefficiencies into actionable insights, Spot enables businesses to optimize space usage, improve employee comfort, and reduce energy costs.

"Most office problems are data problems in disguise," said Henry Levak, VP of Product at Logitech for Business. "Every office has its secrets—how many people are using which rooms, what's in the air, and where energy is wasted. Logitech Spot makes the invisible visible, giving businesses the data they need to make smarter decisions."

Spot's radar technology automatically books and releases rooms based on real-time occupancy.

BOOK SHELF

THE MONK WHO SOLD HIS FERRARI



BY
AUTHORS: AUTHOR: ROBIN SHARMA

PRICE: AED 71.40 (PAPERBACK)

Robin Sharma's The Monk Who Sold His Ferrari is an inspiring fable that blends self-help principles with a captivating story. It follows Julian Mantle, a high-powered lawyer who suffers a life crisis and embarks on a spiritual journey to the Himalayas. Through his transformation, the book explores themes of mindfulness, purpose, and inner peace.

The narrative is simple yet profound, making complex ideas accessible. Sharma introduces practical lessons like mastering the mind, following your purpose, and living with discipline. Concepts such as the "Garden of the Mind" and "Kaizen" (continuous improvement) are presented through engaging metaphors, encouraging readers to cultivate positivity and embrace lifelong growth.

Sophos and Microsoft Unite to Bring AI-Powered **Cyber Defense to Everyone**

Sophos and Microsoft have announced a groundbreaking collaboration that embeds real-time threat intelligence directly into Microsoft Security Copilot and Microsoft 365 Copilot, signaling a new era in cybersecurity. This integration aims to make advanced cyber insights accessible to every user—from SOC analysts to business leaders—through natural language queries inside everyday productivity tools.

Powered by Sophos Intelix, users can now ask questions like "Is this link malicious?" in Teams or enrich alerts with global threat prevalence and sandbox analysis without leaving Copilot. This shift moves security operations beyond traditional consoles toward intuitive, AI-driven workflows that accelerate response times and reduce complexity.

Simon Reed, Chief Scientific Research Officer at Sophos, noted, "The future of SOC productivity is moving beyond graphical interfaces toward human–AI collaboration. AI assistants powered by deep threat intelligence are fundamentally reshaping how analysts work." For small and mid-sized businesses, often constrained by resources, this capability is transformative—especially as attackers can compromise Active Directory in just 11 hours and 96 percent of SMBs struggle to investigate alerts.

Microsoft's Vasu Jakkal emphasized the strategic significance: "AI is the force multiplier for defenders, and when partners like Sophos bring their agentic innovation into the Microsoft Copilot ecosystem, the impact is exponential."

As identity becomes the new perimeter and AI the ultimate co-defender, this partnership marks a pivotal step toward intelligent, contextual, and universally accessible cybersecurity—where protection happens seamlessly in the flow of work.

Check Point and Microsoft Join Forces **to Secure AI Agents**

Check Point Software Technologies has partnered with Microsoft to embed prevention-first AI security directly into Microsoft Copilot Studio, addressing the growing risks of generative AI agent adoption. As enterprises accelerate AI innovation, security and governance have become critical priorities. This integration ensures every AI interaction, workflow, and data connection remains secure, compliant, and aligned with enterprise policies.

The collaboration introduces Check Point's AI Guardrails, Data Loss Prevention (DLP), and Threat Prevention capabilities into Copilot Studio, delivering continuous runtime protection against prompt manipulation, data leakage, and model misuse. With AI agents evolving from conversational assistants to autonomous actors capable of triggering workflows and accessing sensitive data, traditional security controls fall short. "AI agents don't just converse—they act. And when they act, they can access systems, trigger workflows, and handle sensitive data. That's where security must be proactive, predictive, and prevention-first," said Nataly Kremer, Chief Product Officer at Check Point.

Veeam Data Platform v13 Raises the Bar for Cyber **Resilience and AI-Driven Protection**

Veeam Software has launched Veeam Data Platform v13, redefining cyber resilience with advanced AI-driven automation, forensic intelligence, and immutable security. Trusted by over 550,000 customers, Veeam's platform has long been a leader in data availability across cloud, virtual, physical, and SaaS environments. The v13 release builds on this legacy, introducing capabilities that help enterprises outsmart ransomware, accelerate clean recovery, and innovate confidently in the AI era.

"At Veeam, data protection is no longer a backup task—it's a strategic defense mission," said Anand Eswaran, CEO of Veeam Software. Central to v13 is Recon Scanner 3.0, delivering real-time visibility into adversary behavior and mapping threats to the MITRE ATT&CK framework for rapid remediation. Complementing this is the Malware Analysis AI Agent, which autonomously detects and classifies malicious activity, ensuring recovery from clean, verified backups—a critical safeguard as ransomware evolves.

Veeam has also embedded immutability by default, strengthened identity controls, and expanded integrations with security leaders like CrowdStrike, Palo Alto Networks, Splunk, and ServiceNow, bridging backup operations with threat response ecosystems.

ServiceNow and Microsoft Unite to Orchestrate Enterprise **AI at Scale**

ServiceNow has announced a new suite of integrations with Microsoft—including Microsoft Agent 365—ushering in a new era of enterprise AI orchestration, governance, and workflow integration. This collaboration combines Microsoft's trusted cloud infrastructure with ServiceNow's deterministic workflow intelligence to enable organizations to securely connect, govern, and scale AI agents across platforms.

The integrations go beyond basic AI tasks like summarization or chat. They empower AI agents to understand tasks, execute actions autonomously, and integrate seamlessly with enterprise workflows across Microsoft Teams, Outlook, Word, and SharePoint—while remaining governed, auditable, and compliant. "AI agents don't just assist—they collaborate, make decisions, and drive outcomes. But without orchestration, control, and governance, enterprise AI cannot scale safely," said Jon Sigler, EVP & GM, AI Platform at ServiceNow.

Central to this innovation is the AI Control Tower, powered by ServiceNow's CMDB, which integrates with Microsoft Copilot Studio and Foundry to provide real-time oversight into adoption, performance, risk, and ROI. Nirav Shah, CVP at Microsoft, emphasized, "Agent 365 gives organizations a simple, secure way to bring agents under control, extending the same infrastructure.

DIGEST

INITIAL LAUNCHES SAUDI ARABIA'S FIRST MOBILE ENGINEERING SERVICE FOR SMES

Initial has introduced Saudi Arabia's first mobile engineering service, a breakthrough solution designed to deliver fast, flexible, and cost-efficient building maintenance for small and medium enterprises (SMEs). Unveiled at the Smart Built Environment Forum in Riyadh, the service replaces traditional static on-site arrangements with rapid-response teams powered by IoT sensors, predictive analytics, and advanced diagnostics—ensuring faster decision-making and improved first-time fix rates.

"Mobile engineering finally gives SMEs the speed and reliability large corporations have long enjoyed," said Jason Ruehland, Group CEO of Initial.

IFS AND SIEMENS PARTNER TO BUILD THE AUTONOMOUS GRID OF THE FUTURE

IFS and Siemens have announced a strategic partnership aimed at transforming energy, utilities, and critical infrastructure through the convergence of Industrial AI and grid intelligence. This alliance combines Siemens' expertise in electrification and smart infrastructure with IFS's leadership in AI-powered asset management, field service optimization, and planning—addressing urgent challenges such as aging assets, supply chain disruptions, workforce shortages, and the global drive toward decarbonization.

As distributed energy resources like solar, wind, battery storage, and EVs reshape grid dynamics, complexity is soaring.

APPSFLYER LAUNCHES EIGHT AI-POWERED PRODUCTS TO DRIVE AUTONOMOUS MARKETING GROWTH

AppsFlyer has unveiled eight new products that mark its evolution from mobile attribution pioneer to a full-scale Modern Marketing Cloud built for the AI era. Designed to unify measurement, data collaboration, and automation, the new suite empowers enterprises to achieve intelligent, privacy-first growth at scale.

"The Modern Marketing Cloud represents the next evolution of our mission, uniting measurement, data collaboration, and AI into one trusted platform," said Oren Kaniel, CEO and Co-founder of AppsFlyer. "In the AI era, marketers don't just need better insights—they need autonomous growth engines powered by trusted, privacy-safe data."

MANAGEMENT MANTRA

"Leadership is not about being in charge. It's about taking care of those in your charge."
Simon Sinek

SentinelOne Showcases AI-Native Cybersecurity at Black **Hat MEA 2025**

SentinelOne, a global leader in AI-powered cybersecurity, is set to make a strong impact at Black Hat Middle East and Africa 2025, taking place from December 2–4 at the Riyadh Exhibition & Convention Center. The company will spotlight its Singularity Platform, an autonomous security ecosystem that unifies endpoint, identity, cloud, and data protection—helping enterprises innovate securely in the AI era.

A key highlight will be Mortal vs Machine, a live threat-hunting competition where human analysts face off against SentinelOne's agentic AI in real-time incident response scenarios. Scheduled daily from 12:30 PM to 12:50 PM, the activation will demonstrate how speed, precision, and automation redefine cybersecurity outcomes.

Visitors to Hall 1, Stand U121 can explore interactive demos, platform showcases, and expert-led sessions on critical topics, including AI-driven endpoint security, hyperautomation for cyber defense, and unified protection strategies. "The Middle East is entering a new era of digital acceleration, and AI is at the heart of every major transformation initiative," said Meriam ElOuazzani, Regional Senior Director at SentinelOne. "Our mission is to help organizations embrace this shift without compromising security."

As regional businesses adopt Generative AI, cloud-first strategies, and modern identity architectures.

Informatica and Microsoft Partner to Deliver Trusted Data **for Enterprise GenAI**

Informatica has announced advanced integrations with Microsoft's Foundry platform, strengthening its Intelligent Data Management Cloud (IDMC) to deliver trusted, governed, and enterprise-ready AI solutions. Unveiled at Microsoft Ignite 2025, this collaboration aims to help organizations build, deploy, and scale agentic AI applications powered by high-quality, compliant data.

"By integrating our CLAIRE AI engine and IDMC services with Microsoft Foundry, we help customers build AI agents and applications with confidence, compliance, and speed," said Krish Vitaldevara, Chief Product Officer at Informatica. The integration enables AI agents to access near real-time governed datasets through Informatica's Cloud Data Governance, Data Quality, and Master Data Management services using the Model Context Protocol (MCP).

To accelerate adoption, Informatica introduced new GenAI Recipes and agentic blueprints for Foundry, offering ready-to-deploy solutions for domains such as loan processing and insurance claims. These prebuilt templates significantly reduce development time, enabling enterprises to operationalize GenAI capabilities quickly.

ManageEngine Unveils Multi-Portal CloudSpend Architecture **for Next-Gen FinOps**

ManageEngine, the enterprise IT management division of Zoho Corporation, has launched an advanced multi-portal architecture for its CloudSpend platform, designed to transform FinOps for managed service providers (MSPs), cloud service providers (CSPs), and large enterprises operating multi-tenant cloud environments. This innovation addresses the growing complexity of cloud financial management as global public cloud spending is projected to exceed $723.4 billion in 2025.

The new architecture enables organizations to securely track, manage, and govern cloud costs across multiple clients or business units from a single interface—delivering unified visibility while maintaining strict data isolation and governance. "Service providers have long struggled to strike the right balance between visibility and isolation," said Srinivasa Raghavan, Director of Product Management at ManageEngine. "CloudSpend's multi-portal architecture bridges this gap by enforcing isolation and automated cost policies, helping organizations maximize profitability and ensure compliance."

Each tenant receives a dedicated environment with individualized budgets, alerts, workflows, and governance controls, all centrally managed through granular role-based access. Key capabilities include AI-driven anomaly detection and forecasting, intelligent cost-saving recommendations, automated billing and chargeback, and customizable white-labeled dashboards that reinforce client branding.

By simplifying multi-tenant cloud cost management, CloudSpend positions ManageEngine as a next-generation FinOps enabler—empowering organizations to foster financial accountability, scale operations confidently, and optimize cloud investments with precision.

Inception and Mirror Security Partner to Deliver Trusted AI **Security Solutions**

Inception, a G42 company and leading innovator in domain-specific AI, has announced a strategic partnership with Ireland-based Mirror Security, a global leader in GenAI-native cybersecurity. The collaboration aims to co-develop advanced security solutions designed to protect AI systems, agents, and data across government and enterprise environments—addressing one of the most pressing challenges in the AI era: trust.

As generative AI accelerates digital transformation, security remains the biggest barrier to enterprise-scale adoption. The World Economic Forum reports that 93% of cybersecurity leaders expect AI-driven threats to reshape the risk landscape within two years, yet only 5% of organizations feel confident in the security of their AI systems. This partnership seeks to close that gap by combining Inception's agentic AI capabilities with Mirror Security's AI-native protection technologies, including agentic security, automated red teaming, and encrypted AI processing.

"Unlocking AI's true potential demands innovation and uncompromising security," said Ashish Koshy, CEO of Inception. "Together, we will deliver dependable AI-for-security products that give customers confidence as they realize their AI ambitions." Pankaj Thapa, Co-founder and CEO of Mirror Security, added, "The convergence of regulatory pressure, advanced threats, and AI innovation requires new security paradigms. Our partnership ensures secure, scalable AI while eliminating data exposure risks."

Aligned with the UAE's vision to lead in trusted AI, this collaboration will accelerate the development of resilient AI ecosystems—where innovation is matched by governance, compliance, and confidence.

AVEVA Wins Microsoft Manufacturing Partner of the Year for **AI-Powered Industrial Transformation**

AVEVA, a global leader in industrial software and digital sustainability, has been named the 2025 Microsoft Manufacturing Partner of the Year for its excellence in delivering Azure-powered solutions that are redefining manufacturing and industrial operations. Selected from over 4,600 nominations across 100 countries, AVEVA stood out for its ability to help manufacturers harness cloud, AI, and real-time data to accelerate digital transformation, strengthen supply chains, and enable sustainable growth.

The award recognizes AVEVA's deep industry expertise and its long-standing collaboration with Microsoft to empower industrial organizations with secure, scalable platforms and AI-driven intelligence. A flagship solution is AVEVA CONNECT, built on Microsoft Azure, Microsoft Fabric, and advanced generative AI frameworks, which unifies people, processes, plants, and data to deliver real-time operational insights across complex ecosystems.

"We're proud to be named Microsoft's 2025 Manufacturing Partner of the Year," said Rob McGreevy, Chief Product Officer at AVEVA. "Pairing deep industrial domain expertise with hyperscale cloud intelligence can fundamentally reimagine what's possible in manufacturing."

Nicole Dezen, Chief Partner Officer at Microsoft, added, "Our partners harnessed the transformative power of Microsoft's Cloud and AI platforms to deliver solutions.

Nemetschek Group Showcases Digital Blueprint for Middle East's **Future at Big 5 Global 2025**

At Big 5 Global 2025, Nemetschek Group is spotlighting how AI, digital twins, and open collaboration are transforming the Middle East's construction and infrastructure landscape. As a Bronze Sponsor at the region's premier industry event, the global software leader is demonstrating how its portfolio—including ALLPLAN, Bluebeam, dTwin, Graphisoft, Solibri, Spacewell, and Vectorworks—empowers architects, engineers, and builders to deliver sustainable, intelligent, and future-ready built environments.

"The Middle East is a region of extraordinary ambition," said Marc Nezet, Chief Strategy Officer, Nemetschek Group. "Our mission is to drive transformation through open, connected, and intelligent solutions that enable human-centric, sustainable spaces." With giga-projects in Saudi Arabia and urban innovation in the UAE fueling a $264.4 billion construction market, Nemetschek is aligning with national strategies like Saudi Vision 2030 and UAE Net Zero 2050 by showcasing digital twins, AI-driven design optimization, and open BIM workflows.

Beyond the exhibition floor, Nemetschek executives are sharing insights at Big 5 Global Leaders' Summit and FutureTech Summit. Marc Nezet will discuss rethinking innovation for real impact, while Charles Sheridan, Chief Data and AI Officer, will deliver a keynote on AI's role in smarter tools and stronger buildings.

With over seven million users worldwide and a growing regional footprint, Nemetschek continues to lead digital transformation across the AEC/O sector. "Technology is reshaping construction," Nezet concluded. "Our goal is to ensure digitalization delivers meaningful impact—not just smarter buildings, but better cities for generations to come."

SECURITY THROUGH OPENNESS: A NEW APPROACH TO MANAGING VULNERABILITIES

The article argues that true cybersecurity is built on transparency, not secrecy. By openly disclosing and responsibly managing vulnerabilities, organizations strengthen trust, improve risk awareness, and demonstrate technical maturity. Clear, educational communication—rather than alarmism—helps employees and stakeholders understand real risks and respond effectively. A culture of openness encourages learning, accountability, and continuous improvement, ultimately making security a mark of quality rather than a hidden liability.

BASHAR BASHAIREH
AREA VP MIDDLE EAST, TÜRKIYE & NORTH AFRICA AT CLOUDFLARE

"True security can only be achieved through **open, transparent, and responsible** handling of vulnerabilities."

Transparency as a security principle

When it comes to cybersecurity, many organisations struggle to make the right decisions in the tension between protection and openness. Keeping vulnerabilities secret for as long as possible out of fear of reputational damage or misuse may be understandable – but it is not a solution. In a connected world, silence must not serve as a shield. True security can only be achieved through open, transparent, and responsible handling of vulnerabilities.

Employees as well as business partners do not expect absolute perfection, but a credible approach to managing risks. When companies disclose which security vulnerabilities have been identified, analysed, and resolved, they demonstrate control and a sense of responsibility. They also make it clear that transparency is not a liability, but a sign of technical maturity. This is how long-term trust is built – not by concealing problems, but by dealing with them openly and proactively.

Education, not Alarmism

Transparent security communication is not about spreading panic, but about educating. It is important not only to communicate that a vulnerability exists, but also which systems are affected, how high the actual risk is, and what countermeasures have been taken. Clear, factual language helps avoid misunderstandings and enables both employees and customers to take the right actions.

This type of education makes a significant contribution to security awareness – because only those who understand can respond appropriately. In this context, transparency also means fostering an open approach to mistakes in order to establish a climate of psychological safety, where learning and continuous improvement take priority.

Companies should encourage employees to report, for example, an accidental click on a phishing link without hesitation, and they should consistently prioritise transparency in communication as well as the prompt handling of security issues.

Realistic Risk Assessment Instead of Downplaying

Not every vulnerability is equally critical. Effective security communication makes clear why certain risks are classified as "low," "medium," or "high" – and how this assessment is reached. Such transparency helps people understand that security management always involves prioritisation. It prevents overreactions while also avoiding complacency. Those who understand the context are better equipped to assess the threat landscape realistically.

Where developers, security officers, communications teams, and management openly discuss vulnerabilities, a learning organisation emerges. This culture of open exchange strengthens security awareness across all areas – from code development to customer communication. In this way, security awareness is no longer seen as a mandatory training exercise, but as an integral part of the company culture.

Conclusion: View transparency as a strength, not a risk!

Open vulnerability reporting does not signal weakness but strength. It reflects accountability, a willingness to learn, and technical excellence.

An organisation that handles security vulnerabilities transparently reduces risks over the long term, strengthens stakeholder trust, and fosters a culture in which security is not seen as an obstacle, but as a mark of quality.

Bio of Author

Bashar Bashaireh is AVP Middle East, Türkiye & North Africa at Cloudflare. Based in Dubai, he leads the company's operations and team in the region. With over 25 years of experience in the technology and cybersecurity sectors, Bashar has held senior positions at several prominent companies. Before joining Cloudflare, he was the Senior Regional Director for the Middle East and Pakistan at Fortinet, where he was responsible for expanding the company's regional presence. He has also served as Managing Director and Head of Emerging Markets at Micro Focus, CEO of StarLink, and Regional Director at Symantec. His earlier career includes roles at Unify, Aruba, Fortinet, and 3Com. He holds a bachelor's degree in Electrical Engineering from the University of Jordan. MEA

ALLIED BLENDERS & DISTILLERS (ABD) INDIA BOOSTS OPERATIONAL EFFICIENCY WITH INTELLIGENT RPA FROM FINESSE

Strategic automation transforms multi-state reporting and accelerates ABD's digital journey without disrupting business continuity.

Allied Blenders & Distillers (ABD), one of India's leading spirits companies, has taken a decisive step toward digital transformation by partnering with Finesse to implement an intelligent Robotic Process Automation (RPA) framework powered by Automation Anywhere. This strategic initiative is revolutionizing ABD's multi-state reporting and operational workflows, delivering measurable efficiency gains without disrupting day-to-day business.

The Challenge: Manual Processes and Limited Visibility

Before automation, ABD's teams faced a time-consuming and error-prone process. To generate Management Information System (MIS) reports, staff manually accessed multiple state beverage corporation portals, downloaded data, and restructured it into Excel master sheets. Daily, weekly, and monthly reporting cycles consumed significant resources, increased the risk of inaccuracies, and limited real-time visibility into secondary sales and stock positions. These inefficiencies hindered decision-making and slowed operational agility across ABD's vast manufacturing and distribution network.

The Solution: Intelligent RPA for Seamless Automation

Finesse introduced a robust RPA solution designed to automate MIS reporting across all states. The system standardizes report formats, consolidates data, and leverages intelligent processing to enhance accuracy and speed. By eliminating repetitive manual tasks, ABD has unlocked real-time insights into sales and inventory, enabling faster, data-driven decisions.

Early results have been transformative. Reporting cycles that previously took hours are now completed in minutes, with near-zero errors. Departments across the organization report improved productivity, streamlined workflows, and enhanced collaboration.

"We are grateful to ABD Ltd. for trusting Finesse to streamline processes with RPA," said Gaurav Gupta, VP – Sales, Finesse.

"Our disciplined delivery and technical excellence ensured seamless execution, driving clear ROI and measurable business impact," added Manu Devadas, VP – Technology Services, Finesse.

Business Impact: Efficiency and Strategic Advantage

The benefits extend beyond operational speed. By automating MIS reporting, ABD has strengthened its ability to manage secondary sales and stock levels, ensuring better compliance and forecasting. The initiative supports ABD's broader digital transformation goals, positioning the company for sustained competitive advantage in India's dynamic spirits industry.

"The vastly increased operational efficiency we are now experiencing, thanks to Finesse's RPA tools, is extraordinary," said Manas Jena, Head – Automation & Revenue Growth Management at ABD Ltd.

"It has changed not only the way our organization operates on a day-to-day basis but also the breadth and scope of our automation and digitization strategy for the coming years."

MANAS JENA
HEAD – AUTOMATION & REVENUE GROWTH MANAGEMENT, ABD LTD.

"The vastly increased operational **efficiency we are now experiencing** is extraordinary."

MANU DEVADAS
VP – TECHNOLOGY SERVICES, FINESSE

"Our disciplined delivery ensured **seamless execution** and clear ROI."

GAURAV GUPTA
VP – SALES, FINESSE

"We are grateful to ABD for **trusting us to drive automation** excellence."

The Road Ahead: Scaling Intelligent Automation

This successful deployment marks the beginning of ABD's intelligent automation journey. Several additional processes have been identified for future automation and AI integration, signaling a long-term commitment to innovation. Finesse continues to work closely with ABD to expand the program's scope, ensuring that automation becomes a cornerstone of ABD's operational excellence.

Key Takeaways

- Challenge: Manual, Excel-heavy MIS reporting across multiple state portals.
- Solution: Intelligent RPA powered by Automation Anywhere, automating reporting and standardizing formats.
- Impact: Faster, accurate reporting; improved efficiency; enhanced visibility into sales and stock.

To access the complete article log on to: www.enterpriseitworld.com

2026: AI, CLOUD, AND CYBERSECURITY RESHAPE GLOBAL ENTERPRISE—MIDDLE EAST LEADS THE LEAP

From Riyadh to Silicon Valley, enterprises are racing to turn ambition into architecture.

A World on the Brink of Digital Reinvention

The global economy is entering a new era—one defined not by incremental change but by seismic shifts in technology. Worldwide IT spending is projected to surpass $5 trillion by 2026, according to Gartner, as enterprises scramble to embed artificial intelligence, cloud computing, and cybersecurity into their DNA. Yet, amid this global race, one region stands out for its audacity: the Middle East.

Saudi Arabia's Vision 2030 and the UAE's AI Strategy 2031 have transformed the Gulf into a digital laboratory for the future. IT spending in the region is expected to hit $169 billion, making it one of the fastest-growing digital economies globally. Governments are investing billions in hyperscale data centers, sovereign cloud platforms, and AI research hubs. Enterprises are accelerating transformation to meet consumer expectations for speed, security, and personalization.

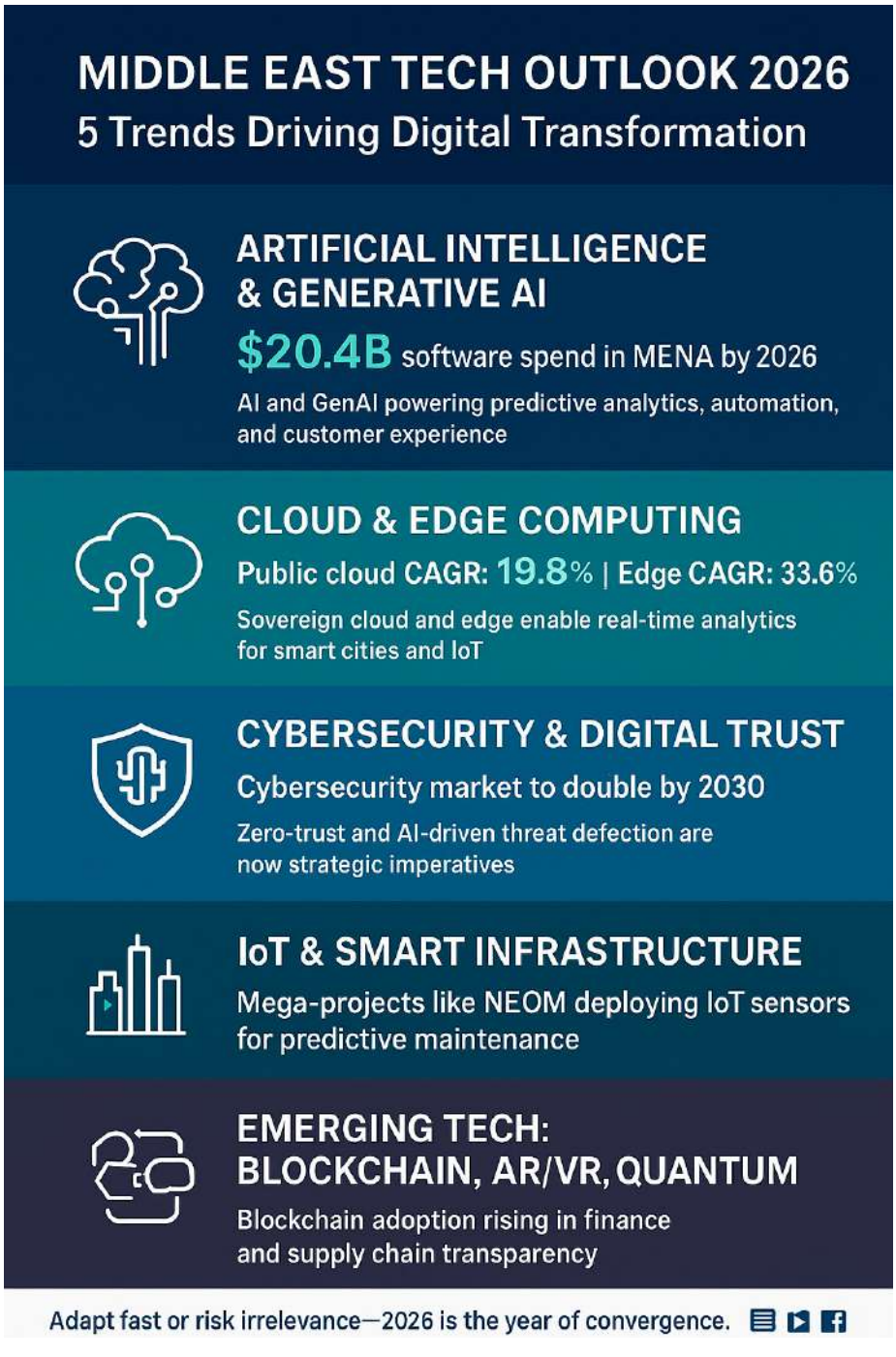
"The region isn't waiting to catch up—it's leapfrogging," says Mim Burt, VP at Gartner. "CIOs here are aligning entire business strategies around AI, not just experimenting with it."

AI Everywhere—But Governance Lags Globally

Artificial Intelligence is no longer a buzzword—it's the backbone of global transformation. From predictive analytics in finance to autonomous logistics in manufacturing, AI is embedded in every sector. Gartner predicts software spending in MENA will grow 13.9% to $20.4 billion, fueled by Generative AI integration across enterprise applications. Globally, McKinsey estimates AI could add $4.4 trillion annually to the world economy by 2030.

Yet, the paradox persists: while AI is everywhere, governance is nowhere. Mike Capone, CEO of Qlik, calls this phenomenon "AI dark matter."

"The question isn't whether AI delivers value—it's why most organizations are still dramatically underachieving," Capone explains. "Right now, AI is dark matter—shaping outcomes but invisible to governance. Walk the halls of any large company and you'll find people quietly using AI in documents, slides, and code every day. That's real productivity—but it's fragmented, ungoverned,



and rarely based on complete data."

Boston Consulting Group research confirms the paradox: only 5% of enterprises worldwide are structurally prepared for an AI future, even as generative tools proliferate at the edges of business. Capone predicts 2026 will be the year this changes.

"The winners will be the companies that turn hidden, ad-hoc AI usage into an explicit, governed system of decisions, where every agent and application stands on the same trusted data."

AI in Action

- Middle East: Saudi banks report a 40% reduction in fraud incidents after deploying AI-driven risk models.
- North America: U.S. healthcare providers use AI for predictive diagnostics, cutting patient wait times by 30%.
- Europe: German manufacturers leverage AI for predictive maintenance, reducing downtime by 25%.
- Asia-Pacific: Indian e-commerce giants deploy AI chatbots, handling 80% of customer queries autonomously.

Cloud and Edge—Sovereignty vs. Scale

Cloud computing is the backbone of digital transformation, but sovereignty is the new battleground. The Middle East is doubling down on sovereign cloud models to meet compliance and residency mandates. Globally, similar initiatives are underway: Europe's Gaia-X project aims to create a federated cloud ecosystem, while India's Digital Public Infrastructure is setting new benchmarks for data localization.

Edge computing is complementing this shift, enabling real-time analytics for smart cities, autonomous vehicles, and industrial IoT. Gartner predicts global edge spending will hit $317 billion by 2026, as intelligence moves closer to where data lives.

"Intelligence itself will start behaving more like a utility than a feature," says Capone. "As smaller models and local inference become mainstream, more decisions will be taken closer to where data lives—in factories, stores, vehicles and devices."

Global Smart City Projects

- Middle East: NEOM deploys edge-enabled IoT sensors for energy optimization.
- Asia: Singapore's Smart Nation initiative uses edge AI for traffic management.
- Europe: Barcelona integrates edge computing for real-time environmental monitoring.

Cybersecurity—The Universal Risk

Cybersecurity is no longer a defensive measure—it's a growth enabler. PwC Middle East warns that AI-driven attacks and quantum threats are rewrit-

MIM BURT
VP, GARTNER

"THE REGION ISN'T WAITING TO CATCH UP—IT'S LEAPFROGGING."

MIKE CAPONE
CEO, QLIK

"AI IS DARK MATTER—SHAPING OUTCOMES BUT INVISIBLE TO GOVERNANCE."

ANAND ESWARAN
CEO, VEEAM

"RESILIENCE IS THE NEW CURRENCY FOR DIGITAL ENTERPRISES."

ing the security playbook. Globally, the cybersecurity market is projected to reach $300 billion by 2026, driven by zero-trust architectures and AI-powered threat detection.

"Cybersecurity is about enabling trust and resilience," says PwC Middle East.

Francis deSouza of Google Cloud adds: "AI will rewrite the security playbook, turning SOCs into engines for automated action."

Veeam's Global Perspective: Resilience as the New Currency

Anand Eswaran, CEO of Veeam, underscores the urgency: "IT and business leaders are entering 2026 with unprecedented complexity. Cybersecurity and AI are today's reality—and accelerating. Organizations must prioritize data resilience and compliance while embracing innovation responsibly."

Key Global Findings from Veeam

- Cybersecurity threats dominate: 49% of IT leaders cite security as the biggest disruptor.
- AI-generated attacks: Seen as the most significant threat (66%), surpassing ransomware (50%).
- Recovery confidence: Only 29% of leaders feel very confident about recovering critical data after a zero-day exploit.

IoT, Blockchain, and Immersive Tech—Global Use Cases

IoT is transforming industries worldwide. In the Middle East, mega-projects like NEOM are deploying IoT sensors for predictive maintenance. In Asia, smart factories in Japan use IoT to optimize production lines. Blockchain is moving from hype to utility in global supply chains, while AR/VR is redefining retail and workforce training.

"Blockchain is moving from hype to utility in supply chain and fintech," says an IBM Middle East executive.

Global Examples

- Retail: U.S. brands use AR for immersive shopping experiences.
- Oil & Gas: Middle Eastern and North American firms deploy VR for safety training.
- Finance: European banks adopt blockchain for cross-border payments.

Act 5: Talent, Governance, and Sustainability

The global skills gap is widening—85 million jobs could go unfilled by 2030, according to Korn Ferry. Middle Eastern nations are investing heavily in digital academies, while global enterprises are embracing controlled decentralization to balance governance with agility.

"You can't rebuild your operating model every time the market swings," says Capone. "The companies we see winning keep governance and sovereignty non-negotiable, and push experimentation to the teams closest to the work."

Sustainability is also shaping IT strategies. Green data centers, energy-efficient AI models, and ESG compliance are becoming boardroom priorities worldwide.

Future Outlook: 2026–2030

- AI as a utility: Intelligence embedded everywhere, priced per decision.
- Global regulatory convergence: Harmonized AI and data laws across regions.
- Quantum computing: From labs to logistics optimization.
- Cyber accountability: Executive liability and ransomware bans gain traction.

Actionable Insights for CIOs Worldwide

- Governance first: Build frameworks for AI and data sovereignty.
- Resilience as strategy: Invest in backup, recovery, and compliance.
- Talent pipeline: Upskill for AI, cybersecurity, and cloud.
- Controlled decentralization: Empower teams without losing control.

Finally...

2026 will be a tipping point. The convergence of AI, cloud, cybersecurity, IoT, and immersive tech will reshape economies, industries, and societies. For enterprises, the mandate is clear: adapt fast or risk irrelevance.

"Over time, the price of intelligence per decision will go down, and the expectations for accountability will go up," Capone concludes. "Adapt fast or risk irrelevance," adds Gartner's Burt. MEA

"BladedFeline's evolving toolkit shows a clear **intent: persistent, stealthy access to high-value** government networks in Iraq and Kurdistan."

IRAN-ALIGNED BLADEDFELINE TARGETS IRAQI AND KURDISH OFFICIALS IN SOPHISTICATED CYBER-ESPIONAGE CAMPAIGN

ESET Research links BladedFeline to OilRig APT group as new tools Whisper and PrimeCache emerge in Operation RoundPress

ESET researchers have uncovered a major cyber-espionage campaign by BladedFeline, an Iran-aligned threat group targeting high-ranking officials in Iraq and the Kurdish region. The operation deployed an arsenal of custom-built tools designed for persistence and stealth, signaling a strategic push to maintain long-term access to sensitive government systems.

The investigation revealed two reverse tunneling utilities—Laret and Pinar—alongside supplementary tools, a custom backdoor named Whisper, and a malicious IIS module dubbed PrimeCache. These discoveries underscore BladedFeline's growing sophistication and its alignment with broader Iranian cyber objectives.

Whisper and PrimeCache: New Weapons in the Arsenal

Whisper operates by logging into compromised Microsoft Exchange webmail accounts and communicating with attackers via email attachments—a tactic that blends into normal traffic to evade detection. PrimeCache, a malicious IIS module, functions as a backdoor and shares code similarities with RDAT, previously attributed to the OilRig APT group.

Based on these overlaps and additional evidence, ESET assesses with high confidence that BladedFeline is a subgroup within OilRig, an Iran-aligned advanced persistent threat actor known for targeting governments and businesses across the Middle East.

Strategic Targets and Regional Motives

BladedFeline's objectives appear clear: sustained access to government networks for intelligence gathering. The group has previously compromised Kurdish diplomatic officials using its Shahmaran backdoor in 2023 and continues to exploit regional vulnerabilities. Recent activity includes targeting a telecommunications provider in Uzbekistan and expanding operations within Iraqi government entities.

Why these targets? Analysts point to Kurdistan's diplomatic ties with Western nations and its vast oil reserves—factors that make it a prime focus for Iranian cyber-espionage. In Iraq, the campaign likely aims to counter Western influence following years of geopolitical tension.

A Persistent Threat Since 2017

BladedFeline has been active since at least 2017, when it infiltrated systems within the Kurdistan Regional Government. It is not the only OilRig subgroup under ESET's watch. Another faction, Lyceum (also known as HEXANE or Storm-0133), focuses on Israeli organizations, including government and healthcare sectors. Together, these groups reflect a coordinated effort to advance Iran's strategic interests through cyber operations.

ESET expects BladedFeline to continue refining its implants and expanding its victim set. The group's emphasis on stealth and persistence suggests that future campaigns will leverage even more advanced techniques to bypass defenses.

Implications for Regional Security

The latest findings highlight the urgent need for governments and enterprises to strengthen cyber resilience. Embedding proactive security measures, monitoring for anomalous activity, and implementing robust incident response plans are critical to countering APT threats. As geopolitical tensions persist, cyber-espionage will remain a preferred tool for state-aligned actors seeking influence without direct confrontation. MEA

CYBERSECURITY THREATS AND AI DISRUPTIONS TOP IT LEADERS' CONCERNS FOR 2026, VEEAM SURVEY REVEALS

Majority Back Ransomware Payment Ban as AI-Driven Attacks and Compliance Pressures Redefine Data Resilience Strategies

As 2026 approaches, IT leaders worldwide are bracing for a year of unprecedented complexity. According to Veeam® Software's latest global survey of over 250 senior IT and business decision-makers, two forces dominate the risk and disruption landscape: cybersecurity threats and the impact of AI maturity and regulation. These findings underscore a seismic shift in priorities as organizations navigate a volatile environment shaped by technological acceleration, compliance mandates, and evolving attack vectors.

Cybersecurity and AI: The Twin Disruptors of 2026

Nearly half (49%) of respondents identified cybersecurity threats as the single biggest disruptor for the coming year. AI maturity and regulation followed closely at 22%, signaling that artificial intelligence is no longer just a productivity enabler—it's a double-edged sword. While AI promises efficiency and innovation, its weaponization by malicious actors is emerging as the most significant threat to data security.

The survey revealed that AI-generated attacks (66%) now surpass ransomware (50%) as the top perceived risk, marking a dramatic evolution in the threat landscape. This shift reflects growing concerns that generative AI tools, once hailed for their transformative potential, are being exploited to craft sophisticated, automated attacks at scale.

Regional Insights: Middle East and Global Trends

In the Middle East, where digital transformation is accelerating under ambitious national strategies, the stakes are even higher. Governments and enterprises are investing heavily in cloud adoption and AI-driven services, but these advances come with heightened exposure to cyber threats. Regional experts warn that compliance with emerging data sovereignty laws—such as those in the UAE and Saudi Arabia—will be critical for organizations operating across borders.

Globally, similar patterns are emerging. In Europe, GDPR enforcement is tightening, while Asia-Pacific markets are introducing stricter localization requirements. For multinational organizations, this means navigating a patchwork of regulations while maintaining operational agility—a challenge that demands robust governance frameworks and resilient infrastructure.

The Risk Readiness Gap: Cyberattacks and AI Missteps Loom Large

When asked which risks they felt least prepared for, IT leaders pointed to cyberattacks (29%) and AI/automation missteps (27%). Despite years of investment in cybersecurity, confidence in recovery remains alarmingly low. Only 29% of respondents expressed strong confidence in their ability to recover critical data following a zero-day exploit, while 59% admitted they were only "somewhat confident."

Cloud outage preparedness is equally concerning: 71% of organizations are either not confident or only somewhat confident in maintaining operations during a multi-day cloud provider outage. These figures highlight a critical vulnerability in resilience strategies, especially as multi-cloud and SaaS adoption accelerates.

Data Visibility: A Growing Blind Spot

The complexity of modern IT environments is eroding visibility. A staggering 60% of respondents reported reduced clarity on where their data resides due to the proliferation of multi-cloud and SaaS platforms. This lack of transparency not only hampers compliance efforts but also complicates recovery planning, leaving organizations exposed to regulatory and operational risks.

Compliance and Sovereignty: The New Battleground

Beyond technical resilience, regulatory pressures are reshaping cloud strategies. Data sovereignty emerged as a top priority, with 46% of leaders rating it "extremely important" and another 30% deeming it "moderately important." This trend reflects a growing recognition that resilience is not merely a technical challenge—it's geopolitical and regulatory. Organizations are preparing for a world where control over data location is as critical as firewalls and backups.

Budget Priorities: Security and Resilience Take Center Stage

In response to these mounting risks, IT leaders are doubling down on security and resilience initiatives. Strengthening cybersecurity was ranked as the single "must-win" IT initiative for 2026 by 45% of respondents, followed by building data resilience (24%). Budgets are following suit: 54% of organizations plan moderate or significant increases in spending on data protection and resilience in the coming year.

The Call for Accountability and Higher Standards

The survey also revealed a strong appetite for governance reforms. 72% of respondents support a ban on ransomware payments, with 51% strongly backing the measure. This stance reflects growing frustration with the cycle of payouts that perpetuate criminal activity. Additionally, 88% believe it will be critical to ensure partners and suppliers meet stringent cybersecurity and data protection standards, signaling a shift toward ecosystem-wide accountability.

Executive responsibility is also under scrutiny. 41% of leaders believe increased executive-level accountability would have a major impact on improving cybersecurity posture, while another 31% see it as moderately impactful. These findings suggest that resilience is no longer confined to the IT department—it's a boardroom imperative.

ANAND ESWARAN
CEO, VEEAM

"Cybersecurity and AI are today's reality – and accelerating **in 2026. Organizations must prioritize data resilience and** compliance while embracing innovation responsibly."

Expert Commentary: Navigating Complexity with Confidence

"IT and business leaders are entering 2026 with unprecedented complexity," said Anand Eswaran, CEO of Veeam. "Cybersecurity and AI are today's reality—and accelerating in 2026. Organizations must prioritize data resilience and compliance while embracing innovation responsibly. At Veeam, we see this as an opportunity to lead with trust, security, and simplicity."

Industry analysts echo this sentiment. According to Gartner, by 2026, 75% of organizations will face AI-driven cyberattacks, and those without adaptive security architectures will suffer disproportionately. IDC predicts that global spending on cybersecurity will exceed $250 billion, driven by investments in AI-based threat detection and zero-trust frameworks.

Illustrative Scenario: The AI-Powered Attack

Imagine a financial services firm leveraging AI for customer engagement. In early 2026, attackers deploy generative AI to craft hyper-personalized phishing emails that bypass traditional filters. Simultaneously, automated bots exploit API vulnerabilities, exfiltrating sensitive data within hours. The firm's lack of visibility across its multi-cloud environment delays detection, resulting in regulatory fines and reputational damage. This scenario underscores why AI-driven threats require AI-driven defenses—and why resilience must be proactive, not reactive.

Actionable Recommendations for CIOs and CISOs

To thrive in this high-stakes environment, IT leaders should adopt a multi-pronged strategy:

- **Invest in AI-Enhanced Security Tools**
Deploy machine learning-based threat detection and behavioral analytics to counter AI-generated attacks.
- **Implement Zero-Trust Architecture**
Assume breach and enforce strict identity and access controls across all environments.
- **Enhance Data Visibility**
Utilize unified dashboards and automated discovery tools to map data across multi-cloud and SaaS platforms.
- **Prioritize Compliance and Sovereignty**
Align cloud strategies with local regulations and maintain auditable control over data location.
- **Strengthen Recovery Confidence**
Regularly test backup and disaster recovery plans under simulated zero-day and outage scenarios.
- **Embed Governance and Accountability**
Elevate cybersecurity to a board-level priority and enforce partner compliance through contractual obligations.
- **Prepare for Ransomware Ban Scenarios**
Develop contingency plans that assume no ransom payments, focusing on rapid isolation and recovery.

Conclusion: A Year of High Stakes and Higher Standards

The Veeam survey paints a sobering picture of the challenges ahead, but it also offers a roadmap for action. By aligning investments with emerging risks and fostering a culture of accountability, IT leaders can turn disruption into opportunity. In a world where data is both an asset and a target, resilience is not optional—it's existential. MEA

DXC LAUNCHES ADVISORYX, WARNS OF WIDENING GLOBAL AI EXECUTION GAP

New research reveals high boardroom intent but weak readiness as enterprises struggle to scale AI responsibly

DXC Technology has unveiled AdvisoryX, a global advisory and consulting group designed to help enterprises navigate the complexities of AI adoption, operating-model redesign, and large-scale technology transformation. The launch comes amid sobering findings from DXC's inaugural global study, which reveals a widening gap between AI ambition and execution across industries.

AI: A Boardroom Priority, But Execution Lags

The AdvisoryX research, based on responses from 2,496 global technology and business leaders, paints a clear picture: AI has become an executive-level priority, with 77% of leaders identifying it as central to boardroom agendas and 30% planning to deploy agentic AI within months. Yet, despite this urgency, 65% of organizations admit they cannot build a clear business case for AI, and an overwhelming 94% face significant challenges in deploying AI at scale.

This contradiction—high intent but weak readiness—is delaying enterprise-wide value creation. Many organizations are still approaching AI with a "projects, not platforms" mindset, limiting scalability and long-term impact.

The AI Execution Gap: What's Driving It?

DXC's study highlights several structural barriers:

- **Foundational Gaps:** Lack of robust data governance, platform architecture, and security frameworks.
- **Cultural Resistance:** Difficulty in aligning people and processes with AI-driven workflows.
- **Risk and Compliance Concerns:** Uncertainty around regulatory frameworks and ethical AI standards.
- **Fragmented Strategies:** AI initiatives often siloed within departments, preventing enterprise-wide integration.

Pete McEvoy, Global Head of AdvisoryX, summed it up: "AI is now a boardroom priority, but most organizations still lack the foundations to scale it responsibly."

Future of Work: Hybrid Human-AI Models

The research also signals profound changes in workforce dynamics. 50% of leaders expect hybrid human-AI decision models to become standard, while 81% predict AI will increase workforce demand—particularly in IT, data, cybersecurity, and software development—by 2028. Far from replacing jobs, AI is expected to create new roles and skill requirements, intensifying the need for reskilling and talent development.

AdvisoryX: DXC's Answer to the AI Challenge

AdvisoryX integrates DXC's capabilities across strategy, operations, technology, people and culture, finance, risk, and user experience. By combining consulting-led engagement with DXC's engineering heritage, the group aims to help enterprises:

- Diagnose gaps in AI readiness.
- Design future operating models.
- Execute transformation with measurable outcomes.

To close the execution gap, DXC has introduced five integrated AdvisoryX solutions covering the full lifecycle of enterprise AI:

- AI Core – Foundational data, governance, and platform architecture.
- AI Reinvent – Industry-specific, scalable use cases across autonomous and human-assisted models.
- AI Interact – Redesigned workflows and natural interfaces for seamless human-AI collaboration.
- AI Validate – Continuous testing, safety, and quality assurance to ensure responsible AI deployment.
- AI Manage – Full lifecycle and production operations for sustained impact.

Strategic Shift: DXC's AI-Driven Future

The launch of AdvisoryX coincides with DXC's refreshed global brand identity, signaling a strategic pivot toward an AI-first future. This approach emphasizes responsible scaling, measurable business outcomes, and sustainable enterprise-wide impact—not just technology adoption.

Why This Matters for Enterprises

The widening AI execution gap is more than a technical challenge—it's a strategic risk. Organizations that fail to bridge this gap risk falling behind in innovation, competitiveness, and compliance. AdvisoryX aims to address this by offering end-to-end guidance, from diagnosis to deployment, ensuring that AI initiatives deliver tangible business value.

Actionable Takeaways for CIOs and CEOs

To close the AI execution gap, DXC recommends:

- Build a Strong Foundation: Invest in data governance, security, and scalable platforms before deploying AI.
- Adopt a Platform Mindset: Move beyond isolated projects to enterprise-wide AI strategies.
- Focus on People and Culture: Drive change management and reskilling initiatives to support hybrid human-AI models.
- Embed Risk and Compliance: Integrate

PETE MCEVOY
GLOBAL HEAD, ADVISORYX, DXC TECHNOLOGY

"Cybersecurity and AI are today's reality – and accelerating **in 2026. Organizations must prioritize data resilience and** compliance while embracing innovation responsibly."

ethical AI frameworks and regulatory compliance into every stage of deployment.

- Measure Outcomes: Define clear KPIs for AI initiatives to track business impact and ROI.

Conclusion: From Ambition to Action

AI is no longer optional—it's existential. But ambition without execution is a recipe for stagnation. DXC's AdvisoryX offers a blueprint for turning intent into impact, helping enterprises scale AI responsibly and sustainably. As McEvoy puts it: "The future belongs to organizations that can operationalize AI at scale—securely, ethically, and with measurable outcomes." MEA

MANUFACTURING BLOCKS MORE RANSOMWARE ATTEMPTS, BUT ADVERSARIES PIVOT TO DATA THEFT AND EXTORTION

Sophos report reveals falling encryption rates, rising double extortion tactics, and mounting pressure on leadership as cybercriminals exploit operational vulnerabilities

The manufacturing industry is fighting back against ransomware—but the battle is far from over. According to the Sophos State of Ransomware in Manufacturing and Production 2025 report, manufacturers are stopping more attacks before data can be encrypted, yet adversaries are shifting tactics toward data theft and extortion-only campaigns. This evolution underscores a sobering reality: even as defenses improve, attackers are finding new ways to maintain leverage.

Based on an independent survey of 332 manufacturing organizations hit by ransomware in the past year, the report paints a nuanced picture of progress and persistent risk. Encryption rates have dropped to their lowest level in five years, but ransom payments remain high, and operational stress continues to ripple across leadership teams.

Key Findings: Progress Meets Persistent Threats

- Encryption Rates Fall, But Extortion Rises: Only 40% of attacks resulted in data encryption, down from 74% last year—a sign of stronger early detection. However, extortion-only attacks surged to 10%, up from just 3% in 2024, as adversaries increasingly rely on stolen data for leverage.
- **Data Theft Persists:** Among organizations that experienced encryption, 39% also had data stolen, one of the highest rates across all sectors surveyed. This trend reflects the growing dominance of double extortion tactics, where attackers encrypt data and threaten to leak it unless paid.
- **Improved Attack Interception:** 50% of manufacturers stopped attacks before encryption, more than double last year's 24%. This progress highlights the impact of layered defenses and proactive monitoring.
- **Expertise Gaps Fuel Vulnerability:** Lack of in-house expertise was cited by 42.5% of respondents, while unknown security gaps (41.6%) and inadequate protection (41%) were also major contributors. On average, organizations identified three internal factors that enabled the attack.
- **Ransom Payments Remain High:** Despite improved defenses, 51% of manufacturers with encrypted data paid the ransom, with a median payment of $1 million against a median demand of $1.2 million.
- **Recovery Costs Decline, Timelines Improve:** The average recovery cost (excluding ransom) fell by 24% to $1.3 million, and 58% of manufacturers fully recovered within one week, up from 44% last year.
- **Leadership Under Pressure:** 47% reported increased team stress, 44% faced heightened pressure from senior leaders, and 27% experienced leadership changes following an attack.

"Manufacturing depends on interconnected systems where even brief downtime can halt production and ripple across supply chains," said Alexandra Rose, Director of Threat Research, Sophos Counter Threat Unit. "Attackers exploit this pressure: despite encryption rates falling to 40%, the median ransom paid still reached $1 million. While half of manufacturers stopped attacks before encryption, recovery costs average $1.3 million and leadership stress remains high. Layered defenses, continuous visibility, and well-rehearsed response plans are essential to reduce both operational impact and financial risk."

The Bigger Picture: Why Manufacturing Is a Prime Target

Manufacturing organizations operate in a high-stakes environment where downtime translates directly into lost revenue and disrupted supply chains. Attackers understand this urgency and exploit it, betting that victims will pay quickly to resume operations. The sector's reliance on legacy systems, operational technology (OT), and complex vendor ecosystems creates fertile ground for exploitation.

Adversary Behavior: Double Extortion Dominates

Sophos X-Ops observed 99 distinct ransomware groups targeting manufacturing over the past year. Prominent actors include:

- GOLD SAHARA (Akira)
- GOLD FEATHER (Qilin)
- GOLD ENCORE (PLAY)

In more than half of incidents handled by Sophos Emergency Incident Response, attackers both stole and encrypted data, reinforcing the dominance of double extortion tactics. Leak sites have become a critical pressure point, where stolen data is published if victims refuse to pay.

Operational Fallout: Stress and Leadership Shake-Ups

Beyond financial costs, ransomware attacks exact a heavy toll on organizational culture. Nearly half of respondents reported increased stress among IT and security teams, while leadership pressure intensified in 44% of cases. Alarmingly, 27% of organizations experienced leadership changes following an attack—a stark reminder that cybersecurity failures can reshape corporate governance.

Sidebar: By the Numbers

- 40% – Encryption rate in manufacturing (down from 74%)
- 10% – Extortion-only attacks (up from 3%)
- $1M – Median ransom paid
- $1.3M – Average recovery cost (excluding ransom)
- 58% – Organizations fully recovered within one week

Strengthening Defenses: Sophos Recommendations

Eliminate Root Causes: Address common technical and operational weaknesses, such as unpatched vulnerabilities. Tools like Sophos Managed Risk can help assess exposure and reduce risk.

ALEXANDRA ROSE
DIRECTOR OF THREAT RESEARCH
SOPHOS

"Despite encryption rates falling to 40%, the **median ransom paid still reached $1 million.** Attackers are adapting faster than defenses."

Defend Every Endpoint:
Deploy dedicated anti-ransomware defenses across all endpoints, including servers, to prevent attackers from gaining a foothold.

Plan and Prepare:
Establish and routinely test a comprehensive incident response plan. Maintain reliable backups and practice restoration to minimize downtime.

Monitor Around the Clock:
Continuous visibility is critical. Organizations lacking in-house resources should partner with a Managed Detection and Response (MDR) provider for 24/7 monitoring and expert response.

Expert Insight: The Road Ahead

Sophos predicts that ransomware actors will continue refining their tactics, leveraging data theft, supply chain compromises, and AI-driven attack automation to outpace defenses. For manufacturers, resilience will hinge on proactive risk management, investment in skilled personnel, and collaboration with trusted security partners.

Future Outlook: A Sector Under Siege

While encryption rates are falling, the rise of extortion-only attacks signals a dangerous pivot. Manufacturing organizations must recognize that data theft is now the primary weapon in the ransomware arsenal. The challenge is not just technical—it's strategic. Cybersecurity must become a board-level priority, integrated into every facet of operations. MEA

INSIDE THE INDUSTRIALIZATION OF CYBERCRIME: WHAT TO EXPECT IN 2026

Automation, AI scale, and machine-speed operations will redefine the global cyberthreat landscape

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

From Innovation to Throughput

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

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

The Next Generation of Offense

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

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

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

The Evolution of Defense

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

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

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

Collaboration and Deterrence

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

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

Looking Ahead

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

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

Velocity and scale will define the decade ahead. Organizations that unify intelligence, automation, and human expertise into a single, responsive system will be the ones best able to withstand what comes next. Read the full Fortinet 2026 Cyberthreat Predictions report to explore detailed forecasts, sector-specific insights, and strategies for building resilience in the era of industrialized cybercrime. MEA

DEREK MANKY
CHIEF SECURITY STRATEGIST AND GLOBAL VICE-PRESIDENT, THREAT INTELLIGENCE, FORTINET.

"Cybercrime is no longer just evolving—it is **industrializing at a scale that requires defenders to** operate at machine speed,"

ENDAVA REVEALS READINESS GAP AS UAE AND SAUDI ORGANISATIONS HEAD TOWARD AI-NATIVE FUTURES

New research shows strong ambition for AI-native transformation, but operational foundations and responsible adoption remain key challenges

Organisations across the UAE and Saudi Arabia are racing toward an AI-native future, but many lack the operational readiness to make it a reality, according to new research from Endava. The study, based on senior business leaders in both markets, highlights a growing appetite for agentic AI—systems capable of autonomous, self-improving operations—yet reveals gaps in funding, governance, and foundational capabilities.

AI-Native: A Strategic Imperative

The research shows overwhelming consensus on the importance of AI-native transformation: more than nine in ten respondents believe it is essential to maintaining a competitive edge. Many organisations have mapped out strategies, but execution remains uneven. Over a third report that while an AI-native roadmap exists, budgets to implement it have not yet been secured.

Despite these hurdles, optimism is strong. Three-quarters of leaders expect their organisations to achieve an AI-native operating model by 2028, signaling an accelerated shift over the next three years.

Agentic AI Reshaping Innovation

Adoption of agentic AI is already changing how innovation happens across the Gulf. 73% of respondents say traditional agile methodologies are losing relevance as firms move toward autonomous systems capable of managing complex processes in real time. This trend is most visible in fintech, where 81% believe agentic AI is creating new business models and revenue streams, lowering barriers to entry and intensifying competition.

Leaders also see transformative potential in customer experience and operational resilience. Agentic AI promises stronger fraud detection, personalised financial guidance, and faster, always-on service, while enhancing organisational robustness through automated compliance and real-time risk management.

The Readiness Gap

Momentum aside, the study reveals that 85% of organisations are still focused on basic AI applications—such as chatbots, predictive analytics, and workflow automation—before progressing to advanced agentic systems. Concerns around data privacy, security, and transparency continue to slow adoption, while data quality and cybersecurity risks rank among the most significant barriers.

To bridge this gap, organisations are embedding ethical guidelines into AI development (50%), aligning systems with regulatory requirements (42%), and strengthening data privacy protections (41%). These steps reflect a growing commitment to responsible AI integration as the region moves toward an AI-native future.

"Organisations in the UAE and Saudi Arabia are at a pivotal moment," said David Boast, General Manager – UAE & KSA, Endava. "There is a clear understanding of the value that an AI-native future can unlock, but also a recognition that responsible adoption is essential. Those that invest in agentic AI with strong governance frameworks today will be best placed to lead the next wave of innovation across the region."

Looking Ahead

As AI-native ambitions accelerate, success will depend on closing readiness gaps, building trust, and embedding governance into every stage of transformation. For organisations that act now, the rewards include greater agility, resilience, and competitive advantage in an increasingly digital economy. MEA

DAVID BOAST
GENERAL MANAGER – UAE & KSA, ENDAVA

"Those that invest in agentic AI with **strong governance today will lead** the next wave of innovation."

ADI BLEIH
CHECK POINT SOFTWARE TECHNOLOGIES

"One compromised dependency **can become a direct pathway into** your cloud and CI/CD systems."

SHAI-HULUD 2.0: THE SUPPLY CHAIN ATTACK THAT REDEFINED RISK

A highly coordinated npm campaign exposed tens of thousands of repositories, proving how a single dependency can open the door to cloud and CI/CD compromise.

The JavaScript ecosystem has been rocked by one of the most aggressive supply chain attacks of 2025. Dubbed Shai-Hulud 2.0—or "The Second Coming" by its operators—the campaign unfolded between November 21 and 23, compromising over 600 npm packages and 25,000 GitHub repositories in mere hours. The fallout? Thousands of leaked developer and cloud credentials, and a stark reminder of the fragility of modern software supply chains.

Unlike traditional malware that activates post-installation, Shai-Hulud 2.0 weaponized the npm preinstall lifecycle script, allowing its payload to execute even if installation failed. This gave attackers early access to development environments, bypassing conventional defenses. Adding to its stealth, the campaign used the Bun runtime instead of Node.js, evading standard detection tools while siphoning secrets from AWS, Azure, GCP, SSH keys, GitHub tokens, and CI/CD pipelines.

A New Level of Sophistication

Once triggered, the malware harvested environment variables and credentials, packaged them into JSON files, and uploaded them to attacker-controlled GitHub repositories. It then established persistence by registering infected systems as self-hosted GitHub runners, inserting rogue workflow files, and enabling automated propagation across the JavaScript ecosystem. In some cases, a destructive failsafe wiped local files if containment was detected.

The scale of exposure is staggering. Check Point's analysis uncovered 14,206 leaked secrets, including 2,485 still valid, impacting 487 GitHub organizations. Multi-cloud environments and developer pipelines were directly compromised, illustrating how dependency-level attacks can escalate into systemic breaches.

"Shai-Hulud 2.0 is a highly coordinated supply chain attack with an unusually aggressive execution chain. By activating before installation completes and exfiltrating secrets into attacker-controlled GitHub repositories, the operators gained rapid access to significant volumes of cloud and developer credentials. Our analysis of more than 20,000 repositories created as part of the campaign shows the breadth of the exposure. This type of incident demonstrates how a single dependency can become a direct pathway into CI and CD systems and cloud environments. The scale and speed of the spread resemble some of the most disruptive supply chain incidents we have seen in recent years, and it carries echoes of the widespread ripple effects seen during Log4j. Organizations should act immediately by auditing dependencies, rotating all potentially exposed secrets and securing their build pipelines."— Adi Bleih, Security Researcher, External Risk Management, Check Point Software Technologies

What Organizations Must Do Now

Security experts urge immediate action for any enterprise using npm:

- Audit dependency manifests and lockfiles to identify compromised packages.
- Clear npm caches and remove infected modules.
- Rotate all secrets—cloud keys, GitHub tokens, CI/CD credentials.
- Inspect GitHub runners and workflows for unauthorized changes.

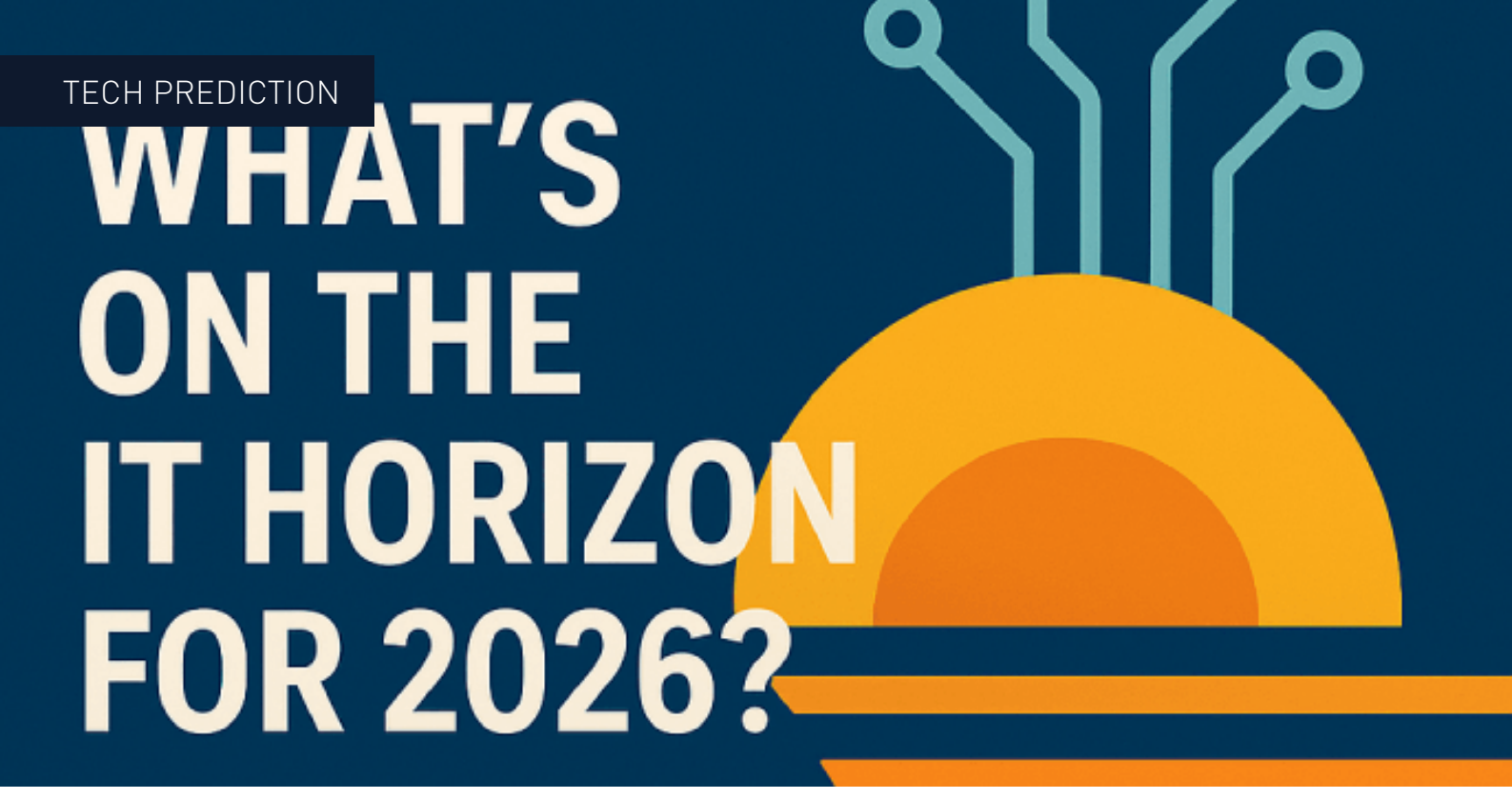
Preventive measures include enforcing multi-factor authentication (MFA), implementing SBOM-based scanning, monitoring for unexpected repositories, and isolating CI/CD environments to reduce blast radius.

The Bigger Picture

Shai-Hulud 2.0 is more than a breach—it's a warning. By exploiting overlooked lifecycle scripts and alternative runtimes, attackers demonstrated how innovation in attack vectors can outpace traditional defenses. As software supply chains grow more complex, organizations must adopt continuous monitoring, zero-trust principles, and multi-layered security frameworks to safeguard developer ecosystems.

Bottom line:

The Second Coming of Shai-Hulud underscores a harsh truth—every dependency is a potential breach point. For enterprises, the mandate is clear: secure your pipelines, harden credentials, and treat supply chain security as a first-class priority. MEA



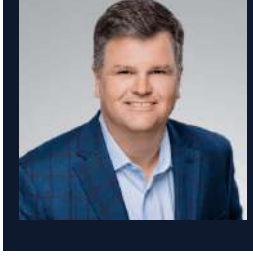
WHAT'S ON THE IT HORIZON FOR 2026? INFOBLOX EXPERTS WEIGH IN

As the pace of technological change accelerates, 2026 is shaping up to be a defining year for IT and cybersecurity. The breakthroughs of 2025—AI-powered innovation, tightening global regulations and the escalating complexity of cloud and network environments—have pushed IT teams into a new era of constant adaptation. In the year ahead, that evolution will only intensify. From AI-driven cyberthreats and the rise of autonomous security operations to an expanding attack surface across IoT, cloud and supply chains, Infoblox experts reveal what IT leaders should expect—and prepare for—as they navigate the fast-moving landscape of 2026.

2025 has proven itself to be a groundbreaking year for networking, security and cloud. With the proliferation of AI technologies, new global regulations and the growing complexity of cloud infrastructure, IT teams have found themselves on constantly shifting sands.

That state of flux is only set to accelerate in 2026. IT teams shouldn't just try to weather the storm; they need to be dynamic and adaptive, leaning into new approaches and continuously staying ahead of emerging threats.

To help teams prepare for what's next, Infoblox experts shared their predictions for how the IT landscape will evolve in 2026. MEA

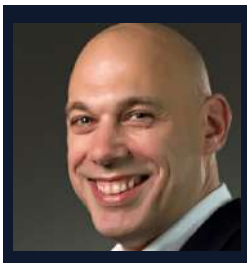


SCOTT HARRELL
CHIEF EXECUTIVE OFFICER

The mass personalization of cyberattacks will disrupt the classical kill chain model, making it more challenging for security teams to predict and prevent attacks—and making it more likely organizations will be patient zero. With AI, attackers can tailor their strategies to target specific individuals or organizations, rendering traditional defense mechanisms less effective. This shift will require security teams to develop new approaches to detect and mitigate highly personalized threats.

BRAD RINKLIN
CHIEF MARKETING OFFICER

Polymorphic and sentient malware will become more prevalent, posing a significant threat to cybersecurity. This type of malware will be capable of changing its code and behavior to avoid detection, making it harder for security systems to identify and neutralize it. The emergence of sentient malware will mark a new era in cyberthreats, where AI-driven attacks become increasingly sophisticated and resilient. It's critical to invest in advanced detection and response capabilities to stay ahead of these evolving threats.



CRAIG SANDERSON
PRINCIPAL CYBERSECURITY STRATEGIST

The hyper-personalization of attacks, as seen in Japan, will become more prevalent, making it harder to defend against targeted threats. Attackers will increasingly tailor their strategies to specific individuals or organizations, rendering traditional defense mechanisms less effective. This trend will require security teams to develop new approaches to detect and mitigate highly personalized threats. The challenge will be to stay one step ahead of attackers who are becoming more sophisticated in their methods. The obvious technological shift will be the use of AI in threat intelligence generation and a new approach that targets the infrastructure threat actors use, rather than targeting each campaign.

COLEMAN MEHTA
HEAD OF GLOBAL PUBLIC POLICY AND STRATEGY

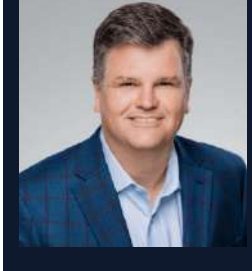
In 2026, the ease of executing attacks without technical proficiency will lead to an increase in cyberthreats. As attack tools become more user-friendly, individuals who previously lacked the skills to launch cyberattacks will now be able to do so. This will result in a surge of cyberthreats. The democratization of cyberattack capabilities will pose a significant challenge for global cybersecurity efforts.

CHRIS USSERMAN
GLOBAL PUBLIC SECTOR CHIEF TECHNOLOGY OFFICER

Cybercrime-as-a-service will supercharge financially motivated threat actors. Financially motivated groups are no longer limited by their in-house skills, largely fueled by an AI-enabled ecosystem. In 2026, they'll further expand their capabilities by tapping into a maturing cybercrime-as-a-service ecosystem, outsourcing everything from exploit kits to credential dumps and initial access brokers. This further industrialization of cybercrime will continue to blur the line between opportunistic and highly skilled adversaries, accelerating the pace and impact of financially motivated attacks.

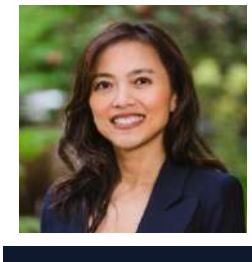
JOHN WOJCIK
SENIOR THREAT RESEARCHER

In 2026, we will see a significant acceleration of automation within the cyber-enabled fraud industry in Southeast Asia. This region will face substantial challenges as cybercriminals and scam centers respond to mounting law enforcement pressure by increasing their rate of AI-driven tool adoption and integration amidst disruptions within their human labor supply chains. The use of deepfake software suites and jailbroken large language models for social engineering will become more prevalent, making it increasingly difficult to detect and prevent fraud. This shift will require a concerted effort to detect, let alone address and mitigate the growing threats.



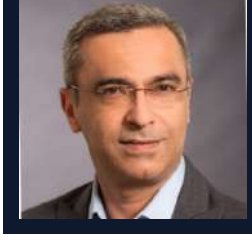
SCOTT HARRELL
CHIEF EXECUTIVE OFFICER

As cloud infrastructure grows more dynamic and complex, the traditional human-led troubleshooting model is reaching its limits. Even without AI, the sheer scale and fluidity of modern cloud environments, combined with intricate networking and security layers, already challenge human comprehension. Add intelligent agents into the mix, and we're entering a world where machines not only detect anomalies faster than humans but also resolve them in ways that are too fast, too subtle and too interconnected for manual intervention. This represents a paradigm shift where human troubleshooting becomes obsolete and trust in autonomous systems becomes essential.



DANELLE AU
VICE PRESIDENT, PRODUCT MARKETING

In 2026, SOC teams will increasingly use AI to reduce the burden on analysts, improving efficiency and effectiveness. By automating routine tasks like triage, forensic collection and real-time data correlation, AI will allow analysts to focus on more complex and strategic issues. The integration of AI into SOCs will be a game-changer for the cybersecurity industry.



FARAZ ALADIN
VICE PRESIDENT, TECHNICAL MARKETING

Security teams will need to undergo a mindset shift to fully utilize the capabilities of AI and stay ahead of emerging threats. Embracing AI as a critical component of our security strategy will be essential in addressing the increasing sophistication of cyberthreats. This shift will involve continuous learning and adaptation to keep up with the rapidly evolving technology landscape. By fully leveraging AI, we can enhance our defenses and better protect against future threats.

SCOTT HARRELL

CHIEF EXECUTIVE OFFICER

IoT devices will become a bigger target for attacks due to the ease of creating and deploying attacks against them. The proliferation of IoT devices in homes and businesses presents an opportunity for attackers to get persistent footholds from which they can pivot and launch attacks or wreak havoc and create disruption of operations. With AI, it will be more attractive to develop and execute attacks on these devices, leading to an increase in IoT-related security incidents.

DR. RENÉE BURTON

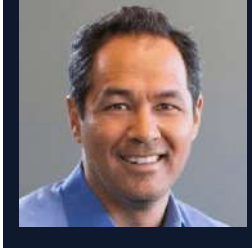
HEAD OF INFOBLOX THREAT INTEL

The adoption of cloud services for all aspects of businesses combined with the necessity to maintain accurate DNS records for these services will continue to expose enterprises to risks, including brand reputation and compromise of their own systems. These attacks are most often via dangling DNS records and are ones already experienced by most large enterprises.

CHRIS USSERMAN

GLOBAL PUBLIC SECTOR CHIEF TECHNOLOGY OFFICER

Threat actors will increasingly target third-party vendors and managed services, especially those with embedded access to customer environments. Compromising a single solution provider can provide immediate access to hundreds of downstream organizations. This “one-to-many” attack model, seen in recent supply chain breaches, will drive demand for implementing comprehensive Zero Trust principles, calls for tighter vendor vetting (i.e., product certifications) and extending continuous monitoring of partner activity.



CRICKET LIU

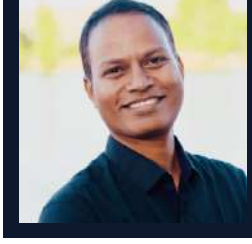
EXECUTIVE VICE PRESIDENT AND CHIEF EVANGELIST

Governments worldwide will increasingly mandate or strongly recommend the use of Protective DNS services as part of national cybersecurity strategies. This will be especially prevalent in sectors deemed critical infrastructure—such as healthcare, energy and finance—where threats can have outsized impacts.Protective DNS technologies will become more intelligent, incorporating behavioral analytics, machine learning and real-time traffic flow analysis. Instead of simply blocking known malicious domains, systems will detect anomalies in DNS queries—such as unusual query volumes, timing patterns or geographic inconsistencies—that may indicate command-and-control activity or data exfiltration.

DR. RENÉE BURTON

HEAD OF INFOBLOX THREAT INTEL

Though attackers will become faster and more sophisticated by using language models and deepfakes, DNS remains constant. It doesn’t care about these advancements. This makes DNS security more vital than ever to protect against these evolving threats. Ensuring robust DNS security will be crucial in safeguarding digital infrastructure. Balancing Security, Usability and Regulation



MUKESH GUPTA

CHIEF PRODUCT OFFICER

Balancing security and usability will remain a significant challenge. While robust security measures are essential, organizations should not compromise the user experience. Striking the right balance between security and usability is crucial to ensure that customers feel secure without being inconvenienced. This balance is particularly important in banking, where user trust and satisfaction are paramount.

ED HUNTER

SENIOR DIRECTOR, INFORMATION SECURITY

The tension between security and privacy will remain a central issue in 2026. Data governance—who owns data, how it’s used and under what conditions—will continue to evolve, with Europe leading the way through progressive legislation. Expect new laws and frameworks to emerge globally as governments grapple with the implications of AI-driven data processing.

NETAPP UNVEILS 2026 ENTERPRISE TECHNOLOGY PREDICTIONS CENTERING DATA INTELLIGENCE

AI moves from pilot to practice, cloud strategies mature, and cybersecurity becomes embedded as enterprises prepare for a data-driven future

As businesses step into 2026, the pace of technological change shows no sign of slowing. Organizations are seeking clear direction to navigate new challenges and seize opportunities driven by rapid advances in artificial intelligence (AI), cloud solutions, and cybersecurity. In response, NetApp has compiled insights from its global network to share practical predictions that reflect changes already underway—helping enterprises understand what moves will matter most in the year ahead.

AI Moves From Pilot to Practice

In 2026, AI is expected to graduate from experimental projects to become a mainstream business tool. Success won't hinge on having the largest data sets but on managing data intelligently—keeping it organized, accessible, and secure. NetApp leaders emphasize that an intelligent approach to data management will enable companies to unlock real-world value from AI across diverse business areas. From predictive analytics to automated workflows, the shift from pilots to production will define competitive advantage.

Cloud Strategies: Beyond Migration

Cloud adoption is entering a new phase. The conversation is moving beyond "lift and shift" toward workload placement based on performance, privacy, and data location. Enterprises need flexible systems that accommodate both local and regional requirements without adding administrative complexity. Automation and smart policy controls will play a critical role, allowing teams to focus on outcomes rather than routine maintenance. The goal: hybrid agility, where workloads run where they perform best—whether on-premises, in the cloud, or at the edge.

Cybersecurity: Embedded, Not Added

As threats evolve, cybersecurity is no longer an afterthought. Businesses are embedding smarter protective measures into operations from the start. The demand for early detection, rapid response, and robust recovery plans is surging. With decisions increasingly data-driven, ensuring accuracy, safety, and ethical use of information is paramount. NetApp predicts that proactive security—integrated into every layer of infrastructure—will become a baseline expectation, not a differentiator.

Simplifying Infrastructure for Agility

Organizations are also rethinking infrastructure to make it simpler and more responsive. Modern tools now enable businesses to adjust capacity dynamically, improve access, and minimize disruption as data needs grow. This flexibility ensures that scaling up doesn't mean slowing down. Intelligent infrastructure will underpin resilience, enabling enterprises to adapt quickly to market shifts and regulatory changes.

The Big Picture: Intelligence Everywhere

NetApp's overarching message is clear: preparing for 2026 means weaving intelligence and agility into every part of the organization. From AI-driven insights to automated cloud governance and embedded security, the future belongs to businesses that treat data not just as an asset but as a strategic advantage. Challenges will persist—but with the right approach, they can become opportunities.

Bottom Line:

2026 will reward enterprises that combine data intelligence, operational flexibility, and security-first thinking. Those that move beyond experimentation to execution—while keeping governance and resilience front and center—will set the pace in an increasingly digital economy. MEA

SUHAIL HASANIAN

SENIOR REGIONAL DIRECTOR & GM MEA, NETAPP

"Success in 2026 won't depend on the size of your **data, but on how intelligently you** manage it—organized, accessible, and secure."

DOMAIN-SPECIFIC AI: WHY CUSTOMIZATION IS THE FUTURE

Artificial intelligence is no longer just about adopting the latest model—it's about adopting the right one. As organizations move from experimentation to real-world implementation, generic AI is proving insufficient for complex, industry-specific challenges. Domain-specific AI, built on tailored data and infrastructure, is emerging as the key to unlocking true business value.

Artificial intelligence has developed rapidly in recent years. Generative AI (GenAI) is rapidly gaining ground and is now widely used, in applications and from automated customer service to advanced data analysis. However, in practice it turns out that a one-size-fits-all model is often not sufficient. Organizations encounter limitations when AI solutions are not tailored to their specific sector or field. Gartner therefore predicts that by 2027 more than 50% of AI models will be sector-specific. This customization will lead to more accurate and relevant results, because the models are trained on datasets that specifically match the issues and dynamics of a particular industry.

Why generic AI falls short

Many companies are currently experimenting with general AI models, but in practice they often encounter various challenges. For example, an AI model that is not specifically trained on medical data may struggle to correctly analyze X-ray images. In the financial sector, a general model cannot detect fraud, simply because it does not recognize all the complex patterns that are important in this industry.

In addition, training AI models on industry-specific data often requires a different approach. Collecting and processing qualitative and representative datasets is a skill in itself. Without well-structured data, an AI model remains limited in its capabilities, which can lead to inefficient use of resources and wrong decisions. As a result, more and more organizations are opting for domain-specific AI solutions that better meet their needs and add direct value to their business operations.

Sectors where custom AI is essential

The benefits of domain-specific AI are visible in almost every sector. Some examples:

- Healthcare: AI is playing an increasingly important role in medical image recognition, such as analyzing MRI scans and X-rays. Custom models can detect subtle abnormalities that are difficult for human doctors to recognize. This increases the accuracy of diagnoses and can save lives.
- Research and education: Universities and research centers use AI for complex data analyses. Depending on the field, models can, for example, analyze genetic datasets, simulate climate change or study linguistic patterns. Generic models often lack the necessary depth and precision to provide useful insights.
- Financial sector: Banks and insurers rely on AI for fraud detection and risk analysis. Algorithms that are specifically trained on transaction data can recognize suspicious patterns that might otherwise go unnoticed. This contributes to a safer financial ecosystem.
- Manufacturing: In the manufacturing industry, AI is used for quality control and predictive maintenance. Domain-specific models can detect anomalies in production lines or predict when machines need maintenance, increasing efficiency and minimizing downtime.

Challenges in implementing domain-specific AI

While the benefits of domain-specific AI are evident, implementing it also presents challenges. Organizations looking to deploy customized AI models must consider several key factors:

- Data quality and availability: The success of AI depends on the quality of the data on which the model is trained. Domain-specific AI requires reliable, well-structured, and representative datasets. This requires a thorough approach to data collection, cleaning, and labeling.
- Data security and sovereignty: Many organizations, especially in regulated sectors such as healthcare, finance, government, and energy, must ensure that sensitive data remains protected and compliant. Intellectual property, patient records, financial transactions, and proprietary research cannot simply be exposed to public cloud training environments or shared external datasets. Maintaining full control over where data resides and how it is processed is crucial to preserving confidentiality, compliance, and competitive advantage.
- Infrastructure requirements: AI workloads can grow quickly and unpredictably, especially as models evolve, are retrained, or require different types of processing. This makes it important for companies to have an infrastructure that can scale seamlessly, unify Computation and Storage, and support both development and production environments without introducing operational complexity. When the infrastructure is fragmented or built from disconnected systems, performance bottlenecks, higher costs, and delays in value delivery and usecases can arise.
- Expertise: Developing and training domain-specific models requires specialized knowledge. Data scientists and AI experts play a crucial role in this, but these professionals are in short supply. Investing in the right talent and partnerships is therefore essential.

The role of a strong infrastructure

A robust and flexible IT infrastructure platform is essential for the successful implementation of AI solutions, especially in complex domain-specific applications. An environment that brings compute, storage, and data processing closer together helps AI models to be trained and deployed more efficiently, while reducing unnecessary data movement and operational overhead.

A scalable and easily managed platform ensures that organizations can start small and expand as AI initiatives grow, without needing to constantly re-architect or replace underlying systems. This allows teams to experiment, refine, and operationalize models faster, supporting continuous improvement and adaptation to new datasets and business needs.

In addition, a strong infrastructure plays a crucial role in maintaining data security and sovereignty. For organizations working with confidential, regulated, or proprietary data, keeping information within controlled environments is essential. A cohesive platform that ensures

AHMED RASHAD
SR. AI SPECIALIST, MIDDLE EAST & AFRICA AT NUTANIX

"Domain-specific AI is no longer a niche solution, but **a necessary step for companies that want** to realize the full potential of artificial intelligence"

secure data processing, access governance, and compliance controls allows companies to leverage AI without exposing sensitive datasets to external or unmanaged environments. This enables innovation while preserving privacy, trust, and regulatory alignment.

With a future-proof infrastructure, companies can respond quickly to changing requirements while maintaining performance, reliability, and cost efficiency. This forms the foundation for domain-specific AI to deliver sustained value in day-to-day operations

Customized AI as a strategic advantage

Domain-specific AI is no longer a niche solution, but a necessary step for companies that want to realize the full potential of artificial intelligence. Organizations that focus on customization benefit from better performance, more efficient use of resources and faster innovation.

The key to success lies in a strategic AI approach, in which the right balance is found between data, infrastructure and expertise. By investing in a solid foundation, companies can use AI smartly and purposefully, gaining a competitive advantage in a world increasingly driven by automation and intelligent technologies.

Bio of Author

Ahmed Rashad serves as Senior AI Specialist for the Middle East and Africa at Nutanix, where he leads efforts to design and deploy advanced AI solutions tailored to regional business needs. With deep expertise in both generative AI and domain-specific modeling, Ahmed helps organizations across sectors—including healthcare, finance, manufacturing, and research—translate complex data into actionable insights. His work emphasizes the importance of robust, scalable infrastructure, data quality, and regulatory compliance, ensuring that AI initiatives are both efficient and secure. Through a strategic blend of technology leadership and regional insight, he enables companies to harness AI responsibly and effectively to drive innovation, growth, and competitive advantage. MEA

PORTWORX BY PURE STORAGE HELPS CIOS BRIDGE VMWARE TO KUBERNETES WITH CONFIDENCE

New Kube Datastore brings familiar VM workflows to Kubernetes, enabling enterprises to modernise without disruption while strengthening cyber resilience.

For many CIOs, the journey to modern, cloud-native infrastructure feels less like a migration and more like navigating a minefield. Virtual machines (VMs) still host the most critical workloads and data in the enterprise, yet rising VMware costs and uncertain roadmaps have forced organisations to rethink their strategy. At the same time, Kubernetes has become the platform of choice for modern applications and nearly all new AI deployments. Add growing cyber threats and talent shortages, and the stakes for getting this transition right have never been higher.

"This is where Portworx comes in," said Venkat Ramakrishnan, Vice President and General Manager, Portworx by Pure Storage. "By bringing familiar architecture and workflows to Kubernetes, we eliminate the steep learning curve that often slows modernisation. Enterprises can run everything from lightweight edge VMs to heavy VDI workloads on Kubernetes without disruption or cyber risk. This makes Kubernetes a viable platform not only for new, cloud-native applications but also for traditional VM workloads."

Introducing Kube Datastore for Cloud-Native Virtualisation

Building on its position as a leading Kubernetes data management platform, Portworx has launched Kube Datastore, a modern VM architecture optimised for cloud-native deployments and built for KubeVirt, the most widely adopted virtualisation effort in the Kubernetes ecosystem. With contributions from Red Hat, SUSE, Microsoft, and Oracle, KubeVirt and Kube Datastore together deliver:

- Intelligent storage abstraction: A unified, high-performance data layer across Kubernetes clusters to power VM workflows like provisioning, migration, vMotions, snapshots, and recovery at cloud scale.
- Operational continuity: Retain trusted VMware-like workflows such as Advanced Storage Migration and Enhanced Storage Rebalancing.
- Flexible deployment: Run VMs across edge environments, Citrix VDI workloads, or nested control planes without requiring VMware as a hypervisor.
- Smooth migration: Move from VMware to Kubernetes without compromising uptime or disaster recovery requirements. Customers using Pure Storage® FlashArray can leverage Rapid VM Migration to significantly cut migration time.

Cyber Resilience and Business Continuity

Cloud outages and ransomware attacks are more aggressive than ever, making business continuity and disaster recovery (BCDR) a board-level priority. Portworx delivers a consistent BCDR operating model for Kubernetes-hosted VMs, including:

- Granular recovery: PX-Backup now supports VM file-level backup and restore for tailored SLAs.
- Metro disaster recovery: Synchronous DR with FlashArray ActiveCluster™ achieves zero RPO for critical workloads.

These capabilities help enterprises reduce downtime, accelerate recovery, and strengthen cyber resilience while ensuring data remains safe and recoverable.

Reducing TCO and Accelerating Modernisation

Virtualisation costs are rising sharply, and delaying decisions only compounds risk. Portworx helps CIOs mitigate CapEx and OpEx by providing a cost-efficient entry point for migrating VMs to Kubernetes. By running VMs and containers side by side on Kubernetes and automating familiar VMware workflows, enterprises can reduce overprovisioning, improve agility, and lower operational costs.

"Advanced storage capabilities are critical to enable and accelerate a successful transition from traditional virtualisation platforms to a modern KubeVirt approach that allows companies to set themselves up for success across containers, virtual machines, and AI workloads," said Gary Chen, Research Director, Software Defined Compute, IDC.

VENKAT RAMAKRISHNAN
VP & GM, PORTWORX BY PURE STORAGE

"Modernisation doesn't have to mean disruption — Kubernetes **can now run your most critical** VM workloads with confidence."

Bottom line:

The VMware-to-Kubernetes transition doesn't have to be a leap of faith. With Portworx, CIOs gain a clear path to modernisation—controlling costs, securing data against outages and cyber threats, and empowering existing teams to move faster. MEA

EMERSON EXCHANGE 2026 IN DUBAI TO SHAPE THE FUTURE OF INDUSTRIAL AUTOMATION

Registration opens for Emerson's flagship users' conference featuring cutting-edge technologies, expert insights, and hands-on training

Emerson has officially opened registration for Emerson Exchange 2026, its premier global users' conference, scheduled for May 19–21 at the Dubai World Trade Center. For the first time, this flagship event will be held in the Middle East, bringing together more than 2,000 industry professionals from over 50 countries to explore the next era of industrial automation.

With the theme "Imagine the Next," Emerson Exchange 2026 will challenge delegates to look beyond today's digital transformation and envision breakthroughs that will define tomorrow's operations.

"Our customers are striving to make faster, smarter decisions, advance toward truly autonomous operations and unlock new levels of performance and value," said Liam Hurley, President, Middle East & Africa at Emerson. "Exchange will provide them with the inspiration and insight they need to realize these goals."

A Global Forum for Innovation and Collaboration

The three-day event promises a dynamic mix of expert-led sessions, interactive exhibits, and networking opportunities. Attendees will gain firsthand exposure to advanced automation technologies driving measurable improvements in safety, reliability, productivity, and sustainability.

The conference will feature over 300 presentations across multiple tracks, covering topics such as:

- Intelligent automation and autonomous operations
- Safety excellence and production optimization
- Asset performance and reliability
- Sustainability and energy transition strategies
- Modernization projects and digital transformation

Complementing these sessions, executive panels will address industry-shaping forces, including cybersecurity, artificial intelligence, and workforce development.

Immersive Technology Expo and Hands-On Training

A 5,000-square-meter interactive technology expo will showcase Emerson's latest innovations alongside solutions from strategic partners. Delegates can explore cutting-edge tools and applications designed to optimize operations and accelerate sustainability goals.

For those seeking practical skills, Emerson Exchange 2026 offers hands-on training courses with over 600 seats available, enabling participants to deepen technical expertise and enhance professional development.

Industry-Specific Forums

Specialized forums will cater to key sectors such as oil and gas, refining, chemicals, power, life sciences, and metals and mining, addressing critical priorities like energy transition, cybersecurity, and AI adoption. Real-world case studies will demonstrate how advanced technologies are solving operational challenges and delivering strong ROI.

LIAM HURLEY

PRESIDENT, MIDDLE EAST & AFRICA, EMERSON

"Imagine the Next: A global forum to shape the future of automation and sustainability."

Why Dubai? A Strategic Choice

"Companies across the Middle East are embracing next-generation automation to drive transformational improvements in efficiency, safety, and sustainability," Hurley noted. "Their ambition to position the region as a global hub for advanced manufacturing makes Dubai the perfect setting for Emerson Exchange 2026."

Registration and Details

For full agenda details and to secure your place at Emerson Exchange 2026, visit Emerson.com/Exchange2026. MEA

DON'T LET YOUR WEBSITE CRASH THIS HOLIDAY SEASON

In this high-stakes holiday season, retailers can't leave performance or security to chance. A comprehensive holiday readiness strategy is the only way to ensure your website stays fast, available, and resilient when it matters most.

CHRISTIAN REILLY
FIELD CTO, CLOUDFLARE

"The holiday season is make-or-break for retailers, and only **those who unify performance, availability, and security will stay** fast, resilient, and profitable when the surge hits."

The holiday season remains a make-or-break period for most retailers. Purchases in November and December often comprise about 19% of total annual sales. And a growing volume is happening online: Salesforce reported that online sales reached an all-time high of $1.2 trillion globally in 2024.

As mobile shopping continues to dominate — about 69% of global online purchases in 2024 were made via mobile devices — retailers need their sites to be fast, secure, and always available. Meanwhile, cybercriminals are becoming more sophisticated, leveraging AI to power phishing, credential stuffing, bots, DDoS, and ransomware attacks that target ecommerce platforms.

This is why retailers must have a comprehensive holiday readiness strategy that ensures performance, availability, and security.

Understand the Challenges Availability and Performance

Retailers must ensure their websites, mobile apps, APIs, and payment systems perform seamlessly under heavy load. Latency is costly — One recent study showed that pages that take more than four seconds to load experience a bounce rate of 63%. Traffic surges can be massive: Requests to ecommerce sites (from legitimate shoppers) reached 405 billion on Black Friday 2024, according to data analyzed by Cloudflare.

Resource Constraints

IT and security teams are expected to deliver personalized omnichannel experiences while managing higher volumes and tighter budgets. Many struggle with scale, complexity, and evolving threats.

New Cybersecurity Threats

Attackers are using AI to create realistic phishing, deepfakes to deceive employees, bots to scrape pricing data and commit fraud, and ransomware that adjusts its tactics autonomously.

Strengthen Security with a Unified Platform

Retailers benefit from a unified platform that integrates performance, infrastructure scaling, and advanced security instead of managing multiple tools.

Defending Against Bots

Malicious bots can scrape data, steal credentials, or execute fake transactions. An effective bot management solution distinguishes between good and bad bots and blocks harmful activity without affecting legitimate customers.

Handling DDoS Attacks

DDoS attacks can flood networks with terabits of traffic per second. A cloud-based defense with a global network backbone is essential to absorb such attacks while keeping services online.

Ransomware and Credential Attacks

Phishing remains a leading cause of breaches. Compromised credentials allow attackers to move laterally within systems. Multi-factor authentication, zero-trust architectures, and robust email security are key defences.

Data Protection

Compliance with PCI DSS and other regulations requires encryption, client-side attack prevention, and data-loss prevention (DLP). Network segmentation further limits the impact of breaches.

Deliver Omnichannel Experiences, Efficiently

Shoppers today move seamlessly between mobile, web, and in-store experiences. Retailers need consistent, responsive performance across all touchpoints.

Scalable Infrastructure

Ahead of the holiday surge, businesses should prepare to scale servers, apps, APIs, and services rapidly. Cloud platforms with auto-scaling capabilities help maintain performance during traffic spikes.

API-first and Developer Productivity

Modern retail relies on connected systems and APIs linking websites, apps, and in-store platforms. APIs enable innovation but are increasingly targeted by attackers. Securing them is essential. The right platform supports developers to create personalized experiences and scale safely.

Unified Vendor Ecosystem

Using too many independent tools creates integration challenges, security gaps, and higher costs. A unified platform simplifies management and improves visibility across security and performance.

Are You Ready for the Winter Surge?

Being prepared means more than scaling infrastructure. It means integrating performance, security, and experience into one cohesive stack — before the busiest shopping weeks begin. Key questions for retailers:

- Can your ecommerce site handle major traffic surges without slowing or crashing?
- Are your defenses ready for bots, DDoS, ransomware, and API attacks?
- Do customers enjoy a seamless experience

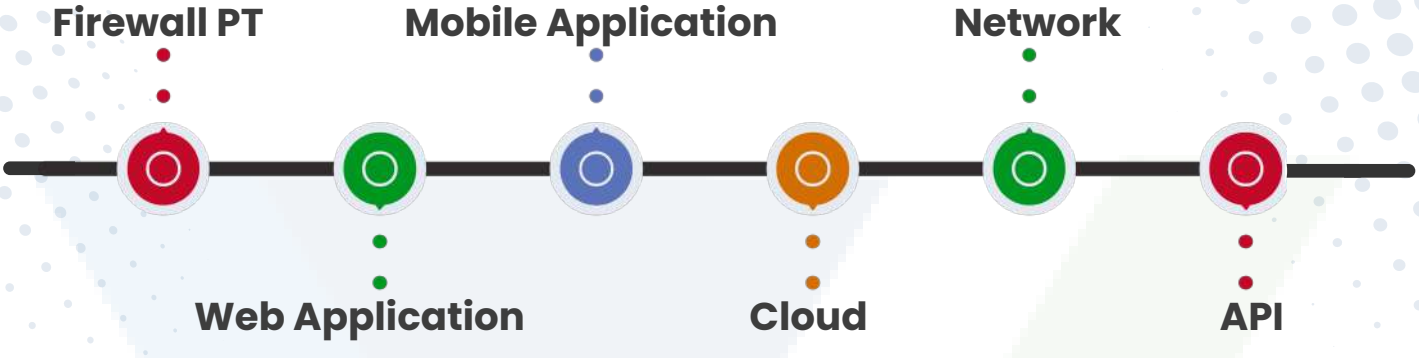
To access the complete article log on to:
www.enterpriseitworldmea.com

zeroday ops

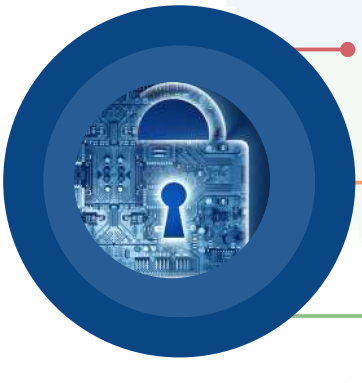
TATTVA
UNLOCKING CYBER CONFIDENCE

OUR SERVICES

VAPT



TRAININGS & SIMULATIONS



- Compliance and Data Privacy Training
- Phishing Simulations
- Multi Lingual Support for Content (Security Awareness Training Content)
- RED Teaming
- Cyber Challenge
- Role-Based Courses
- Infosec Trainings
- Ransomware Simulations

PCI DSS | ISO 27001 | ISO 27701 | GDPR | SOC 2 | HIPAA

info@5tattva.com
www.5tattva.com | www.zerodayops.com
+91-9810005685
+1-(347)298-0694
+506-6152-3953
+971 50 328 9600

LinkedIn
X
Facebook

"Empowering secure, compliant, and resilient digital ecosystems."

معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC GLOBAL

05 - 07 MAY 2026

DUBAI EXHIBITION CENTRE (DEC), EXPO CITY

HOSTED BY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY

وزارة الداخلية
MINISTRY OF INTERIOR

شرطة دبي
DUBAI POLICE

MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE

ENQUIRE FOR 2026!

#gisecglobal

gisec@dwtc.com

SPONSORS & PARTNERS

OFFICIAL DISTRIBUTION PARTNER

SPIRE

LEAD STRATEGIC PARTNER

HUAWEI

STRATEGIC PARTNER

Microsoft aws

DIAMOND SPONSOR

CHECK POINT e& OPSWAT.

PLATINUM SPONSOR

cisco DREAM

GOLD SPONSOR

1Password cpx CLOUDFLARE CROWDSTRIKE Google Cloud Security

GOLD SPONSOR

emt PENTERA kaspersky SECTIGO MENLO SECURITY Trellix