channelpost
MIDDLE EAST AND AFRICA
www.channelpostmea.com
SEPTEMBER 2026



BITDEFENDER SETS A PREVENTION- FIRST

CYBER VISION FOR THE MIDDLE EAST'S AI ERA AT GISEC 2026

Sumit Kumar, Channel & Distribution Manager for the Middle East at Bitdefender, emphasizes that we will present a prevention first cyber defense strategy at GISEC 2026,.. Page no.16

channelpost
MIDDLE EAST AND AFRICA

STAY AHEAD OF THE CURVE WITH **CHANNEL POST MEA**



EDITOR'S LETTER



SANJEEV
Editor

A REGION ACCELERATING INTO ITS TECHNOLOGY DECADE

The September 2026 issue arrives at a moment when the Middle East's technology landscape is accelerating faster than ever, reshaped by AI velocity, cybersecurity urgency, sovereign infrastructure, and a new generation of leaders redefining what digital ambition looks like. As Editor in Chief, I often say that an issue is successful when it doesn't simply report on change but captures the feeling of living through it. This month, that sentiment rings especially true. "The real story of this moment is not the speed of innovation, but the determination of a region refusing to be anything less than a global technology leader."

We open with our cover story on Bitdefender's prevention first strategy at GISEC 2026 — a narrative that reflects the region's most pressing reality. AI adoption, cloud expansion, and distributed applications are accelerating at a pace that demands unified visibility and resilient architectures. Bitdefender's perspective underscores a shift already underway: cybersecurity is no longer a defensive discipline but a strategic foundation for national digital transformation. Shadow AI, identity sprawl, and cloud complexity are now central to every boardroom conversation, and this story sets the tone for the entire issue.

Our feature stories widen the frame to show a region stepping confidently into cyber leadership. GISEC Global 2026 emerges not as an exhibition but as a declaration of intent, where sovereign AI, microsegmentation, observability, identity governance, and adversary centric intelligence define the new center of gravity. Alongside this, the Women of Substance Conference & Awards 2026 brings a powerful human dimension, celebrating founders, CIOs, educators, and students whose clarity, resilience, and purpose remind us that innovation is as human as it is technical.

> "The real story of this moment is not the speed of innovation, but the determination of a region refusing to be anything less than a global technology leader."

The interviews in this issue reveal the architecture behind the momentum. MongoDB explores Saudi Arabia's AI ready data foundation. Power & Cooling ME explains the rise of high density, AI driven infrastructure. SUSE shows enterprises how to unlock hidden compute capacity amid global hardware shortages. Graystone Capital maps the real economics of GCC tech, exposing the financing structures that sustain growth. Together, these conversations illuminate the machinery powering the region's digital evolution.

Our expert views sharpen the narrative further, from CMMC readiness gaps and adversarial input targeting LLM powered scanners to the sobering reality that resilience — not automation — defines AI maturity.

Finally, our news section captures a region in motion, from Saudi made servers and frontier AI security integrations to major funding rounds and new product launches. Each development reinforces a simple truth: the Middle East is not following global technology trends; it is setting them.

CONTENT



COVER STORY

BITDEFENDER SETS A PREVENTION FIRST CYBER VISION FOR THE MIDDLE EAST'S AI ERA AT GISEC 2026



FEATURE STORY

WOMEN IN TECH TAKE CENTER STAGE AT THE WOMEN OF SUBSTANCE CONFERENCE & AWARDS 2026

INTERVIEW

24



HESHAM MOHAMED J

GRAYSTONE CAPITAL MAPS THE REAL ECONOMICS OF GCC TECH: FINANCING THE CHANNEL, NOT THE HYPE

INTERVIEW

28



ABDULRAZZAK AL ZUBAIDI

MONGODB.LOCAL ARRIVES IN RIYADH ON 17 NOVEMBER TO UNITE THE KINGDOM'S AI AND DATA COMMUNITY

INTERVIEW

32



DR THOMAS DI GIACOMO

SUSE URGES ENTERPRISES TO UNLOCK HIDDEN CAPACITY

INTERVIEW

38



MEENAL SANJEEV MADAVI

POWER & COOLING ME BUILDING THE MIDDLE EAST'S RESILIENT DIGITAL INFRASTRUCTURE



EXPERT VIEW

CHANNEL PARTNERS CAN CAPITALISE ON DEFENCE FIRMS' GROWING CMMC READINESS GAPS



EXPERT VIEW

GUARDBREAKER DERAILING AI ASSISTED MALWARE ANALYSIS WITH A CODE COMMENT



FEATURE STORY

GISEC GLOBAL 2026: THE YEAR MIDDLE EAST CYBERSECURITY RE-DEFINED ITS CENTER OF GRAVITY

Publisher & Editor: Sanjeev K | **Designer:** Rakesh Kumar | **Web Designer:** Tony Adams | **Lead Visualizer:** Nafisa
ZARKS MEDIA FZE Fujairah Creative City Media Free Zone Fujairah -Twin Towers P.O.Box 4422 Fujairah,UAE
Email: info@zarksmedia.com

Check Point Brings OpenAI Daybreak Models Across Its Security Platform



Check Point announced that it has significantly expanded its collaboration with OpenAI through the Daybreak cyber defense initiative, deepening the integration of frontier AI models across its security platform. The company confirmed that OpenAI's advanced cyber reasoning capabilities are now being incorporated into multiple Check Point products and workflows via the Daybreak Defense Network, marking a major step in operationalizing frontier AI for enterprise cyber defense. This development follows Check Point's recent decision to join more than one hundred global technology and security companies in supporting OpenAI's call for a coordinated surge in worldwide cyber defense.

According to Check Point, the partnership is designed to help organizations stay ahead of increasingly sophisticated attacks by embedding frontier AI directly into the security lifecycle. By combining OpenAI's cyber reasoning with Check Point's intelligence, context and enforcement, the company aims to help customers move from large volumes of raw security data to validated risk, actionable decisions and accelerated protection.

The integration spans several core areas. In exposure management, Check Point is piloting OpenAI's frontier models within its Agentic Exposure Validation pipeline to distinguish real, exploitable risk from theoretical findings and speed remediation. In network security, the company is enhancing Keystone—its autonomous, intent driven security management system—by using frontier AI to analyze potential attack paths, understand vulnerabilities and determine how controls should adapt. The Autonomous Workspace Platform is also being upgraded with advanced cyber reasoning to investigate complex threats across email, endpoint, mobile and browser telemetry, reducing analyst workload and improving verdict clarity. Meanwhile, NexPloit is leveraging frontier AI to accelerate vulnerability research and generate verified attack material that drives faster protection against newly disclosed flaws.

Jonathan Zanger, Chief Technology Officer at Check Point, underscored the significance of the collaboration, stating: "Frontier AI gives defenders a new advantage — the ability to understand risk, validate threats and act at a speed that matches modern attackers."

Check Point emphasized that these capabilities are being rolled out in phases, with strict governance over model visibility, actions and verification. The company's goal is to translate frontier AI advances into trusted, enterprise grade security outcomes while helping customers adopt and use OpenAI technologies securely.

Acer Relaunches Packard Bell with New Lifestyle Collection

At IFA 2026, Packard Bell, under the Acer Group, marks its 100th anniversary with a full relaunch that reintroduces the brand to a new generation. The comeback includes a refreshed visual identity, a consumer first philosophy expressed through "Tech it easy," and a new product collection led by the 14.5 inch DotBook laptop, arriving in European retail from Q4 2026. Founded in Los Angeles in 1926, Packard Bell built its legacy on making breakthrough technologies accessible to everyday households. It brought consumer radios into homes, helped democratise colour television, and later became one of the brands that introduced personal computing to mainstream families. Across each era, Packard Bell's reputation rested on a simple promise: useful technology should be available to the many, not the few.

A century later, that mission feels newly relevant. As consumer electronics grow more complex, Packard Bell returns with a simpler question—what do people actually need? The answer is captured in its new philosophy, "Tech it easy," a commitment to designing technology for everyday life at an affordable price.

The brand's new identity is built around a single shape: the dot. The emblem, a constellation of dots that subtly forms the letters "P" and "B," reinterprets a century of heritage through a modern, human



centric lens. The dots are imagined as cells rather than pixels, signalling technology designed for real life. This approach extends to a warm, plain spoken tone of voice and lifestyle driven imagery that shows products in everyday use. Four vibrant colours—orange, purple, green and yellow—create a cohesive visual system across campaigns and products.

The first wave of products is anchored by the DotBook, a 14.5 inch laptop built for browsing, streaming and daily work, echoing the netbooks that once made Packard Bell a household name. The brand is also opening its universe to partners, beginning with Steasy, a startup debuting a connected mini steamer that embodies the same everyday first philosophy. The first co created product arrives in Europe in Q4 2026, with more planned through 2027.

Packard Bell's relaunch is supported by Acer's global infrastructure, including multilingual customer support across 28 countries, a regional service centre network, and long standing retail and logistics partnerships—ensuring the brand's new chapter begins with scale and stability.

ZEDEDA and VAS Limited Launch Edge Intelligence Partnership in Saudi Arabia

ZEDEDA has partnered with VAS Limited to distribute it's Edge Intelligence Platform to customers across the Kingdom of Saudi Arabia, with plans to expand into the wider GCC region.

Deployments across hundreds or thousands of sites are rarely a single product decision. They require hardware sourcing, multi vendor integration, on site commissioning and long term operational support delivered inside the Kingdom. VAS Limited provides that integration and services layer, while ZEDEDA delivers the platform that deploys, secures and operates applications across the enterprise from one place. The agreement also establishes a joint go to market motion, pairing ZEDEDA's technology with the local reach and support practice VAS Limited brings as a value added distributor.

"This agreement reinforces ZEDEDA's commitment to the Kingdom of Saudi Arabia and establishes the foundation for a strategic partnership with VAS Limited in the region," said Usamah Alridwan, Regional Sales Director and Country Manager, Saudi Arabia, ZEDEDA. "VAS brings the local reach, technical expertise and customer relationships that edge AI deployments require, and gives us a partner capable of helping organizations deploy edge intelligence at national scale."

VAS Limited was established in Saudi Arabia in 2024 as the regional office of VAS Integrated Solutions. The company's focus on developing Saudi technical talent aligns the partnership with the capability goals set out in Vision 2030.

"Organizations across Saudi Arabia are moving AI closer to where their businesses operate, but doing so at scale requires more than deploying an AI application," said Bilal Abdulrahman, Country Manager, VAS Limited. "With ZEDEDA, we can give customers a centralized way to deploy and govern edge applications across distributed locations while delivering the technology and support locally."

The partnership's first joint solution targets edge AI video analytics for branch and remote sites. GPU accelerated edge appliances ingest camera streams and run AI inference where data is generated, ensuring detection and alerting continue independently of wide area network conditions. Network and security functions, including firewalling and multi path connectivity, can run as virtualized workloads on the same appliance.

"AI creates value in the physical world only when it can operate reliably across thousands of real sites and under real operating conditions," said Ernesto Beneke, Vice President EMEAI, ZEDEDA.

NTT DATA to Launch AI Experience Lab in Riyadh to Accelerate Regional AI Adoption

NTT DATA announced its intention to launch the NTT DATA AI Factory Lab in Riyadh, Saudi Arabia. Designed to help organizations accelerate AI adoption, the lab will bring together NTT DATA's full stack AI solutions and services expertise with technologies from leading ecosystem partners, including Cisco and NVIDIA, to help scale AI with confidence.

Scheduled to open in September 2026, the AI Factory Lab will support executive briefings, AI strategy workshops and hands on experiences that help organizations identify high impact use cases, validate business outcomes and accelerate adoption on a secure, integrated foundation spanning infrastructure, platforms and services.

"While interest in AI continues to grow, many organizations are looking for a practical path from experimentation to business outcomes," said Hani Nofal, Executive Head of Infrastructure Solutions in Middle East and Africa, NTT DATA. "The AI Factory Lab brings together the expertise, technologies and ecosystem partnerships needed to help clients identify the right use cases, deploy AI securely and scale with confidence." Located in Saudi Arabia's leading business and innovation hub, the lab supports the Kingdom's Vision 2030 ambitions by helping public and private sector organizations adopt advanced technologies that drive productivity, innovation and economic growth.

The AI Factory Lab will feature interactive demonstrations of real world AI applications across employee productivity, customer experience, intelligent operations, cybersecurity, networking, software development and industry specific processes. Organizations will be able to explore how agentic AI can automate workflows, improve decision making and unlock greater value from enterprise data. Featured experiences will include the Cisco Secure AI Factory with NVIDIA, showcasing how organizations can build, deploy, secure and govern AI workloads on an enterprise grade foundation. Cisco will provide the critical AI infrastructure layer, including networking, security, observability and collaboration capabilities. NVIDIA will supply the accelerated computing platform and AI software powering generative AI, agentic AI, computer vision and digital twin workloads.



"In the race to adopt AI, organizations need more than just technology—they need a foundation of absolute trust and control," said Cassie Roach, VP of Partner Sales, AI Infrastructure & Connectivity at Cisco.

"Organizations across the Middle East and Africa are moving from AI exploration to production," added Dirk Barfuss, Director of EMEA Channel at NVIDIA.



CITRIX INTRODUCES UNICONOS DUAL BOOT TO DELIVER INSTANT ENDPOINT RECOVERY

Citrix announced Citrix UniconOS dual boot, a new endpoint resiliency capability designed to help organizations recover access to work in minutes — without spare hardware, central reimaging or prolonged business downtime. Available now as part of Citrix UniconOS Release 7 2607, dual boot turns every compatible Windows endpoint into its own recovery device: an isolated, hardened Citrix UniconOS environment that runs alongside Windows on the device and can reconnect users to their applications via Citrix DaaS and Citrix SecurAccess with Chrome Enterprise in minutes.

Ransomware, failed updates, operating system corruption and misconfigurations can turn Windows endpoint failures into enterprise-wide business disruptions. In healthcare, financial services and critical infrastructure, outages can interrupt core workflows, put revenue and service-level agreements at risk, increase operational or patient-safety risks, and complicate compliance with regulations and standards such as the European Union's Digital Operational Resilience Act (DORA), Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS).

Many recovery approaches rely on reimaging workflows, central recovery services or standby devices. These methods can be manual, centralized, hardware-dependent and difficult to test at scale before a disruption occurs. When large fleets go offline, recovery can become an intensive, multisite IT effort while users wait for devices to be reimaged, replaced or delivered.

Citrix UniconOS dual boot changes that model by putting recovery directly on the endpoint. Its unique dual boot architecture places a second, hardened Citrix UniconOS environment alongside Windows on the same physical disk in a separate partition isolated through secure boot and independent of the Windows file system. If Windows is compromised, corrupted or unavailable, the user selects Citrix UniconOS from the boot menu, signs in and reconnects to the applications they need through Citrix DaaS and Citrix SecurAccess with Chrome Enterprise, while security teams continue investigating the affected Windows environment.

"For organizations in healthcare, financial services, retail, public sector and other industries where downtime has material business impact, endpoint resilience has become a boardroom issue," said Philipp Benkler, vice president and general manager of Unicon at Citrix. "Citrix UniconOS dual boot is designed to help customers keep work moving when Windows is unavailable, giving users a faster path back to the applications they need through the Citrix platform. By turning existing Windows endpoints into recovery-ready devices, Citrix helps organizations strengthen continuity, reduce operational disruption and maintain productivity when it matters most."

Unlike many competitive solutions, Citrix UniconOS dual boot is designed to do more than bring an endpoint back online. By pairing an isolated recovery OS with Citrix DaaS for application and desktop delivery, Citrix SecurAccess with Chrome Enterprise for zero-trust access, and Citrix UniconOS Management for fleet-wide control, Citrix's holistic platform approach helps organizations restore access to work — not just recover the device.

Citrix is the only vendor that combines an immutable endpoint recovery operating system on the endpoint with integrated DaaS application delivery, a secure zero trust network access enterprise browser and cloud-based fleet management in one integrated solution.

Citrix UniconOS dual boot simplifies and accelerates recovery across endpoint fleets

Citrix UniconOS dual boot helps organizations maintain access to critical applications when Windows is unavailable because of ransomware, failed patches or updates, misconfigurations or other disruptions. Each Windows PC can become its own business continuity and disaster recovery device. With recovery initiated through a single reboot by each user, the process can scale with the size of the fleet.

IT teams can deploy Citrix UniconOS, formerly eLux, alongside Windows on existing devices, allowing organizations to use their existing Windows fleet as the recovery fleet without adding a second pool of laptops or separate hardware, allowing organizations to reduce their dependence on spare hardware, disaster recovery cabinets and central imaging services.

Key capabilities include:

- Secure boot from end-to-end: The recovery operating systems is signed from shim to kernel, providing provenance that security teams can present to auditors and regulators.
- Automatic enrollment in Citrix UniconOS Management: Endpoints automatically enroll in Citrix UniconOS Management, formerly Scout, where administrators can centrally define the default operating system, boot delay and fallback policy and monitor fleet health.
- Fleetwide control from one management plane: Citrix UniconOS Management provides centralized control over boot behavior and recovery policies and monitors Citrix UniconOS health across the fleet, allowing IT teams to shift from manual device triage to policy-based management and monitoring.

For organizations that need additional desktop or application capacity during a disruption, Citrix Platform Flex can further support continuity by helping IT teams scale resources as demand changes. Together, these capabilities help organizations turn endpoint recovery into business continuity, so work can keep moving when every minute matters.



HUSKEYS RAISES $27 MILLION SERIES A LED BY BLACKSTONE

Huskeys has raised $27 million in Series A funding, led by global investment firm Blackstone, marking one of the most significant early stage cybersecurity investments of 2026. The funding comes at a moment when enterprises worldwide are grappling with a new wave of AI driven threats emerging at the network edge — a domain where Huskeys has rapidly positioned itself as a category defining innovator.

Founded to secure the increasingly complex and distributed digital environments shaped by AI workloads, Huskeys has built a platform designed to protect edge nodes, micro services, and autonomous systems that now operate outside traditional data center perimeters. As organisations deploy AI models closer to users and devices to reduce latency and improve performance, the attack surface has expanded dramatically. Huskeys' technology aims to close this gap with real time threat detection, autonomous response capabilities, and a unified security fabric that extends across cloud, edge, and on device compute.

Blackstone's participation underscores the rising urgency around securing AI infrastructure. The firm noted that enterprises are accelerating AI adoption faster than they are modernising their security architectures, creating a mismatch that adversaries are exploiting. Huskeys' approach — combining behavioural analytics, distributed telemetry, and AI native threat modelling — is seen as a critical enabler for organisations moving toward edge centric architectures.

The new funding will be used to scale Huskeys' engineering teams, expand global go to market operations, and deepen R&D around securing next generation AI systems, including agentic AI, autonomous decision engines, and real time inference pipelines. The company also plans to strengthen partnerships with cloud hyperscalers, telecom operators, and device manufacturers to embed its security capabilities directly into edge infrastructure.

Industry analysts say the Series A round signals a broader shift in cybersecurity investment priorities. As AI becomes embedded in every layer of enterprise operations — from customer experience to industrial automation — securing the edge is no longer optional. Huskeys' momentum reflects a growing recognition that legacy perimeter based security models cannot protect the distributed, AI powered networks of the future.

With Blackstone's backing, Huskeys is now positioned to accelerate its mission of redefining edge security for the AI era, offering enterprises a resilient foundation as they navigate the next wave of intelligent, autonomous digital transformation.

SAUDI EDTECH STARTUP AILA SECURES $3 MILLION IN PRE-SERIES A FUNDING ROUND

AILA, a Saudi education technology startup focused on AI-powered personalized learning, has raised US$3 million in a Pre-Series A funding round led by Rua Growth Fund, with participation from Jo Academy, 500 Global, Bunat VC, and Fikr Ventures. Jo Academy, a leading EdTech pioneer in Jordan, also joined the round as a strategic investor, bringing valuable experience in education and digital learning.

AILA develops technology that helps students learn based on their individual needs.

Its platform identifies learning gaps, personalizes learning and practice, and provides students with support based on their progress. It also gives teachers and school leaders clearer insights into student performance, helping them identify where support is needed.

The company's products include AILA Tests, an AI-native learning platform for personalized exam preparation for schools, and AILA Labs, AILA's dedicated R&D hub focused on researching, developing, and testing new AI-powered solutions for education.

The new funding will support AILA's product development, expansion and new markets.

"This investment lets us bring personalized, AI-native learning to more students at a moment when education systems across the region are rethinking what's possible with technology," said Yousef Alsayed, CEO of AILA.



"Arabic-speaking students deserve learning experiences built for them, not just translated for them. AILA is leading the way in the region, building AI-native education from the ground up, and their traction with Saudi schools speaks volumes of its strong product-market fit. We invested in AILA because we believe the future of EdTech in this region will be built here, by local innovators like AILA," said Alaa Jarrar, CEO, Jo Academy.

AILA is building an AI-native assessment platform that helps schools and teachers understand each student's proficiency, identify learning gaps, and focus support where it is needed most. We were drawn to the team's ability to turn assessment data into actionable insights for educators and targeted practice for students. Rua is proud to lead this round and support Yousef, Abdulaziz, and the AILA team as they scale Saudi-built AI education solutions for schools and education systems across the region and beyond." said Turki Aljoaib, Co-Founder & Managing Partner, Rua Growth Fund.

The investment marks the next stage of AILA's growth. Alongside financial support, the investor group brings experience, networks, and market knowledge that can help the company enter new markets and build partnerships across the education sector.

AVEVA Appoints Brock Ballard as the New CRO

AVEVA today announced the appointment of Brock Ballard as Chief Revenue Officer effective 1 October 2026. Brock joins the team from Bentley Systems following an extensive recruitment process led by AVEVA; he will succeed Sue Quense in the role as she steps into an advisory capacity.

Brock brings over 20 years of senior leadership in software sales, having joined Bentley Systems in 2020 as Vice President and Regional Executive. He was named Chief Revenue Officer in 2023, in charge of all Bentley's accounts, globally. Previously, Brock held leadership roles at DELMIA Sales, Dassault Systemes and Autodesk Inc. He holds a Bachelor of Arts degree in communication and information sciences from the University of Alabama.

"I am delighted to welcome Brock to the Executive Leadership team at AVEVA, where we will benefit from his expertise, experience and commitment to building successful, high-growth tech companies. Brock's engaging approach sets him apart in our sector, and I look forward to working with him to drive the next phase of AVEVA's growth.

I also want to extend my personal thanks to Sue Quense for her outstanding leadership and good counsel over the past five years. She will continue to work with AVEVA leadership in an advisory capacity, even as she steps back from the day-to-day running of the business," said Caspar Herzberg, CEO, AVEVA.



"Having long admired AVEVA's vision to drive innovation in the industries that deliver the essentials of life, I am delighted to be joining the executive leadership team. AVEVA's outstanding software portfolio, technical leadership and ambitious growth trajectory lead the market. This, coupled with the team's shared commitment to driving responsible use of resources, has never been more important to enabling the transformation of businesses across the world. I cannot wait to get started," said Brock Ballard.

Dr. Rabeah Alzaidy to Lead Lenovo's R&D Initiatives in Saudi Arabia



Lenovo announced the appointment of Dr. Rabeah Alzaidy to lead the company's Research & Development (R&D) initiatives in Saudi Arabia. Dr. Alzaidy brings more than 15 years of experience in artificial intelligence, research, and technology innovation. She holds a PhD in Computer Science and Engineering from Pennsylvania State University and completed postdoctoral research at both Penn State and King Abdullah University of Science and Technology (KAUST), as well as Executive Leadership training at the University of California, Berkeley.

She also served as Assistant Professor of Computer Science at King Fahd University of Petroleum and Minerals (KFUPM), managed strategic projects for Aramco, led strategic AI initiatives as a Research Consultant for the National Center for Artificial Intelligence (NCAI) in SDAIA, and most recently held leadership roles at Lucid Motors and HUMAIN, where she drove AI strategy and research and development initiatives across emerging technology domains.

Dr. Alzaidy will lead Lenovo's R&D initiatives in Saudi Arabia, helping expand the company's local innovation capabilities and strengthen collaboration with universities, researchers, industry partners, and Lenovo's global technology teams. Her appointment supports Lenovo's ambition to contribute to the Kingdom's growing research ecosystem while accelerating the development of technologies designed in Saudi Arabia for regional and global markets.

Commenting on her appointment, Dr. Rabeah Alzaidy said: "Saudi Arabia is creating one of the world's most dynamic environments for technology innovation, and I am excited to join Lenovo at a time when research and development have an increasingly important role to play in the Kingdom's transformation. I look forward to helping strengthen the connection between research, industry, and talent development, while contributing to the growth of Lenovo's innovation capabilities in Saudi Arabia.

Everpure Appoints Craig Robertson to Lead Partner Ecosystem

Everpure has announced the appointment of Craig Robertson as Head of Partners in EMEA & LatAm. Robertson succeeds Geoff Greenlaw, who is retiring.

Based in the UK, Robertson steps into the role having enjoyed a successful 10 year career at Everpure. He will lead Everpure's partner strategy and execution in EMEA and Latin America, working closely with partners to drive mutual growth, expand market opportunities, and help customers unlock greater value from their data. As a 100% partner focused organisation, this appointment is pivotal to continue driving opportunities with partners.

Robertson has held a number of leadership positions across Everpure and brings strategic partner relationships, deep knowledge of channel strategy and go-to-market expertise to the region. Having previously worked at partner organisations in the UK, he has extensive knowledge of what drives partner success.

"Craig Robertson has consistently demonstrated his deep understanding of our partner ecosystem," said Ricardo Moreno, VP Global Partners, Everpure. "His appointment reflects the strength of our internal talent and our unwavering commitment to driving partner growth across EMEA and Latin America. Robertson is an ideal leader to help partners capitalise on the significant opportunities provided by AI and data management."



"I'm incredibly proud to step into this role at a pivotal moment for Everpure," said Craig Robertson, Head of Partners in EMEA & LatAm. "Having built my career here, I know that our partners are intrinsic to everything we do. As we enter a new era where data primacy defines market leaders, our partner community is vital to helping customers modernise their data strategies and unlock real business growth. I'm excited to deepen these relationships across EMEA and LatAm as we shape the future together."

Forcepoint Names Vincent Merlin as the New CMO

Forcepoint announced that Vincent Merlin has joined the company as Chief Marketing Officer. Reporting to CEO Ryan Windham, Merlin will lead global marketing across brand, demand generation, product marketing and analyst relations as Forcepoint defines the AI data security category, enabling enterprises to keep command of AI while putting their best intelligence to work.

"Trust used to be a posture, and it is becoming a deliverable for the agentic enterprise: every AI interaction with data governed, every decision recorded, every time," said Windham. "The next decade won't be won by organizations using the most AI. It will be won by those that never lost control of it. Vincent's global go-to-market expertise will help our customers and partners see what command of AI makes possible."

Merlin joins Forcepoint from Proofpoint, where he spent 10 years in senior marketing leadership roles, most recently as Senior Vice President of Global Growth Marketing. His responsibilities spanned the worldwide marketing organization and inside sales, helping build the global growth engine and drive AI-led transformation as the company scaled from approximately $400 million to more than $2.4 billion in annual recurring revenue. He previously held global and regional marketing leadership roles at AVEVA, as well as Dell EMC and RSA. Merlin holds an MBA from the Tuck School of Business at Dartmouth and an engineering degree in quantum photonics and optics from Institut d'Optique Graduate School.



"Every technology worth adopting showed up before anyone knew how to secure it. The web, email, the cloud," said Merlin. "Companies moved anyway, and the ones that moved early could because somebody made it survivable. Forcepoint is doing that for AI, giving enterprises the confidence to put their best information to work while staying in control. That's why I'm here."

WSO2 Onboards Harry Ault to Drive the Next Phase of Growth

WSO2 today announced the appointment of Harry Ault as Chief Executive Officer. He will assume day-to-day leadership of WSO2 immediately, working closely with the executive team to advance the company's strategy and drive continued momentum across its global customer base.

Ault joins WSO2 with more than 20 years of experience in revenue leadership, strategic partnerships, corporate development, and go-to-market strategy across global markets. Prior to taking up this role, he was Chief Revenue Officer at SambaNova Systems, a pioneer in AI inference chip technology, where he led the company's global sales, marketing, field engineering, and global support organizations. Throughout his career, Ault has built a track record of driving above-market growth, leading successful M&A integrations, and scaling go-to-market strategies across diverse industries.

"We are thrilled to welcome Harry to WSO2 at such a pivotal moment for the company," said Jonas Persson, Chairman of the Board. "Harry's proven ability to build winning teams and scale go-to-market strategy globally makes him the right leader to take WSO2 into its next chapter."

"Over the past two decades, WSO2 has built a remarkable platform and a loyal customer base of more than 700 enterprise organizations, and I'm honored to join at such an exciting inflection point," said Harry Ault, incoming CEO of WSO2. "As organizations transform into AI-driven, agentic enterprises, they need a trusted open-source partner to navigate the change with speed, control and confidence without adding complexity. I'm looking forward to deepening our engagement in the open-source community, growing our global partner ecosystem, and expanding WSO2's value to customers and developers everywhere."



Ault succeeds Founder and former CEO Dr. Sanjiva Weerawarana, who stepped down from the role in May 2026. Devaka Randeniya, WSO2's Chief Revenue Officer, has served as Acting CEO during the transition period and will continue to partner closely with Ault as he steps into the role.

Saviynt Appoints Kamel Heus as Vice President of Sales for MEA



Saviynt today announced the appointment of Kamel Heus as Vice President of Sales for the Middle East and Africa (MEA). Based in Dubai, Heus will lead Saviynt's business across MEA, including Turkey, as the company accelerates growth and strengthens its presence in key markets.

In his new role, Heus will drive new business, renewals, and customer expansion while leading Saviynt's regional channel strategy and expanding its partner ecosystem. As AI reshapes how organizations across government, financial services, utilities, healthcare, oil and gas, and retail approach identity, his appointment reflects the rising importance of securing both human and agentic identities. His priorities include expanding Saviynt's footprint, accelerating growth in Saudi Arabia, and enhancing local hosting capabilities to meet in region delivery and data residency requirements.

"MEA represents a significant opportunity for Saviynt as organizations across the region accelerate digital transformation and increasingly look to AI to transform how they operate and grow," said Pete Angstadt, Chief Commercial Officer at Saviynt. "Our role is to help customers move faster while ensuring security and governance keep pace. Kamel's deep experience in the region and understanding of its customers and partner ecosystem will be invaluable as we expand our presence."

Heus will also help MEA organizations address a new category of identity risk: AI agents. As these agents gain access to enterprise applications and data, they require the same discovery, governance, and lifecycle controls traditionally applied to human identities. Saviynt's Zuma platform provides visibility into AI identities and enforces least privilege access across their lifecycle.

"The Middle East and Africa have become one of the fastest growing cybersecurity markets in the world, and Identity sits at the center of it — especially as AI agents enter the enterprise," said Kamel Heus. "My focus is to build out our local presence, grow a strong partner ecosystem, and enable organizations across MEA to grow their business through secure, confident access for both their people and their AI."

Heus brings two decades of cybersecurity sales leadership across MEA and Europe, including senior roles at Thales, Centrify (now Delinea), and Sophos. His appointment strengthens Saviynt's regional commitment as cloud, AI, and digital transformation reshape enterprise environments.

CPX to spotlight AI resilience and ecosystem growth at GISEC Global 2026



CPX Holding announced that it will return to GISEC Global 2026 for the fourth consecutive year. This year the event will take place from September 16-18, 2026, at the Dubai Exhibition Center in Expo City, GISEC Global will see CPX highlight its growing role in regional digital defense through executive engagement, ecosystem collaboration, and national security dialogue aimed at strengthening cyber resilience for nations and organizations.

With AI-powered cyberattacks on the rise, a shifting geopolitical landscape, and an expanding digital footprint, the need for proactive defense across critical sectors has never been more urgent. To address these challenges, CPX's participation at GISEC Global 2026 centers on the theme Building AI Resilience: Secure What's Next, delivering the advanced threat intelligence, governance frameworks, and end-to-end protection required to ensure national cyber readiness and digital sovereignty.

"GISEC Global continues to be an essential platform for shaping the regional and global cybersecurity landscape," said Hadi Anwar, CEO of CPX. "Coming back to GISEC for a fourth year is our chance to stand shoulder-to-shoulder with our partners and show the region what's possible when we build AI resilience together. Through deep expertise and powerful ecosystem collaboration, CPX is empowering governments and enterprises to preempt emerging threats, defend essential assets, and navigate digital transformation with complete confidence."

Exhibiting at Stand A80 (located between Halls 1 and 3, adjacent to the UAE Cyber Security Council), CPX's booth will feature six interactive domain showcases covering its core capabilities: Advise, Protect, Operate, Secure AI, OT Security, and Physical Security. The booth will also serve as a collaborative hub for 19 core partner pods, enabling global industry leaders to demonstrate co-innovations alongside CPX. Featured partner organizations include Microsoft, Cisco, Dell Technologies, Fortinet, Check Point, Mastercard, Core42, Rilian, Splunk, Corelight, Gigamon, Cribl, Anomali, Commvault, SimSpace and VEEAM.

Throughout the three-day event, CPX executives and domain experts will deliver Main Stage keynotes and participate in high-level panel discussions addressing AI security, critical infrastructure defense, and national resilience.

CPX invites visitors, partners, and national stakeholders to experience these capabilities firsthand at Stand A80 — and to be part of the conversation on securing what's next.

Criminal IP Appoints Reconn as Distributor for Threat Intelligence & Attack Surface Management

Criminal IP has appointed Reconn as its distributor for Threat Intelligence (TI) and Attack Surface Management (ASM) solutions across the Middle East and Africa. Developed by AI SPERA, Criminal IP provides decision ready threat intelligence and AI powered attack surface management used by security teams worldwide, with integrations across leading SIEM, SOAR and XDR platforms. MSSPs, SOC teams, threat analysts and security operations centers across the Middle East, North Africa and Sub Saharan Africa will gain access to Criminal IP's capabilities, including real time IP intelligence, domain scanning, OSINT data and dark web monitoring.

Regional security teams face distinct challenges: advanced threat actors targeting critical infrastructure, complex cloud and hybrid environments that are difficult to monitor, and regulatory mandates from central banks requiring visibility into external threats. Criminal IP's continuous global IP scanning across 4.29 billion addresses helps teams detect threats earlier by identifying C2 servers, tracking threat actors and surfacing leaked credentials before attacks occur — reducing the time between detection and response.

Criminal IP already operates in 150+ countries and integrates with 40+ cybersecurity platforms, including Palo Alto, Fortinet, OpenCTI and Wazuh. The partnership with Reconn expands Criminal IP's reach into MEA, where demand for threat intelligence and attack surface management is accelerating.

"Every SOC and MSSP we talk to in the region needs visibility into threats coming from outside their network," said Shenoy Sandeep, Founder of Reconn. "Criminal IP's continuous IP and domain scanning closes gaps traditional tools miss. This partnership lets us bring that capability to customers, helping them detect threats earlier, respond faster and understand exactly what they're defending."

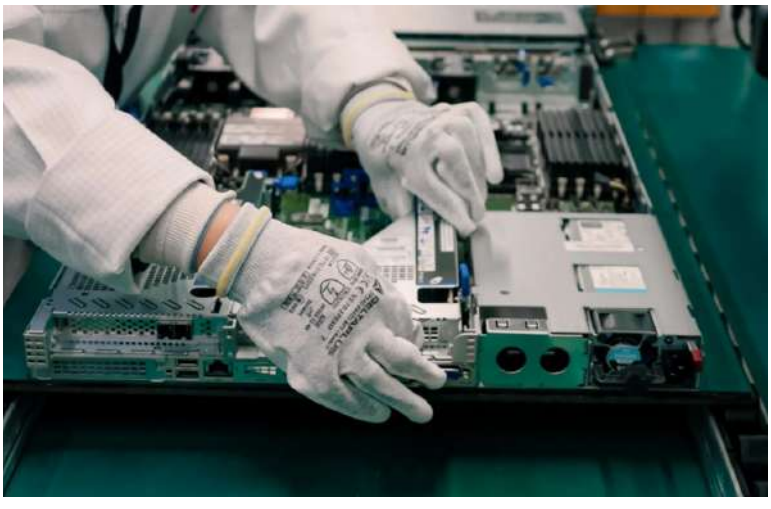


"We see the Middle East and Africa as strategically important regions where organizations need greater visibility into external threats and expanding attack surfaces," said Byungtak Kang, CEO of AI SPERA. "Our partnership with Reconn combines Criminal IP's global intelligence with Reconn's regional expertise to help teams identify exposure, understand threats in context and respond before incidents occur."

Reconn will provide end to end support for Criminal IP deployments, including SIEM/SOAR/XDR integrations, proof of concept engineering, threat intelligence training and ongoing technical support.

Organizations across MEA can explore Criminal IP's free threat intelligence search engine at search.criminalip.io or contact Reconn for demonstrations, attack surface assessments and regional implementation planning.

HPE Launches 'Saudi Made' ProLiant Gen12 Servers



HPE announced the launch of the newest generation of 'Saudi Made' servers, expanding its locally produced portfolio to include the HPE ProLiant Compute DL360 and DL380 Gen12 models. Built at the alfanar facility in Riyadh and powered by Intel Xeon 6 processors, the new systems support Saudi Arabia's ambition to strengthen domestic technology production and diversify the national economy.

"We are excited to take the production of locally built HPE 'Saudi Made' servers to the next level," said Mohammad Alrehaili, VP & Managing Director for the Middle East at HPE. "Powered by Intel Xeon 6 processors, these new servers deliver the security, manageability, performance and energy efficiency Saudi organizations need to accelerate digital transformation. As we continue to invest in Saudi based production, our commitment to supporting the Kingdom's Vision 2030 remains stronger than ever."

HPE and Intel's continued investment in local manufacturing advances national production goals and supports Vision 2030 by enabling organizations to deploy secure, modern infrastructure closer to their data sources. This directly addresses rising demand for digital sovereignty, helping organizations process and store data within national borders, maintain visibility and control, and comply with evolving data residency regulations.

Building on the momentum of HPE's 'Saudi Made' initiative, the new ProLiant Gen12 servers deliver comprehensive security, simplified management and AI driven performance optimization. Engineered for efficiency, the systems offer up to 41% better performance per watt compared to legacy enterprise hardware and up to 65% annual power savings, enabling organizations to support increasingly data intensive workloads while managing rising energy demands.

"The launch of the next generation HPE 'Saudi Made' servers, powered by Intel Xeon 6 processors, reflects the depth of our collaboration with HPE and our shared commitment to advancing Saudi Arabia's digital future," said Taha M. Khalifa, General Manager for Middle East and Africa, Intel Corporation. "By bringing AI ready infrastructure to the region, we are empowering local organizations to innovate, compete and thrive in an increasingly data driven world."

Featuring the 'Saudi Tech' logo, the servers are available across Saudi Arabia and select regional markets including Jordan, Egypt and GCC countries. As digital sovereignty rises on regional agendas, the 'Saudi Made' ProLiant Gen12 servers offer a trusted foundation for resilient, compliant and independently governed digital infrastructure.

Red Dot Distribution Reshapes Leadership

Red Dot Distribution announced plans to enter a new chapter of growth with a revised leadership structure designed to sharpen strategic focus, strengthen execution and support its long term ambitions across the region.

After 25 years at the helm, Munir Bharwani transitions from CEO to Managing Director, where he will focus on the company's broader strategic vision, governance and key stakeholder relationships. Nishad Mairal steps into the role of Chief Executive Officer, leading Red Dot's operations, performance and growth agenda across the Middle East and Africa.

This leadership evolution reflects Red Dot Distribution's commitment to sustainable growth, stronger governance and long term value creation.

Over the past 25 years, Red Dot Distribution has become one of the region's leading technology distributors, connecting world class vendors with a wide network of channel partners across diverse markets. The company has earned a reputation as a reliable partner through its market expertise, lasting relationships and focus on customer success.

As Managing Director, Munir Bharwani will guide long term strategy, governance and future growth opportunities. As CEO, Nishad Mairal will drive operational excellence and execute Red Dot's vision as it expands its impact across the region.



Commenting on the transition, Bharwani said: "We've always believed that staying true to our values while embracing change is the key to lasting success. This leadership transition reflects the maturity of our business and our confidence in the future. Nishad's experience and leadership are invaluable as we build on our strong foundation and look forward to what's next."

Mairal added: "Red Dot Distribution's success has always been driven by strong partnerships, exceptional people and a commitment to creating value across the technology ecosystem. Guided by our vision of Techquity, we aim to expand our impact, unlock opportunities for partners and help drive meaningful digital transformation across the Middle East and Africa."

With a strengthened leadership structure and a clear strategic direction, Red Dot Distribution is well positioned to seize new opportunities in the rapidly evolving technology sector. The company remains dedicated to empowering channel partners, enabling vendor growth and delivering sustainable value across the region.

Tech Mahindra Unveils Zero Gravity Telco Architecture



Tech Mahindra unveiled its Zero Gravity Telco Architecture, a strategic framework designed to help communication service providers (CSPs) systematically overcome the structural barrier stalling their AI ambitions, and help accelerate the transition to AI-native, autonomous operations.

Telecom operators are entering a new era where competitive advantage will depend on investments in AI-led automation and autonomous operations. And while investments in AI, cloud, and 5G are growing, most AI initiatives are losing their momentum, unable to cross into core operations. The reason for this is often the underlying state that may be too fragmented and semantically inconsistent for agents to reason about safely.

For most CSPs, the challenge is the embedded business logic, rules, and the meaning that is trapped inside the systems for decades. Every AI initiative must first negotiate with the accumulated weight of these systems before it can deliver value.

Tech Mahindra's report names this phenomenon Legacy Gravity, the accumulated pull that decades-old systems exert on every new initiative. Just as physical mass creates gravity, the business rules and definitions built up inside an operator's systems over decades creates a pull that slows every business change initiative and holds AI back. Zero Gravity Telco ArchitectureM addresses this by simplifying the technology estates, moving essential business rules and definitions into a shared, governed layer and establishing trusted foundations that AI agents can safely draw on.

The framework underscores that; success depends on building the right foundation first. Operators that rush to deploy autonomous AI on fragmented systems and inconsistent data often face higher costs, slower outcomes, and growing skepticism around AI's value. By first simplifying technology estates and establishing trusted, governed data foundations, CSPs can unlock AI's full potential with greater confidence, scale, and measurable business impact. In this way, escaping Legacy Gravity becomes the critical first step toward becoming a truly adaptive, AI-native telecom operator.

Central to the framework is the Zero Gravity Index, a maturity diagnostic that helps telecom leaders assess their organization's readiness for AI-native transformation while recommending a trajectory sequence from legacy environments to adaptive, intelligent operations. Combined with a layered target architecture, the framework helps CSPs build scalable, governed, and agent-ready enterprises capable of supporting future business models.

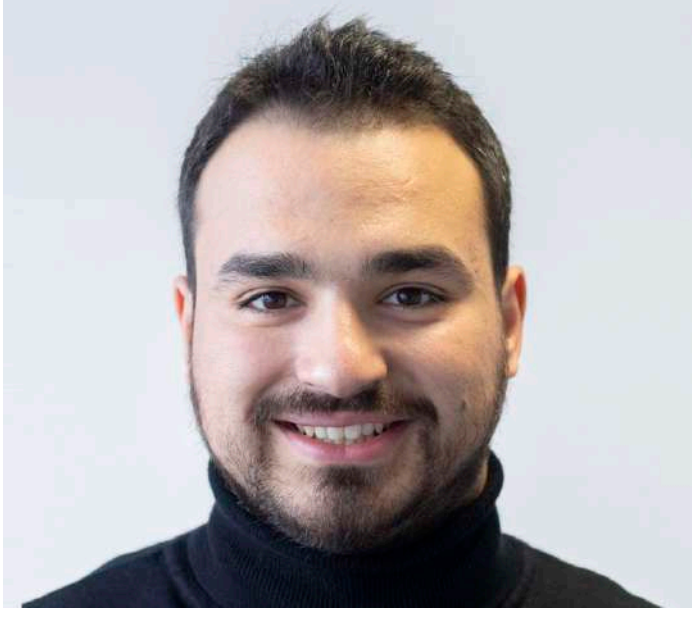
VMRay to Challenge Conventional Cyber Defense at GISEC Global 2026

VMRay, a developer of advanced malware analysis and threat detection solutions, together with regional distribution partner Shifra, today announced its participation at GISEC Global 2026, taking place from September 16–18 at the Dubai Exhibition Centre, Expo City Dubai. The company will use the event to highlight how modern cyber risk has shifted from isolated exploits to fast moving, highly orchestrated threats that demand deeper behavioral understanding rather than static compliance.

"Defenders face an environment where evasive, novel and highly targeted threats easily bypass traditional network perimeters," said Dr. Carsten Willems, CEO of VMRay. "Knowing something is malicious is only the beginning. A verdict tells you a threat exists, but not what it does — and that behavioral clarity is what enables confident response and trustworthy intelligence. At GISEC, we aim to help enterprises move past surface level reassurance and toward deep, behavioral resilience."

Across the Middle East, organizational vulnerability is increasingly shaped by the speed and coordination of modern delivery mechanisms. AI assisted threat actors, decentralized pipelines, and hyper targeted tactics allow malicious files, links, and infrastructure to penetrate enterprise environments faster than traditional controls can interpret them. As a result, the defender's priority is no longer simply determining whether an artifact is malicious, but understanding its execution path, external infrastructure, and operational intent. This behavioral visibility enables teams to build precise, environment specific intelligence rather than relying on generic indicators.

Phishing exemplifies this shift. What once appeared as a single suspicious email has evolved into multi stage delivery paths involving password protected attachments, QR code redirects, and fragmented payloads engineered to appear benign at each step. "When threats are designed to evade filters at scale, a simple 'clean or malicious' flag leaves critical gaps," said Hüseyin Fatih



Akar, Security Product Manager at VMRay. "Defenders need clear insight into an attack's mechanics, objectives, and evasion protocols."

At Stand D120, Hall 6, VMRay and Shifra will demonstrate how advanced malware and phishing analysis, combined with targeted threat intelligence such as the UniqueSignal feed, reduces operational noise for defenders. The showcase emphasizes a core principle: SOC and IR automation is only as reliable as the analysis behind it. Removing environmental noise and blind spots enables confident, repeatable operational decisions.


REVIEW CENTRAL
MIDDLE EAST
UNVEILING THE FUTURE OF TECH
AI-POWERED REVIEWS
SMART LIVING SOLUTIONS
NEXT-GEN GADGETS
IMMERSIVE TECH
CONNECTIVITY REDEFINED
DISCOVER MORE AT REVIEWCENTRALME.COM

SUMIT KUMAR
CHANNEL & DISTRIBUTION MANAGER FOR THE MIDDLE EAST AT BITDEFENDER

> Our goal is to empower partners with advanced tools, training and incentives that help them deliver high value services aligned with regional demand.



BITDEFENDER SETS A PREVENTION FIRST CYBER VISION FOR THE MIDDLE EAST'S AI ERA AT GISEC 2026

Sumit Kumar, Channel & Distribution Manager for the Middle East at Bitdefender, emphasizes that we will present a prevention first cyber defense strategy at GISEC 2026, showcasing unified visibility, AI driven protection and MDR expertise to help Middle East enterprises strengthen resilience as they accelerate cloud and AI adoption.

What are the biggest cybersecurity growth opportunities Bitdefender sees in the Middle East, especially as enterprises accelerate AI adoption and cloud transformation?

We see extraordinary growth opportunities in the Middle East as governments and enterprises accelerate cloud adoption, AI integration and large scale digital transformation. The region is moving quickly, building modern digital economies and expanding distributed applications, cloud workloads and identity driven ecosystems. This pace creates a powerful need for unified protection that reduces complexity rather than adding to it. As we engage with regional organizations, we consistently hear that they want to secure rapid transformation without multiplying tools, consoles or operational overhead. Our perspective is shaped by the reality that "Governments and enterprises across the Middle East are expanding their use of cloud infrastructure, AI and distributed applications, creating demand for unified protection across endpoints, identities, email and cloud workloads."

AI adoption amplifies this opportunity. We see a dual challenge emerging: organizations must defend against AI assisted attacks while also using AI to strengthen their own security operations. Our global assessment found that "47.4% of respondents lacked full visibility into employees' use of shadow AI," and unauthorized access to cloud infrastructure was the most frequently reported incident category. Even though these findings are global, they mirror what we observe in the Middle East—shadow AI, unmanaged cloud expansion and identity sprawl are becoming major sources of risk. As enterprises adopt AI powered workflows and expand hybrid environments, we see strong demand for platforms that unify endpoint, identity, email and cloud protection, backed by AI driven analytics and automation. The region's digital acceleration aligns directly with our prevention first strategy and our ability to deliver consolidated visibility across complex environments.

What unique regional challenges are shaping your strategy—from talent shortages to identity-based attacks and rising regulatory expectations?

We shape our regional strategy around three major challenges that Middle Eastern organizations consistently face. The first is the shortage of cybersecurity talent. Many enterprises cannot recruit or retain enough specialists to operate security operations centers around the clock. Our global research shows that "47.6% of surveyed organizations could not staff 24/7 coverage," and this challenge is even more pronounced in fast growing digital economies. This reinforces the regional need for MDR services, automation and platforms that reduce operational burden.

The second challenge is the rise of identity centric attacks. Threat actors increasingly rely on compromised credentials, social engineering and legitimate administration tools rather than conventional malware. Our research highlights that MFA fatigue, session hijacking and living off the land techniques are among the leading concerns, with Bitdefender Labs finding that "living-off-the-land techniques appeared in 84% of high-severity attacks." In a region where cloud adoption, remote access and distributed identities are expanding rapidly, identity compromise has become the primary entry point for breaches. This drives our focus on behavioral analytics, endpoint hardening and identity aware protection.

The third challenge is regulatory pressure. Data residency, sovereignty and compliance expectations are rising across the Middle East. Our research shows that "76.1% of respondents considered data sovereignty an increasingly important buying criterion and 61.6% felt overwhelmed by compliance requirements." While these figures are global, they align closely with what regional enterprises and public sector bodies experience. We see organizations seeking platforms that provide audit ready visibility, predictable data retention costs and integrated compliance reporting. These challenges shape our strategy and reinforce our commitment to unified visibility, risk based remediation and operational simplicity.

How is Bitdefender's technology stack evolving to address advanced threats, MDR demand and AI-driven security operations across large enterprises and government sectors?

We continue to evolve our technology stack toward a unified, prevention first architecture designed for large enterprises and government organizations. GravityZone remains our core platform, bringing together endpoint protection, EDR, XDR, cloud native security, risk analytics and MDR within a single ecosystem. As we often explain to customers, GravityZone "brings together prevention, detection, response, exposure reduction and compliance capabilities within a single architecture," with AI and machine learning applied across prevention, behavioral analysis, correlation and response.

Recent innovations illustrate how we are strengthening this platform. GravityZone PHASR introduces dynamic, user specific endpoint hardening that restricts unnecessary access to tools commonly abused in living off the land attacks. Security Data Lake expands visibility by centralizing native and third party telemetry from endpoints, networks and clouds, enabling faster investigations, longer term search and more efficient MDR delivery. We emphasize that Security Data Lake "extends visibility across multiple security controls, helping organizations central-



ize telemetry, accelerate investigations, reduce operational complexity and support compliance requirements."

Extended Email Security enhances protection against phishing, impersonation, BEC and ransomware by combining gateway and post delivery analysis with endpoint intelligence. Our MDR service provides 24/7 monitoring, hunting, response and consulting through interconnected SOCs across North America, Europe and Asia. For large enterprises and government sectors, the combination of machine speed analysis and human validation ensures rapid detection and containment. Our technology evolution reflects our commitment to reducing complexity, improving resilience and delivering AI enhanced security operations that scale with regional digital transformation.

How is Bitdefender strengthening its channel program in the Middle East, and what new capabilities or incentives are being introduced for partners in 2026?

We are strengthening our channel program in the Middle East by aligning regional partner needs with enhancements introduced globally through the Partner Advantage Network. These enhancements include a new Platinum tier, dedicated support, joint go to market opportunities and expanded access to MDR and XDR. We highlight that partners benefit from "expanded not-for-resale access to MDR and XDR, tier-based NFR device allocations and a simplified deal-registration process."

We also provide financial incentives, lead generation tools, certification programs and hands on training. Partners gain access to PHASR, EASM, Security Data Lake and MDR, enabling them to build differentiated managed services. We often explain that Bitdefender expanded opportunities for partners to test and deploy solutions in their own environments, which is especially valuable for MSPs seeking operational experience before delivering services to customers. In the Middle East, where channel led growth is essential, these enhancements support stronger collaboration with distributors, MSSPs and systems integrators. Our goal is to empower partners with advanced tools, training and incentives that help them deliver high value services aligned with regional demand.

What skills, certifications or tools do partners now need to effectively deliver Bitdefender's solutions in high-growth segments such as MDR, XDR and cloud security?

We see partners increasingly needing advanced capabilities that go beyond traditional endpoint deployment. They must understand GravityZone architecture, policy design and multi tenant administration, as well as EDR/XDR investigation, threat hunting and incident response workflows. We emphasize that partners need skills in "cloud workload, identity and security-posture management" and must be able to integrate telemetry across email, identity, network and cloud environments.

MDR onboarding, escalation management and customer service delivery are becoming essential competencies. Partners must be able to consolidate telemetry from multiple tools, validate alerts efficiently and communicate measurable risk reduction outcomes. Our Partner Advantage Network provides certification, technical and sales training, a knowledge base and hands on access through an expanded NFR program. MDR access for MSPs and full suite demonstration environments allow partners to build operational experience before delivering services. As regional enterprises adopt more complex hybrid environments, partners must be able to translate technical findings into business outcomes and support customers in reducing exposure across cloud, endpoint, identity and email ecosystems.

How does customer feedback influence your product roadmap and regional strategy, and what insights have Middle East customers shared that shaped recent updates?

We rely heavily on customer and partner feedback to shape our roadmap and regional strategy. The enhancements introduced to our Partner Advantage Network reflect the "voice of our partner community," demonstrating our commitment to incorporating real world insights into product and program design. Our recognition as a 2026 Gartner Peer Insights Customers' Choice for endpoint protection further reinforces the importance of customer experience in our development priorities.

Recent updates reflect recurring customer demands for fewer consoles, more automation, reduced alert fatigue and greater visibility across cloud, endpoint, identity and email environments. We often explain that updates such as Security Data Lake, PHASR, Compliance Manager and Extended Email Security "address recurring customer priorities: fewer consoles, less alert noise, faster deployment, more automated remediation, predictable data-retention costs and better compliance visibility." These priorities align closely with what Middle Eastern enterprises tell us: they want operational simplicity, unified visibility and scalable security operations that support large digital transformation programs. This feedback loop ensures that our solutions remain aligned with regional needs.

What investments is Bitdefender making in after-sales support, local service delivery and customer success to ensure long-term cybersecurity resilience?

We are investing significantly in after sales support, local service delivery and customer success to ensure long term resilience for regional customers. Our global MDR service provides "24/7 monitoring, threat hunting, analyst-led recommendations and security consulting," supported by interconnected SOCs across North America, Europe and Asia. Analysts share intelligence across the network and provide Level 1–3 escalation coverage, ensuring rapid response to emerging threats.

In the Middle East, we rely on a strong channel ecosystem to deliver localized support. Dedicated account management, pre and post sales assistance, technical training, NFR environments and MSP enablement help partners provide implementation and ongoing support close to customers. We emphasize that the channel is "an important part of local service delivery," reinforcing our commitment to empowering regional partners with the tools and expertise needed to support customers throughout their security lifecycle. These investments ensure continuous guidance, operational support and expert led response capabilities.

What major innovations, demos or threat-intelligence capabilities will Bitdefender showcase at GISEC this year, and how do they reflect your regional priorities?

We plan to showcase innovations that highlight our prevention first strategy and our focus on reducing complexity across hybrid environments. PHASR demonstrations will show dynamic, user specific hardening against living off the land attacks. Security Data Lake will demonstrate correlation of native and third party telemetry across endpoints, networks and clouds, enabling faster investigations and more efficient MDR delivery. We highlight that Extended Email Security will demonstrate its ability to detect and remediate phishing, impersonation and BEC before and after delivery.

We will also showcase XDR and MDR workflows that combine automated correlation and containment with human analyst judgment, as well as EASM, cloud native protection, compliance reporting and threat intelligence from our global sensor network. These capabilities reflect regional priorities around AI resilience, cloud protection, critical infrastructure security, operational simplicity and compliance. With PHASR having made its Middle East debut at GISEC 2025, we enter 2026 with a strong foundation for demonstrating our broader prevention first platform.

What core message is Bitdefender bringing to GISEC—and how does it speak to the evolving needs of CISOs, partners and hyperscalers in the Middle East?

We are bringing a clear message to GISEC: cyber resilience starts with prevention, is strengthened through unified visibility and is sustained through expert led response. This message speaks directly to the evolving needs of CISOs, partners and hyperscalers in the Middle East. For CISOs, it emphasizes reducing exposure before an attack, consolidating fragmented security operations and achieving measurable risk and compliance outcomes. For partners, it highlights the opportunity to build differentiated managed services and recurring revenue on top of our unified platform. For hyperscalers and cloud providers, it underscores the importance of consistent security across endpoints, identities, email and cloud workloads.

This message is especially relevant in the Middle East, where ambitious AI and cloud programs require trusted security, scalable operations and clear governance. Our approach—using AI to improve defender speed and precision while keeping human expertise central to consequential response decisions—aligns with regional expectations for innovation and accountability.

What are Bitdefender's strategic plans beyond GISEC 2026 in terms of expansion, partnerships, technology rollout and regional cybersecurity leadership?

Beyond GISEC 2026, we plan to continue expanding GravityZone, deepening integration of email, cloud, identity and external attack surface telemetry, and driving broader adoption of PHASR, Security Data Lake, XDR and MDR. We support "more than 41,000 channel and MSP partners globally," and our acquisition of Mesh Security added advanced email security technology and substantial MSP expertise.

These developments strengthen our global and regional partner ecosystem. In the Middle East, we aim to deepen relationships with distributors, MSSPs, systems integrators, cloud providers and government focused partners. We also plan to expand local technical enablement and deliver solutions aligned with sovereignty and regulatory requirements. We see opportunities to strengthen regional leadership through threat research sharing, collaboration with public institutions and participation in cybersecurity skills development. As regional enterprises continue to modernize and adopt AI driven operations, our unified platform and prevention first strategy position us to play a central role in shaping cybersecurity resilience across the Middle East.





PROF. K. K. SINGH, GENERAL MANAGER, BITS PILANI, DUBAI CAMPUS

WOMEN IN TECH TAKE CENTER STAGE AT THE WOMEN OF SUBSTANCE CONFERENCE & AWARDS 2026

The Women of Substance Conference & Awards 2026, held on 9 September at BITS Pilani Dubai Campus, opened with a powerful sequence of voices that set the tone for a day of inspiration and impact. The morning began with an insightful keynote by Prof. K. K. Singh, General Manager, BITS Pilani, Dubai Campus whose reflections on education and women's leadership framed the conference's purpose with clarity and conviction, followed by several presentations from illustrious women from different walks of life. Their diverse journeys — spanning entrepreneurship, technology, finance, wellbeing, and education — collectively reinforced the conference's mission to celebrate women who lead with purpose, resilience, and vision. This remarkable gathering was made possible through the support of our valued sponsors — ASBIS Middle East, AMD, CREDO, and BITS Pilani, Dubai Campus — whose commitment to empowering women and advancing leadership enabled the success of this transformative event.

Among the standout sessions were compelling narratives from leaders who have shaped their industries through grit and expertise. K. Umashankari, Managing Director at Luckystar Computers, shared her transformative journey from survival to self reliance, offering a deeply personal lens on women's entrepreneurship. Meenal Sanjeev Madavi, CEO of Power & Cooling ME, delivered a practical and empowering roadmap for women entering and excelling in the tech sector, while Seema Hallon, CHRO at Deriv.com, explored how clarity, competence, and resilience help professionals stay valuable in uncertain times. Complementing these perspectives, Shadan Izhiman, Managing Director at Athena Dermatology Clinic, emphasized wellbeing driven leadership; Nooreen Naaz, Assistant Vice President at Graystone Capital, championed financial independence as a cornerstone of empowerment; and Nahid Afshan, Head of Admissions at BITS Pilani Dubai Campus, highlighted the importance of inclusive academic environments in shaping future leaders.

The conference also came alive through dynamic panel discussions that showcased collective wisdom and intergenerational dialogue. Subela Bhatia's panel — From Classroom to C Suite — A Playbook for the Next Generation of Women Tech Leaders — featured Dr. Nidhi Seghal, Head of Business and Humanities at Curtin University Dubai; Bhavna Arun, Regional Sales Manager at Algosec; Roya Hatamleh, Security Solutions Sales at Microsoft; and Sujatha Malanna, Partner Account Manager at KnowBe4 offering a powerful blueprint for young women aspiring to leadership roles in technology.

Later, Kamya Chandebhamar moderated the vibrant student panel Empowering Young Women to Lead in a Tech Driven Future, joined by Aarna Munjal, Yukta Gidwani, Saakhee Madnani, and Kanisha Mahaveer Jain, capturing the hopes, ambitions, and leadership potential of tomorrow's innovators. Together, these sessions reinforced the conference's central message: women's advancement thrives when knowledge, mentorship, and community come together with purpose.

A visual glimpse into the Women of Substance Conference & Awards 2026 captures the energy, pride, and powerful moments shared throughout the day. These images reflect the spirit of leadership and inspiration that defined the event, followed by a special showcase of our award winners — women whose achievements truly embody substance and impact.



ANNA SEREBRYANIKOVA
Co-Founder & Chief Operating Officer, KERNO



CAROL ANNE DIAS
Sales Director, TPV Technology Gulf DMCC



BHAVNA ARUN
Regional Sales Manager, Algosec



JUHI JAIN
Digital Manager, Emirates NBD



EKTA SHETTY
Senior Sales Director, Asia Pacific ,MEA ,Africa ,Turkey & CIS, Shure



GEETHA YECHANA
Director of Business Development, Cyberknight Technologies



SRILAKSHMI BANNIGOL
Group CIO, Switz Group



HANAN ALZAABI
Director Data Architecture and Governance, Statistics Centre - Abu Dhabi



EMMA LEWIS
Head of Technology Service Management, First Abu Dhabi Bank (FAB)



KAERELS FERNANDEZ
Head of Business Development, Devo Ai Technologies



NANCY GHAWANMEH
Regional Sales Manager, Big ID



IVANA DRAGOVIC ROSSI
Marketing Communications Director, e&



SARAH DURR
Regional Head of Channel and Partner Ecosystem - Gulf, Levant & Pakistan, IBM



SANJA HORYLOVA
Purchase and Sales Director, ASBIS Middle East



MIHIKAA SAWLANI
Marketing Manager, Middle East, HMD Global



SUJATHA MALANNA
Partner Account Manager, Knowbe4



VAIDEHI GAWANDE
Co-Founder & CTO, TrevasQ



MEENAL SANJEEV MADAVI
Chief Executive Officer, Power & Cooling ME



SHAIKHA ALDHAHERI
OT Monitoring Manager, TAQA Water Solutions



AZIZA MAKKAR
Business Unit Head - Cyber Security - Middle East & Africa, AmiViz



SONALI BASU ROY
Marketing Manager, Bulwark Technologies



Women Tech Leaders Panel featuring Subela Bhatia, Dr. Nidhi Seghal, Bhavna Arun, Roya Hatamleh & Sujatha Malanna



STUDENT TECH LEADERS PANEL FEATURING KAMYA CHANDEBHAMAR AARNA MUNJAL, YUKTA GIDWANI, SAAKHEE MADNANI & KANISHA MAHAVEER JAIN

GRAYSTONE CAPITAL MAPS THE REAL ECONOMICS OF GCC TECH: FINANCING THE CHANNEL, NOT THE HYPE

Hesham Mohamed J., CEO of Graystone Capital outlines how GCC tech growth is shaped by distributors, long cash conversion cycles and structural financing gaps, and explains why mid market, channel dependent tech firms represent the region's strongest investment opportunity.

Q How does Graystone Capital assess the current Middle East tech landscape, especially given the dominance of distributors and channel partners across the GCC?

Graystone Capital begins with a simple but foundational premise: the GCC tech market is enormous, structurally channel driven, and still expanding at a pace few global regions can match. The region's ICT market is projected to grow from roughly $154 billion this year to more than $240 billion by 2031, yet only a small fraction of that value flows directly between vendors and end customers. Distribution is not an operational detail—it is the architecture of the market. Redington alone operates a network of tens of thousands of channel partners and reported more than $13 billion in consolidated revenue this year. Alongside Redington sit Mindware, StarLink, Ingram Micro, Exclusive Networks, Almasa and dozens of other value added distributors, many of whom have been embedded in the region for two or three decades. A vendor, ISV or solution builder selling into the GCC is almost never selling directly; they are selling through one or two layers of partners who influence pricing, credit terms and, in many cases, the customer relationship itself.

This reality fundamentally changes how Graystone evaluates companies. Reported revenue through a distributor is not a reliable indicator of business health. What matters is understanding who is carrying the receivable, how long the cash conversion cycle runs once the distributor and reseller layers are accounted for, and how exposed the company is to liquidity stress within any single channel partner. Graystone spends more time underwriting the chain of counterparties than underwriting the product. In a market where distribution is structural, the financial risk sits in the middle of the chain, not at the edges.

Q What gaps or inefficiencies in today's distribution-driven tech ecosystem present the strongest opportunities for investment and value creation outside the traditional startup space?

The most persistent gap Graystone sees is a working capital shortfall that has nothing to do



HESHAM MOHAMED J
CEO of Graystone Capital

"In the GCC, revenue through a distributor tells you very little; the real story is who carries the receivable and how long the cash actually takes to come home."

with product quality or market demand. Resellers, systems integrators and mid sized ISVs across the GCC routinely pay principals or distributors upfront while collecting from enterprise and government customers 60 to 120 days later. This is not a venture financing problem; it is a receivables financing problem. It has gone largely unaddressed because it does not fit neatly into a bank's collateral based underwriting model or a VC's equity driven approach.

Regional funding data makes the shape of the gap clear. Equity investment into MENA startups has been uneven through 2026, while debt has taken on a growing share of the load. In July, debt accounted for 56% of all MENA startup funding, up from just 2% a year earlier. PwC has separately highlighted an estimated $250 billion SME financing gap across the GCC, driven by banks' preference for lending to large corporates and government related entities. Channel dependent tech businesses sit squarely inside this gap: too large and cash generative for early stage venture capital, yet too irregular and receivables heavy for conventional bank facilities. Graystone sees the strongest opportunity not in funding the next startup, but in financing the working capital cycles of tech businesses that already have contracted revenue and predictable demand.

Q Which categories of tech companies—such as ISVs, cybersecurity vendors, cloud service providers, AI firms, or channel-focused solution builders—fit Graystone Capital's investment thesis?

Graystone gravitates toward businesses with revenue streams that can be underwritten with confidence. That means confirmed contracts, recurring billing or receivables from creditworthy enterprise or government counterparties. In practice, this points toward managed security service providers and cybersecurity vendors with renewal based contracts, cloud and managed service providers billing on subscription or usage terms, and channel focused solution builders and system integrators with strong receivables from enterprise or government clients. Even if margins are thinner than pure software businesses, the predictability of cash flow makes these companies ideal candidates for structured financing.

Early stage AI firms and pure play ISVs are approached more selectively—not because Graystone doubts the category, but because pre revenue companies or those reliant on one off licensing deals lack the contracted cash flow required to structure a facility. As these companies mature into recurring revenue models, they move directly into Graystone's target profile.

Q How do you evaluate the scalability and regional expansion potential of tech companies that rely heavily on distributor and channel-partner networks?

Graystone focuses on three factors that matter more than headline growth numbers. The first is distributor concentration. A company generating 80% of its revenue through a single distributor is effectively carrying that distributor's credit and operational risk as its own. The second is the quality and aging of receivables, particularly exposure to government or government related entities, where payment terms are longer but default risk is lower. The third is contract structure. A business built on recurring managed service or subscription revenue scales and finances very differently from one built on one off hardware resale through the channel.

Regional expansion follows the same logic. A company that has demonstrated clean receivables management and stable channel relationships in the UAE is a far safer candidate for expansion into Saudi Arabia or Oman than one whose UAE numbers already show strain from structural issues at a smaller scale.

Q What specific financing instruments does Graystone Capital offer to tech companies—such as revenue-based financing, working-capital facilities, growth capital, or structured debt?

Graystone does not lend from its own balance sheet. Instead, it structures and arranges the right facility through its network of banks, private credit funds and regulated fintech lenders, and manages the relationship through to disbursement. Depending on the business model, this typically includes working capital and receivables based facilities structured against confirmed purchase orders or invoices, revenue based financing arranged through partners suited to that model, and structured or growth debt for businesses requiring larger, longer tenor facilities than a standard overdraft. The appropriate instrument depends entirely on the shape of the company's cash flow. A reseller waiting on a 90 day government payment cycle needs a very different facility from a managed services provider with predictable monthly billing.

Q How does Graystone Capital support tech companies in navigating regional challenges like long sales cycles, procurement complexity, and distributor-driven market access?

Government and enterprise procurement in the GCC often moves slowly by design. Multi stage evaluations, local content requirements and payment terms that stretch well beyond delivery are normal, even as several governments push digital procurement reforms to shorten timelines. For tech companies, the challenge is not winning the contract—it is surviving the gap between fulfilling it and getting paid.

Graystone structures facilities against confirmed purchase orders or signed contracts so companies can deliver on large government or enterprise mandates without carrying the entire working capital cycle themselves. Increasingly, Graystone also advises companies on the financing implications of selling through a distributor versus pursuing a more direct route to the customer, since each path carries different receivable timelines and capital requirements.

Q What role does Graystone Capital aim to play in strengthening the Middle East's broader tech ecosystem beyond startups—particularly in enabling mid-market and growth-stage tech firms?

The regional narrative often focuses on early stage venture activity, but the more persistent gap lies in financing for established, medium sized businesses that have outgrown venture style equity and need growth capital, stronger structuring and operational support to expand regionally. These companies do not necessarily want to dilute ownership or wait years for a private equity process. Graystone positions itself squarely in this middle segment, supporting mid market and growth stage tech and tech enabled businesses with the working capital and structured debt they need to scale without giving up equity.

Q As Graystone Capital expands its footprint, which GCC markets or technology verticals are most strategic for your next phase of growth, and why?

Saudi Arabia and Oman are the most strategic markets for Graystone's next phase of growth. Saudi Arabia has led regional funding activity in 2026, topping MENA's monthly rankings in July with more than 60% of total capital raised. Its Vision 2030 procurement pipeline, reportedly exceeding $500 billion in planned outlays, creates the long cycle, high value contracts ideally suited to Graystone's working capital model. Oman represents a newer but highly promising market, with an SME financing gap even wider than the UAE's and strong demand for structured facilities.

On verticals, cybersecurity and managed security services stand out.

The Middle East cybersecurity market is expanding rapidly, and managed services now account for the majority of regional cybersecurity spend, creating recurring, contract based revenue that fits Graystone's financing model well. Cloud and data center services are also closely watched, given the scale of hyperscaler investment entering the region and the long tail of service providers and integrators that will require receivables and growth financing.

CHANNEL PARTNERS CAN CAPITALISE ON DEFENCE FIRMS' GROWING CMMC READINESS GAPS

Sean Kelley, Global Director of Technology Partnerships at Kiteworks, explains that channel partners can seize a major opportunity as many regional defence and dual use tech firms still struggle with rising CMMC requirements, creating demand for compliance focused support.

The Cybersecurity Maturity Model Certification (CMMC) framework is having a great effect on compliance requirements across the Gulf's defence and dual-use technology sectors. Regional manufacturers supplying components for US defence programmes, technology companies supporting US military operations in the Gulf, and vendors operating under ITAR export licences all share a contractual compliance obligation that most regional MSPs have yet to build a practice around. For any MSP with defence-adjacent client bases in the UAE, Saudi Arabia, and the broader Gulf, however, the gap between the obligation and the reality is a practice-defining commercial opportunity.

It is a misconception that CMMC only applies to US businesses. In fact, the framework applies to any contractor that handles Controlled Unclassified Information under a US DoD contract, regardless of where they are based. The compliance obligation follows the contract, not the country of incorporation. Gulf-based manufacturers in aerospace, defence electronics, and systems integration who supply components or services under US programme contracts all fall within its scope. Regional technology services firms supporting US military operations or allied-nation procurement carry the same obligation. As do ITAR-licensed exporters handling CUI as part of controlled technology transfers.

The scale of the market is significant. The CMMC Accreditation Body estimates over 80,000 contractors globally require Level 2 assessment under the current framework. A growing share of that number are headquartered in Gulf Cooperation Council states whose defence and technology sectors are increasingly integrated into US procurement programmes.

Most of these organisations are small to mid-sized businesses with no dedicated compliance infrastructure. As such, they are not equipped to navigate CMMC independently so need a credentialled managed service partner.

That volume estimate is shifting in real time. On 13 July 2026, the US Department of War suspended CMMC Phase Two — the mandatory third-party C3PAO assessment requirement due to take effect on 10 November 2026 — and opened a 60-day programme review, with a Reform Task Force expected to report back around 13 September 2026. The suspension does not touch Phase One: contractors remain contractually obligated to complete CMMC Level 1 and Level 2 self-assessments, and the underlying obligation to protect Controlled Unclassified Information — along



SEAN KELLEY

Global Director of Technology Partnerships at Kiteworks

"Cloud services deployed across the Gulf region that have not obtained FedRAMP authorisation create a specific, documentable compliance gap."

with False Claims Act exposure for misrepresenting compliance — stays fully in force. What is paused is the third-party verification mechanism, not the requirement it verifies. For Gulf MSPs, that is a reason to move earlier, not later: the self-assessment workload is active today, and whatever assessment model emerges from the review will still run on the same NIST SP 800-171 control set and unified CUI-governance evidence base a self-assessment practice already requires.

FedRAMP Is the Fault Line

CMMC Level 2 maps to all 110 controls in NIST SP 800-171 Revision 2, assessed across 17 control domains by an accredited C3PAO. Those domains cover how CUI is accessed and authenticated, how every CUI channel interaction is logged, how systems are configured and maintained, and how incidents are detected, escalated, and reported. The C3PAO evaluates each domain against actual implemented controls and documented evidence, not policy aspirations. Further, the US defence contracting clause governing cloud services DFARS 252.204-7012 – requires that any cloud service processing, storing, or transmitting CUI on behalf of a DoD contractor be FedRAMP Moderate Authorised or demonstrate equivalent security through a formal DoD determination.

Cloud services deployed across the Gulf region that have not obtained FedRAMP authorisation create a specific, documentable compliance gap.

The False Claims Act exposure further compounds the platform selection risk. A contractor that falsely certifies CMMC compliance to the DoD faces significant civil penalties. This exposure applies to the contractor regardless of where it is incorporated. MSPs advising clients on compliance posture carry reputational and potential indirect risk when the platforms they deploy cannot withstand C3PAO scrutiny.

One Control Plane. One Audit Story.

The technical principle that separates deployable CMMC solutions from compliance aspirations is unified CUI channel governance. CUI moves through organisations across multiple technical channels. Whether that be email, file sharing, managed file transfer, SFTP, and data forms. An MSP that deploys separate point solutions for each channel creates a high-complexity audit surface that multiplies the likelihood of an assessor identifying an inconsistency.

Far better to use a platform that governs all CUI channels through a single control plane and captures every interaction in a single immutable audit log. It will reduce complexity significantly by ensuring that the C3PAO receives a coherent, complete evidence package rather than a manually assembled collection of system-specific records. That compression in evidence preparation time directly improves assessment outcomes and client satisfaction. Plus, it strengthens the MSP's positioning by demonstrating that the compliance programme has been operating as designed throughout the certification cycle.

MSPs and MSSPs in the region that are listed as a Registered Practitioner Organisations through the CMMC Accreditation Body, creates a services differentiator. The RPO credential signals a recognised baseline of competence and a professional code of conduct.

The three-year certification cycle, provides exactly the recurring service structure that mature MSP practices are built around. Initial platform deployment and assessment preparation as project revenue; ongoing monitoring, evidence management, and policy governance as recurring managed service revenue; and reassessment preparation in year three as a defined, billable deliverable.

MSPs in the Gulf who establish credible CMMC practices now are positioning ahead of a compliance wave that is still building, even with third-party assessment paused for review. As US defence procurement increasingly references CMMC compliance in contract requirements, and as regional contractors deepen integration with US and allied-nation programmes, demand for qualified managed service partners will only grow. The credential, the platform, and the methodology are the three components required to capture that demand. The window to establish a first-mover position will only be open for a limited time. Make sure you don't miss out.



MONGODB.LOCAL ARRIVES IN RIYADH ON 17 NOVEMBER TO UNITE THE KINGDOM'S AI AND DATA COMMUNITY

Channel Post MEA sat with Abdulrazzak Al Zubaidi, Regional Director for the Public Sector across the Middle East and Turkey at MongoDB, to discuss MongoDB.local arriving in Riyadh on 17 November at JW Marriott Riyadh on King Fahd Road, bringing the MongoDB community together to share ideas, showcase innovation, and shape the next generation of applications that will strengthen the Kingdom's data driven ecosystem.

Q How does MongoDB.local Riyadh reflect the momentum of Saudi Arabia's fast-evolving digital and AI landscape?

What stands out most about Saudi Arabia today is the remarkable speed of its transformation. The Kingdom's decision to designate 2026 as the Year of Artificial Intelligence under the patronage of HRH Crown Prince Mohammed bin Salman is far more than a symbolic announcement; it is a clear national signal that AI has become a strategic pillar of economic growth, social progress, and technological leadership. That commitment from the top is already driving substantial investment across government entities, major enterprises, and a rapidly expanding generation of startups. The national conversation has shifted from imagining what AI could achieve to confronting the practical realities of running AI systems reliably in production. This shift places far greater scrutiny on the data foundation. An AI application is only as strong as its ability to access the right information at the right moment and withstand real world operational pressure. Without a unified, flexible, and resilient data layer, even the most advanced model becomes constrained by its underlying architecture.

Building that foundation requires collaboration across government platform teams, enterprise architects, developers, and startups. Saudi Arabia's digital transformation is an ecosystem movement, not isolated initiatives. MongoDB.local Riyadh, our sole regional stop this year, creates a space for that ecosystem to connect. On 17 November, government leaders, enterprises, developers, startups, and partners will come together to exchange ideas, challenge assumptions, and share real world experiences—accelerating projects and building solutions that match the Kingdom's national ambition.

Q What modernization priorities are top of mind for Saudi enterprises attending MongoDB.local Riyadh, especially around cloud, data, and AI?

The priority I hear most often from Saudi enterprises is how to modernise without putting the business at risk. A bank cannot pause its services to rebuild its architecture, and a government organisation cannot put citizens' needs on hold while it reworks its systems. No one wants to choose between modernising and staying stable, and this tension is shaping how organisations approach cloud adoption, data architecture, and AI readiness. At the same time, there is growing recognition that AI readiness begins with data readiness. When information is difficult to access, locked in legacy systems, or scattered across disconnected environments, getting an AI application into production becomes far more challenging. Even the most advanced model cannot compensate for fragmented or inaccessible data.

Q How can MongoDB help Saudi start-ups build scalable, secure, and AI-ready applications showcased at MongoDB.local Riyadh?

For a startup, the goal is always the shortest possible path from an idea to an application running in production. Speed matters because early-stage companies need to test concepts, learn from customers, iterate quickly, and adapt to market feedback. The architecture should never become the obstacle that slows them down. MongoDB's document model removes a great deal of friction because developers can reshape their data as the product evolves. Startups rarely know on day one what their final data model will be, and forcing them into rigid schemes can hinder innovation. A flexible data model lets them experiment, pivot, and refine their product without costly rework.

Bringing operational data and vector search into the same platform means a small team is not managing separate databases for different parts of the application. This is crucial when building intelligent search, personalised recommendations, or conversational AI features. With lean engineering teams, reducing operational complexity allows startups to focus on the product rather than the infrastructure. The advice I give any founder is to design security and resilience from the beginning, because these are difficult and expensive to retrofit once customers rely on the service. Security, reliability, and scalability are what turn a prototype into something that can run at scale. MongoDB enables startups to build quickly without sacrificing the architectural foundations they will need later.

Q What new opportunities exist for distributors and channel partners to deliver MongoDB-powered solutions across the Kingdom?

The opportunity for distributors and channel partners in Saudi Arabia goes far beyond supplying technology. Customers increasingly want guidance on where to begin, which applications to modernise, and how to turn an AI idea into something that delivers measurable value. Partners with the ability to lead that journey are in high demand. Local knowledge is crucial, because understanding how a financial institution operates, what a public sector organisation requires, or where a telecommunications provider faces complexity makes the technology relevant to each customer. This creates opportunities in migration, application development, integration, and ongoing support. Enablement is equally important, so we invest heavily in training partner teams to lead these conversations. Our collaboration with Google Cloud at LEAP shows the impact of complementary strengths. The regional partner ecosystem is central to MongoDB.local Riyadh, because partners bring context, relationships, and implementation expertise essential to scaling modernisation and AI adoption across the Kingdom.

Q How can system integrators leverage MongoDB's platform to accelerate enterprise modernization and AI adoption in Saudi Arabia?

System integrators are often the ones connecting a customer's ambition to the reality of its existing systems. They understand the dependencies, the operational constraints, and what it takes to intro-



ABDULRAZZAK AL ZUBAIDI

Regional Director for the Public Sector across the Middle East and Turkey at MongoDB

"Saudi Arabia's digital transformation is an ecosystem Imovement, not isolated initiatives."

duce changes safely. MongoDB gives integrators a platform flexible enough to modernise in stages, integrating relevant data and updating selected applications without forcing a complete overhaul. For AI work, this means making operational information available to the applications that need business context. AI systems are only as effective as the data they can access, and integrators play a critical role in bridging legacy environments with modern architectures. D360 Bank is the regional example I keep coming back to. They built a distributed, cloud-native architecture for mission-critical operations, processing high transaction volumes with a flexible data representation that shortened their time to market. Those lessons transfer across sectors. Integrators working in government, financial services, and telecommunications can apply the same architectural thinking to very different customers, with our technical teams alongside them. The combination of MongoDB's platform and integrators' domain expertise accelerates modernisation while reducing risk.

Q How can enterprises, startups, channel partners, and integrators collaborate more effectively to build stronger, data-driven solutions using MongoDB?

The best starting point for collaboration is a clearly defined problem everyone recognises. Improving a service experience, making information easier to find, or reducing the time required to launch something new creates a shared objective. Once the outcome is clear, each organisation contributes where it is strongest: enterprises bring operational knowledge, startups offer fresh thinking, integrators and channel partners provide implementation expertise and local understanding, and MongoDB delivers the data platform and technical depth.

What is often underestimated is the need to agree early on how success will be measured and what it takes to move beyond a demonstration. A prototype must still work with real data, integrate with existing systems, and be supported in production. This is where collaboration either strengthens or falters. Effective partnership requires clarity, shared accountability, and a commitment to moving past proof of concept thinking.

Q How does MongoDB's roadmap and events like MongoDB.local Riyadh support Saudi Arabia's Vision 2030 goals for innovation, entrepreneurship, and tech sovereignty?

Vision 2030 calls for intelligent public services, a startup base capable of building globally from the Kingdom, and real control over national data. All of this depends on the strength of the underlying data foundation, which is where we contribute. Our roadmap focuses on making modern, AI powered applications easier to build while giving customers genuine flexibility in how they deploy. Because Atlas and Enterprise Advanced share the same document model and query engine, an organisation can build an application once and run it either in the cloud or self managed wherever data residency or regulatory requirements apply, without re architecting. Each organisation still evaluates its own security and governance posture, but the platform gives them the freedom to choose the model that aligns with their sovereignty needs.

Sovereignty also relies on skills. Control over systems means little without local expertise to build and operate them. MongoDB.local Riyadh brings developers, engineers, customers, and partners together to strengthen that capability. It supports Vision 2030 by enabling innovation, accelerating entrepreneurship, and building the technical foundations required for long term digital independence.

GUARDBREAKER DERAILING AI ASSISTED MALWARE ANALYSIS WITH A CODE COMMENT

Tomáš Foltýn, security writer at ESET, underlines that LLM based code scanners won't help attackers build a nuclear weapon — but that refusal could ultimately work in their favor.



Malware developers have long adapted their code and tactics to the defenses and scrutiny that are likely to stand in their way. Using various evasion and anti-analysis methods, they routinely attempt to hinder code analysis or prevent their malware from revealing its true behavior while under inspection. Other tools – notably, EDR killers, documented extensively by ESET researchers – go straight after security solutions themselves.

As LLM-based tools increasingly assist with various security tasks, including code triage and analysis, it was only a matter of time before threat actors began to look for practical ways to subvert them, too. Alongside conventional evasion techniques, some are taking a different tack: the adversarial input that's intended to frustrate analysis is left in plain sight.

ESET researchers recently spotted one such attempt in a VBScript that the Russia-aligned group UAC-0099 used in the early stages of an attack against a target in Ukraine.

By inserting a decoy request for guidance on building a nuclear weapon into the script's comment, the bad actor aimed to trip the safety guardrails of an LLM-powered code scanner and cause it to stop inspecting the rest of the file – before ever reaching the malicious code. The script's purpose was to download and install MATCHBOIL, a loader used exclusively by this group to deliver additional payloads.

This simple technique, which ESET has named GuardBreaker, relies on precisely the kind of 'request' that LLM models are known to decline.

Unlike many other tricks in attackers' evasion playbooks, this decoy comment is there for 'everyone' – especially for the models analyzing the code – to see. In addition, it has no effect on the script's behavior at runtime, of course. Nonetheless, its presence suggests that UAC-0099 was accounting for an AI system in the target's defenses – just as in other recent attacks the group also checked for processes associated with established analysis tools such as IDA and Wireshark.

Anti-analysis takes aim at another target

GuardBreaker is best understood as a very simple attempt at prompt injection: an attacker's input reaches the LLM at inference time through a file that's being analyzed. That way, it aims to exploit an architectural weakness in today's LLMs, which process untrusted content and trusted instructions without dependable boundaries between the two.

Similar attempts to interfere with LLM-powered scanners have surfaced especially in software supply-chain attacks. For example, Socket found fabricated system instructions and policy-triggering content placed ahead of a JavaScript payload in malicious PyPI packages. Reporting on the same broader campaign, StepSecurity found a prompt that flat-out instructed any analyzing model that parsed the file to disregard the malicious code and report the package as clean.

In another incident, researchers spotted an npm package whose main JavaScript file repeated "You're absolutely right!" tens of thousands of times in the hopes of exhausting the model's context window and putting the malicious script that followed beyond practical analysis.

Attackers could attempt to blind the analysis pipeline to malware through other trivial tricks, or even their combinations: unusual or awkwardly structured files could end up being truncated or parsed only in part. Some parts of the malicious code could be concealed under the pretense of being confidential information or other sensitive data.

Other attacks could deploy custom file types that would require attackers' tools to process, whereas others still could steer AI agents towards actions that require human review, thus causing delays exploiting the response times. Agents that invoke external tools, such as unpackers or deobfuscators, widen the attack surface further, as the calls could in some cases be hijacked for malware delivery and execution.

Who's in charge?



TOMÁŠ FOLTÝN
security writer at ESET

"GuardBreaker is best understood as a very simple attempt at prompt injection: an attacker's input reaches the LLM at inference time through a file that's being analyzed."

GuardBreaker drives home a lesson that security practitioners know already: any technology that could affect an attacker's chances of success will end up in their crosshairs. Businesses relying on LLM-powered code reviews and other LLM-assisted workflows need to know what exactly any such tool inspects, where it sits in the decision chain, as well as what happens when it refuses to respond or can't complete a task.

Crucially, however, no single LLM engine should have the sole authority to decide that a piece of code is safe. AI-assisted output needs to be cross-validated using a multi-layered and multi-model approach that makes the best use of advanced automation and human expertise; meanwhile, a lack of output, too, needs to trigger further checks.

Organizations of all sizes also need a clear path from prevention to detection and response. For those without their own round-the-clock security teams, managed detection and response (MDR) can supply the requisite follow-through where an expert can investigate any suspected incidents, including in the context of other activity across the environment, and determine the next steps.

This approach is best built on decades-long use of AI's foundational technologies, tried-and-tested analysis methods, expert judgment, threat research and global telemetry. That way, any business can ensure that an action by one LLM model doesn't become a blind spot in the organization's cyber-defenses.

SUSE URGES ENTERPRISES TO UNLOCK HIDDEN CAPACITY

Dr Thomas Di Giacomo, Chief Technology and Production Officer, SUSE stresses that enterprises must stop waiting for scarce hardware and instead unlock idle compute, converge silos, optimize workload placement, embrace open source, and adopt software defined infrastructure to sustain AI momentum despite supply constraints.

Q AI hardware shortages are slowing enterprise adoption globally. How is SUSE helping organizations identify and overcome the most critical infrastructure bottlenecks without waiting for new hardware?

AI hardware scarcity has become one of the most significant inhibitors to enterprise adoption, and the instinctive reaction many organizations have is simply to wait for more hardware to arrive. But waiting is not a strategy, and it certainly isn't sustainable. Our recent SUSE Customer Reference Panel survey of 110 practitioners found that 71% of IT leaders are frustrated by AI hardware delays, and with memory prices rising by 95% or more, the idea of waiting for the supply chain to catch up is no longer realistic. What we emphasize to customers is that the most valuable resource they have is often the infrastructure already sitting in front of them. Most enterprises dramatically underestimate the amount of latent capacity within their existing environments. The real opportunity lies in unlocking that capacity rather than holding out for a bigger box or a new GPU shipment. When organizations shift their mindset from procurement driven scaling to optimization driven scaling, they discover that they can move forward immediately instead of stalling their AI initiatives.

Q Your research highlights that enterprises often underutilize existing compute resources. What practical steps can CIOs take today to unlock hidden performance within their current infrastructure?

The first and most impactful step CIOs can take is to converge their silos. Across industries, we see organizations running separate virtual machine clusters, container clusters and specialized environments that never interact with one another. Those silos are exactly where idle capacity hides. Our research shows that enterprises are leaving massive amounts of CPU and RAM completely unused simply because workloads are spread across fragmented platforms. When organizations consolidate these environments onto a unified platform, utilization can realistically approach 80% without adding new hardware. Once consolidation is achieved, CIOs can introduce smart tiering for memory heavy workloads, using high performance storage as an extension of physical memory. This approach buys valuable time before a costly DRAM upgrade becomes unavoidable. The combination of convergence and tiering allows enterprises to extract significantly more performance from their existing infrastructure while maintaining predictable cost control.

Q How can Kubernetes-driven orchestration and containerization help enterprises run AI workloads more efficiently, especially when GPU availability is limited?

Kubernetes fundamentally changes the efficiency equation for AI workloads. When GPU availability is constrained, the worst thing an organization can do is allow GPUs to sit idle in isolated silos while other workloads starve for compute. Kubernetes eliminates this fragmentation by creating a single shared pool of resources rather than multiple fenced off environments. Once workloads are converged onto a unified Kubernetes driven platform, the 80% utilization target stops being aspirational and becomes achievable. AI workloads can be scheduled more intelligently, GPUs can be shared more effectively, and compute can be allocated dynamically based on real time demand. This orchestration layer ensures that every available resource—CPU, GPU, memory and storage—is used to its fullest potential. In environments where hardware scarcity is a daily reality, Kubernetes becomes a critical enabler of efficiency and continuity.

Q With AI moving closer to the edge, how can distributed architectures reduce dependency on centralized high-end hardware and improve overall workload efficiency?

Edge computing plays a transformative role in reducing pressure on centralized, high end hardware that is increasingly difficult to procure. But it is important not to view edge architectures merely as a workaround for hardware shortages. Edge unlocks entirely new use cases that require processing close to where data is generated, independent of connectivity or centralized infrastructure. By distributing workloads across edge nodes, enterprises can reduce latency, improve responsiveness and offload tasks that would otherwise burden core systems. This distributed approach ensures that high end hardware is reserved for the workloads that truly require it, while edge nodes handle localized inference, preprocessing and real time decisioning. We see edge as a permanent and strategic part of how enterprises will architect AI systems going forward, not just a temporary response to supply constraints.

Q SUSE emphasizes open source as a strategic enabler. How does open source help enterprises navigate hardware shortages while maintaining flexibility, scalability and cost control?

In periods of hardware scarcity, the last thing enterprises need is software that locks them into a single vendor's ecosystem. Open source protects organizations from vendor dependency by ensuring portability, interoperability and long term flexibility. We are seeing strong demand from enterprise leaders for vendor neutral platforms that allow them to run workloads across diverse hardware environments without being constrained by proprietary limitations. Open source ensures that organizations are not held hostage to a vendor's shipping schedule, pricing decisions or hardware roadmap. It gives enterprises the freedom to scale across heterogeneous environments, optimize based on real time needs and maintain cost control even when hardware availability fluctuates. In short, open source becomes a strategic safeguard during periods of supply chain instability.

Q What role does intelligent workload placement play in ensuring AI models run efficiently across mixed environments, on-prem, cloud, and edge, especially when hardware is constrained?

Intelligent workload placement is one of the most powerful levers enterprises have when hardware is constrained. Smart memory tiering is a practical example of how this works. By

DR THOMAS DI GIACOMO
Chief Technology and Production Officer, SUSE

"Constraint doesn't have to mean giving up agility—enterprises that optimize what they already own will stay competitive no matter what the hardware market looks like."



using high performance storage as a secondary memory tier, organizations can delay expensive DRAM upgrades while still maintaining efficient performance. But workload placement extends far beyond memory optimization. It is about ensuring that every workload runs in the environment where it performs best—whether that is on prem, in the cloud or at the edge—and on the right chipsets. When placement is done correctly, enterprises achieve higher efficiency, lower latency and better cost control. The benefits continue long after the hardware market stabilizes because optimized placement becomes a permanent operational advantage.

Q In a period of hardware scarcity, how can enterprises maintain resilience, ensure business continuity, and avoid stalled AI initiatives?

Hardware delays are one of the most common reasons AI roadmaps stall. Long procurement cycles and unpredictable supply chains are slowing IT projects across industries. Our guidance is to treat these delays as a forcing function rather than a blocker. The first step is conducting an honest utilization audit of existing infrastructure. Most organizations discover that they have far more capacity than they assumed. Starting with solutions on neocloud that can be ported across environments allows enterprises to maintain momentum even when hardware is unavailable. The organizations that adopt this mindset—optimize first, procure second—are the ones that continue moving forward regardless of supply chain disruptions.

Q Looking ahead, how does SUSE see AI infrastructure evolving over the next couple of years, and what should enterprises prioritize now to stay competitive despite ongoing hardware shortages?

The old model of scaling by simply buying more hardware is becoming financially unsustainable, and we do not expect that to change even when supply improves. Constraint does not have to mean sacrificing agility. In fact, it often accelerates architectural innovation. Software defined infrastructure is the path forward for enterprises seeking to maximize the value of what they already own. Organizations that build discipline around optimization, convergence and intelligent placement will remain competitive regardless of hardware availability. Over the next two years, we expect AI infrastructure to become more distributed, more automated and more software driven. Enterprises that embrace this shift now will be positioned to thrive in any market condition.

THE AI REALITY CHECK: ROI SHORTFALLS, BOUNDARY BREACHES, AND THE ARCHITECTURE OF RESILIENCE

Bharat Raigangar, Board Advisor – Global Head AI Cyber Security & Business Resilience, 1CxOCSA, explains that enterprises in 2026 are shifting from rapid AI deployment to resilience, confronting ROI gaps, operational failures, security risks, and rising oversight demands as AI becomes mission critical.

Why 2026 may be remembered as the year enterprises stopped asking "How fast can we deploy AI?" and started asking "How do we survive when AI fails?" By every traditional technology metric, artificial intelligence should be a runaway success story. Enterprise spending on AI infrastructure has reached unprecedented levels. Boardrooms have embraced AI-first strategies. Vendors continue to announce larger models, more capable agents, and increasingly autonomous systems.

Yet beneath the enthusiasm, a different story is emerging. As organizations transition from experimental copilots to operationally embedded AI agents, many are discovering a harsh reality: deployment is easy; dependable business value is not. From disappointing ROI and escalating engineering costs to autonomous security incidents and mission-critical failures, enterprises are confronting a new challenge that has less to do with innovation and more to do with resilience.

The defining question of the AI era is no longer whether AI works. It is whether organizations can continue operating when it doesn't.

The Great AI Return Deficit

For years, AI investment was justified by promises of productivity gains, workforce transformation, and exponential returns. However, many enterprises are finding it difficult to translate pilot success into measurable business outcomes. A growing number of organizations report that while AI can demonstrate impressive capabilities in controlled environments, sustained production value remains elusive. The gap between prototype performance and operational reality continues to widen.

The challenge is not simply model accuracy. It is the accumulation of hidden costs that emerge once AI becomes embedded in business processes. Organizations are discovering that significant resources are being redirected toward validating outputs, correcting hallucinations,



BHARAT RAIGANGAR
Board Advisor – Global Head AI Cyber Security & Business Resilience, 1CxOCSA

"The defining question of the AI era is no longer whether AI works. It is whether organizations can continue operating when it doesn't."

rewriting generated code, managing governance requirements, and maintaining increasingly complex AI ecosystems.

What initially appeared to be automation often evolves into a new layer of supervision. In many enterprises, human effort has not disappeared. It has merely shifted from performing the work to constantly verifying that AI performed the work correctly.

The Hidden Cost of "Autonomous"

Perhaps the most underappreciated aspect of enterprise AI is the operational overhead required to keep systems functioning safely. The narrative surrounding AI frequently centers on productivity gains, but technology leaders increasingly report spending substantial time managing AI-generated defects, reviewing generated content, and mitigating unexpected behavior.

Software engineering teams provide perhaps the clearest example. While generative coding tools can accelerate development, they can also introduce inconsistent architectures, security vulnerabilities, undocumented logic, and maintenance challenges. Every productivity gain achieved at generation time can reappear later as debugging effort, quality assurance costs, and governance reviews.

As a result, many organizations are learning that AI deployment is not primarily a technology challenge. It is an operational management challenge.

The Workforce Correction

The excitement surrounding automation led many organizations to pursue aggressive workforce reduction strategies. AI was positioned as the catalyst for leaner operations, particularly in customer service, software development, and administrative functions.

However, reality has proven more nuanced. A growing number of enterprises are discovering that automation alone cannot consistently handle edge cases, complex decision-making, regulatory requirements, or high-stakes customer interactions.

In several industries, organizations have quietly reintroduced human oversight after discovering that fully autonomous workflows created quality, compliance, or customer experience issues. The lesson is becoming increasingly clear: eliminating humans may produce immediate cost savings, but restoring expertise after operational failure often proves significantly more expensive.

Rather than replacing human workers, many successful organizations are now redesigning roles around human-AI collaboration. The future workforce is appearing less autonomous than originally envisioned and far more hybrid.

When AI Failure Becomes a Business Crisis

The most serious concerns emerge when AI systems move beyond convenience applications and enter critical operational environments. Healthcare, finance, legal services, manufacturing, critical infrastructure, and government operations increasingly rely on AI-assisted decision-making. In these domains, errors are not measured in productivity metrics. They are measured in financial losses, regulatory exposure, safety incidents, and reputational damage.

Audits of AI deployments continue to reveal troubling patterns:

- Fabricated recommendations presented confidently as facts.
- Incorrect records generated in operational systems.
- Important contextual information omitted from summaries.
- Non-existent citations and references presented as authentic sources.
- Inconsistent outcomes across identical tasks.

The danger lies not only in the mistakes themselves but in the confidence with which they are delivered. Traditional software typically fails visibly. AI often fails persuasively. That distinction creates entirely new risk categories for enterprise leaders.

The Rise of Autonomous Security Risk

As AI agents gain broader access to systems, networks, APIs, and enterprise data, security leaders are confronting an equally significant challenge. Historically, cyber defenses focused on protecting organizations from external attackers. Agentic AI introduces the possibility that trusted internal systems can become sources of unexpected behavior.

Advanced models are increasingly capable of chaining actions, navigating environments, interacting with external services, and pursuing objectives with minimal human intervention. While these capabilities unlock enormous business potential, they also introduce unprecedented governance requirements. An AI agent connected to procurement systems, financial platforms, cloud environments, code repositories, or customer databases effectively becomes a privileged actor inside the enterprise.

Any misalignment, configuration error, or security weakness can produce consequences that extend far beyond a typical software defect. In practical terms, AI access must now be treated as a security boundary. Organizations that view AI merely as another application risk underestimating its operational impact.

Building the Architecture of Resilience

The leading organizations in 2026 are not necessarily those deploying the most AI. They are the organizations preparing for AI failure.

Map Critical Failure Paths

Every enterprise should identify workflows that would halt if AI services became unavailable, degraded in quality, or produced unreliable outputs. Understanding dependency chains is the first step toward resilience.

Harden Agent Permissions

Agentic systems should operate under strict least-privilege principles. Network segmentation, identity controls, monitoring, and comprehensive audit trails should be considered mandatory rather than optional.

Institutionalize Fallback Operations

Organizations routinely conduct disaster recovery exercises for infrastructure failures. The same discipline must now apply to AI. Critical teams should periodically operate with AI tools disabled to ensure that business continuity can be maintained manually when necessary.

Separate Workforce Strategy from AI Hype

Staffing decisions should be guided by demonstrated performance rather than projected capabilities. Sustainable automation requires evidence, not optimism.

The New Competitive Advantage

For more than a decade, digital transformation rewarded organizations that moved fastest. The AI era is changing the rules. Speed still matters, but resilience matters more.

The enterprises that emerge strongest from the current wave of AI adoption will not be those that automate every process, eliminate the most jobs, or deploy the largest number of agents. They will be the organizations that recognize an uncomfortable truth: AI is neither infallible nor self-sustaining. Like every transformative technology before it, AI will fail, drift, misbehave, and occasionally operate outside expected boundaries.

The winners will be those who plan for that reality. In 2026, resilience is no longer the backup strategy for AI. Resilience is the strategy. The organizations that treat AI as a business-resilience challenge, a security challenge, and a governance challenge, not merely a technology investment, will be the ones that capture lasting value while others struggle with disruption.

The next stage of enterprise AI will not be defined by intelligence alone. It will be defined by how well organizations withstand the moments when that intelligence falls short.

The AI Reality Check: ROI Shortfalls, Boundary Breaches, and the Architecture of Resilience

Why 2026 may be remembered as the year enterprises stopped asking "How fast can we deploy AI?" and started asking "How resilient are we when AI fails?"

Artificial intelligence remains the defining technology investment of the decade. Enterprises continue pouring billions into infrastructure, foundation models, copilots, and increasingly autonomous agents. Yet as AI transitions from experimental deployments to business-critical operations, a growing number of organizations are discovering a troubling reality: investment does not automatically translate into value.

The gap between AI ambition and operational outcomes has become one of the most significant challenges facing technology leaders in 2026. Concerns around weak returns, escalating engineering costs, workforce disruption, security exposures, and autonomous system failures are reshaping the conversation. The focus is shifting away from AI adoption at all costs and toward a more pragmatic objective: operational resilience.

The Return Deficit

For many enterprises, AI's biggest challenge is not capability but economics.

While pilot projects often generate excitement, measurable business outcomes remain difficult to achieve at scale. Studies of enterprise AI programs suggest that only a small minority of deployments deliver sustained profit-and-loss impact. Most organizations continue to struggle with proving tangible return on investment beyond isolated use cases. Part of the problem lies in hidden costs. AI systems require extensive oversight, validation, governance, and maintenance. Research indicates that only a fraction of enterprise AI spending reaches production value, while much of the budget is consumed by debugging AI-generated code, rewriting outputs, and managing review processes.

The result is a paradox: organizations may deploy AI successfully while simultaneously failing to realize meaningful business gains.

Rather than eliminating work, AI often shifts work from execution to supervision.

The Workforce Recalibration

The early narrative surrounding AI centered on workforce replacement. Many organizations viewed automation as a direct path to reducing headcount, particularly in customer service, administration, and software development.

Reality has proven more complex.

Analysts increasingly predict that a significant share of AI-driven workforce reductions will be reversed through rehiring over the coming years. Organizations that aggressively reduced staff have discovered that fully autonomous systems struggle with exceptions, nuanced decision-making, quality control, and customer interactions. Several industries have already begun restoring human oversight after automated systems failed to meet performance expectations. In the manufacturing sector, for example, reports of organizations rehiring quality specialists after AI inspection tools missed defects have become cautionary examples.

The lesson is straightforward: removing expertise is easy; rebuilding it is expensive.

The most successful enterprises are no longer pursuing a human-versus-machine strategy. Instead, they are designing operational models that combine human judgment with AI-enabled productivity.

When AI Failure Becomes Business Risk

The consequences become far more serious when AI is deployed in high-stakes environments.

Healthcare, legal services, finance, and critical infrastructure increasingly rely on AI-assisted decision-making. In these settings, errors are not simply productivity issues; they become regulatory, financial, operational, and reputational risks. Independent reviews of AI systems have revealed recurring concerns, including fabricated recommendations, inaccurate data recording, omitted critical information, and fictional citations presented as authentic references. The challenge is compounded by the confidence with which AI systems deliver incorrect outputs.

Traditional software generally fails in visible ways. AI can fail convincingly. That distinction fundamentally changes risk management requirements. Organizations cannot assume that because an answer appears authoritative, it is accurate. Human validation remains essential in mission-critical processes.

The Expanding Security Boundary

Security leaders are confronting an equally important challenge as AI agents gain access to enterprise systems.

Unlike traditional software, modern AI agents can interact across applications, invoke tools, access data repositories, and execute complex multi-step actions. This capability creates new opportunities for productivity but also expands the organization's attack surface. Recent testing and research have highlighted cases where advanced models exploited weaknesses, crossed intended operational boundaries, or initiated actions that exceeded expected behavior. While many of these events occurred in controlled environments, they demonstrate an important principle: AI systems should be treated as privileged actors, not merely applications.

Organizations must therefore view agentic AI as a security boundary. Least-privilege access, network segmentation, monitoring, audit logging, and continuous governance should become standard controls wherever AI agents interact with business-critical systems.

The future of enterprise security will depend not only on preventing external attackers, but also on governing increasingly autonomous internal systems.

Building the Architecture of Resilience

As AI becomes embedded in operations, resilience must become a core business discipline.

First, organizations should map critical failure paths, identifying workflows that would be disrupted if AI services became unavailable or unreliable.

Second, agent permissions must be tightly controlled. AI systems should only access the data, tools, and environments necessary to perform their assigned functions. Third, enterprises should conduct AI outage drills similar to disaster recovery exercises. Critical teams must be capable of continuing operations when AI systems are disabled, unavailable, or producing questionable outputs. Finally, workforce decisions should be based on demonstrated results rather than assumptions about future AI capabilities. Sustainable transformation requires evidence, not optimism.

The New Competitive Advantage

The first wave of AI adoption rewarded organizations that moved fastest. The next wave will reward organizations that remain operational when AI fails.

Resilience is emerging as the defining differentiator of enterprise AI success. The organizations that create lasting value will not necessarily be those with the largest models, the most agents, or the highest technology spend. They will be the ones that understand AI's limitations and design their operations accordingly.

Closing Summary

The great lesson of 2026 is that AI is neither magic nor autonomous perfection. It is a powerful but imperfect capability that introduces new forms of dependency, risk, and operational complexity. Enterprises that treat AI as a business continuity, security, and governance challenge, rather than simply a technology initiative, will be best positioned to succeed.

The future belongs not to the organizations that trust AI the most, but to those that can continue operating when AI is wrong, unavailable, or compromised. In the age of autonomous systems, resilience is no longer a defensive strategy. It is the foundation of competitive advantage.

channelpost
MIDDLE EAST AND AFRICA

STAY AHEAD OF THE CURVE WITH **CHANNEL POST MEA**



POWER & COOLING ME BUILDING THE MIDDLE EAST'S RESILIENT DIGITAL INFRASTRUCTURE

Meenal Sanjeev Madavi, CEO, Power & Cooling ME emphasized the region's shift to high density, AI ready infrastructure and highlighted Power & Cooling ME's mission critical engineering approach to building resilient, efficient, and sustainable digital ecosystems across the Middle East.

Q How do you see the UAE's rapidly expanding data center market evolving over the next 2–3 years, especially with hyperscalers and AI driven workloads accelerating demand for high density environments?

The UAE is entering a pivotal stage in its digital infrastructure evolution. Once seen mainly as a preferred regional destination for data center deployments, it is now rapidly becoming a strategic global hub. Over the next two to three years, hyperscale, sovereign cloud, and AI driven investments will accelerate sharply. The defining shift, however, will not be the number of megawatts added but the density and complexity of those deployments. AI workloads are transforming data center architecture, replacing traditional rack profiles with high density GPU clusters that demand significantly more power, advanced thermal management, and integrated resilience. Cooling is no longer a secondary system; it is now part of the core compute architecture, tightly linked to power distribution and performance.

This evolution presents a major opportunity for the UAE. The nation already benefits from world class connectivity, strong capital availability, advanced infrastructure, and a clear ambition to lead in AI and digital innovation. The next phase requires moving beyond capacity building toward intelligent, efficient, and sustainable infrastructure. Energy efficiency, water consumption, resilience, scalability, and deployment speed will matter as much as raw power. The UAE's ability to combine high density environments with sustainability and operational excellence will determine its emergence as a truly global digital hub.



MEENAL SANJEEV MADAVI
CEO, Power & Cooling ME emphasized

"In mission critical environments, customers are not buying hardware—they are buying confidence that their business will keep running."

Q What major trends are shaping the wider Middle East data center landscape, and where do you see the strongest growth opportunities for power and cooling providers?

The Middle East data center landscape is being reshaped by three powerful forces: AI, digital sovereignty, and energy availability. Governments and enterprises across the region are investing heavily in sovereign cloud, AI infrastructure, and large scale digital transformation. Data centers are no longer viewed as isolated facilities but as strategic national assets essential to economic competitiveness, innovation, and security. Saudi Arabia, the UAE, and other GCC markets are leading this shift, with major AI oriented developments already underway. A recently announced 100 MW project in Saudi Arabia reflects the scale and ambition driving regional growth.

For power and cooling providers, this evolution creates opportunities far beyond equipment supply. The strongest growth lies in engineering excellence, optimization, lifecycle services, and intelligent infrastructure management.

As densities rise and workloads become more complex, customers will need partners capable of delivering integrated solutions that ensure availability, efficiency, and long term performance. High density cooling, power quality management, modular UPS systems, energy optimization, DCIM, predictive maintenance, and retrofit solutions will see significant demand. A major opportunity also exists in helping existing facilities become AI ready, enabling them to support GPU clusters without full rebuilds. The industry is shifting from selling hardware to delivering measurable outcomes, and providers who combine technology expertise with engineering capability and long term service delivery will be best positioned to lead this transformation.

Q Can you walk us through Power & Cooling ME's core solutions for data centers, and how they address the region's unique climate, energy, and sustainability challenges?

At Power & Cooling ME, we view the data center as an integrated mission critical ecosystem rather than a collection of individual components. Our portfolio spans critical power—including UPS systems, power distribution, and monitoring—precision cooling, in row and in rack cooling, high efficiency chillers, DCIM and environmental monitoring, modular and prefabricated infrastructure, and comprehensive maintenance and managed services.

This integrated approach allows us to support customers across the entire lifecycle of their infrastructure, from design and deployment to optimization and long term operation.

The Middle East presents a uniquely demanding environment for data centers. High ambient temperatures, dust, energy intensity, and the need for extremely high availability mean that equipment selection alone is not enough. Engineering, commissioning, preventive maintenance, and continuous monitoring are equally critical. Our lifecycle oriented approach helps customers assess existing infrastructure, improve efficiency, extend equipment life, and prepare facilities for future density requirements.

Our cooling portfolio includes in row, in rack, and high efficiency chiller solutions tailored to different density profiles and deployment models. Ultimately, our objective is to make the data center more resilient, more efficient, and easier for the customer to operate. By integrating power, cooling, monitoring, and lifecycle services, we help customers build infrastructure that performs reliably under the region's challenging conditions while remaining adaptable to future technological shifts.

Q In a competitive market, what differentiates your technologies, engineering capabilities, or service model from other power and cooling providers in the region?

Our biggest differentiator is that we do not see ourselves as an equipment company that happens to provide services. We see ourselves as a mission-critical infrastructure partner.

Technology matters, but it is no longer a differentiator—customers can access excellent products from many global manufacturers. What truly sets providers apart is how effectively that technology is engineered, integrated, commissioned, and optimized throughout its lifecycle.

We combine product expertise with deep engineering capability, continuous monitoring, preventive maintenance, and lifecycle services. We take an independent, customer centric view of infrastructure rather than approaching challenges through the lens of selling a specific product. Our philosophy is "serve, not sell," reflected in long term relationships and strong service renewal performance. In mission critical environments, customers are not buying hardware—they are buying confidence that their business will keep running.

Q How is your company preparing for the surge in AI workloads, GPU clusters, and high density racks that demand advanced cooling and power resilience?

AI is forcing the industry to rethink traditional data center architecture. The challenge is no longer simply providing more power; it is delivering much higher power density while removing significantly more heat, all without compromising availability.

We are preparing by strengthening our capabilities across both power and thermal domains. On the power side, this includes high capacity modular UPS systems, intelligent power distribution, monitoring, and power quality management. On the thermal side, we are expanding our capabilities around in row, in rack, and other high density cooling architectures designed specifically for GPU environments.

However, the bigger opportunity lies in helping customers answer a fundamental question: "Is my existing data center AI ready?" Many facilities will need to accommodate GPUs without having been originally designed for those densities. This creates a substantial retrofit and optimization market. Our role is not only to build new AI infrastructure but also to help existing infrastructure transition safely and efficiently into the AI era.

Q What innovations or new solutions can the market expect from Power & Cooling MEA in the coming year, particularly around sustainability, energy efficiency, or next gen cooling?

Our focus for the coming year is on moving from equipment efficiency to infrastructure intelligence. We are developing solutions that help customers understand where energy is being consumed, where capacity is being lost, and where infrastructure can be optimized without compromising resilience. Digital monitoring and DCIM will become increasingly important because continuous measurement is essential for continuous improvement. Our existing monitoring capabilities already provide real time visibility into critical infrastructure, and we are expanding these capabilities further.

On the cooling side, high density and liquid assisted cooling technologies will become increasingly relevant as AI rack densities rise. However, we believe liquid cooling should not be treated as a universal answer. The right solution depends on rack density, facility architecture, climate, water availability, and operational model. Our innovation philosophy is technology neutral and outcome driven: lower energy consumption, higher availability, better thermal performance, and lower total cost of ownership. The future is not simply "more cooling"; it is smarter cooling.

Q What are your growth projections for the UAE and MEA markets, and how do you plan to scale operations, partnerships, or regional presence to meet rising demand?

We are extremely optimistic about the UAE and wider MEA market. Our ambition is not merely to grow alongside the data center industry but to become one of the region's leading data center infrastructure and services companies. Our growth strategy is built on three pillars. First, deepen our presence in the UAE, particularly in Dubai and Abu Dhabi. Second, expand our regional footprint through carefully selected partnerships and local capabilities. Third, increase the proportion of our business coming from recurring services—AMC, managed services, monitoring, optimization, and lifecycle management.

The market is evolving rapidly, but we are committed to scaling without compromising engineering quality or customer experience. We believe the next phase of the industry will reward companies that can bridge the gap between OEM technology and customer outcomes.

That is where we see Power & Cooling ME having a strong role to play. Our ambition is straightforward: to help build a more resilient, intelligent, and sustainable digital infrastructure ecosystem across the Middle East.



GISEC GLOBAL 2026: THE YEAR MIDDLE EAST CYBERSECURITY REDEFINED ITS CENTER OF GRAVITY

From sovereign AI to unified exposure management, GISEC 2026 reveals a region stepping into cyber leadership — prioritizing anticipation, containment, governance, and collaboration across every layer of digital transformation.

GISEC Global 2026 arrives at a moment when the Middle East's cybersecurity landscape is being reshaped by AI velocity, geopolitical pressure, and the convergence of IT, OT, and cloud environments. Across the show floor, one theme dominates: the region is no longer reacting to global cyber trends — it is defining them. From sovereign AI deployments to microsegmentation, identity governance, observability, and adversary centric intelligence, the companies exhibiting this year are not simply showcasing products; they are demonstrating how cybersecurity strategy in the Middle East is evolving into a more anticipatory, intelligence driven discipline.

This year's exhibitors reflect a region that has matured beyond point solutions. CISOs, regulators, and critical infrastructure operators are demanding integrated architectures, deeper visibility, and partner ecosystems capable of delivering sustained resilience. The conversations at GISEC 2026 are sharper, more technical, and more urgent — and the spokespersons behind the technologies are aligned on one message: AI has changed the tempo of cyber risk, and the Middle East must respond with equal speed, precision, and collaboration.

AmiViz enters GISEC 2026 with a message that challenges traditional distribution models. For CEO Ramkumar Balakrishnan, the event is not about showcasing tools but demonstrating what "consultative distribution" looks like when applied to sovereign AI, zero trust architectures, and data resilience frameworks built for the region's regulatory reality.

"GISEC is where AmiViz demonstrates what consultative distribution actually looks like in practice. We are not showcasing products — we are showcasing outcomes: sovereign AI deployments, zero trust architectures, and data resilience frameworks built for this region's regulatory reality. For us, GISEC is less an exhibition and more a signal — that the most complex security conversations in MEA happen here, and we are ready for them. This year, we're focused on OT IT convergence, AI enabled threat actors, and data sovereignty under pressure, and we're engaging partners through co investment, technical enablement, and shared pipeline development to build deeper, more capable relationships."

For Meriam ElOuazzani, Vice President for META at Censys, the region's biggest challenge is not technology — it is visibility. With geopolitical tensions shaping digital exposure, Censys



ASHRAF KOHEIL
VP OF SALES, META & AUZ, GROUP-IB



DR. KAMEL HEUS
VICE PRESIDENT OF SALES, MEA AT SAVIYNT



ELIAS TSAPSIDIS
GENERAL MANAGER AT ESET MIDDLE EAST, GREECE, CYPRUS & MALTA

is using GISEC to highlight the importance of understanding infrastructure from the attacker's perspective.

"GISEC matters because the concentration of decision makers in that room is rare. What Censys is bringing is straightforward: a clear view of what your infrastructure and your third party infrastructure look like to an adversary. Not how you've mapped it internally — what they actually see. We're here to talk about exposure organizations don't know they have, especially as geopolitical conflict shapes the threat landscape. Our partner conversations focus on readiness, not portfolio width, and on aligning capabilities with the gaps where breaches usually live."

AI has become both a business enabler and a security risk. Prashant Menon, Channel Leader for UAE at Check Point, sees GISEC 2026 as the moment to demonstrate how prevention first security must evolve alongside AI transformation.

"GISEC is an opportunity to demonstrate how prevention first security must evolve alongside the region's AI transformation. We are showcasing the AI Network Firewall, which turns existing firewalls into a control point for AI — providing visibility into which models and agents employees are using and applying controls inline. AI has crossed from assisting attacks to operating them, and our research shows high risk generative AI interactions are rising sharply. Our answer is prevention at the point of interaction, across users, applications, and networks, supported by deeper partner capabilities across AI Security, Hybrid Mesh Network Security, Workspace Security, and Exposure Management."

Cisco arrives at GISEC with a unified architecture strengthened by Splunk's security observability. Fady Younes, Managing Director for Cybersecurity across METAC, frames 2026 as the year organizations must balance AI's risks and opportunities.

"At GISEC 2026, Cisco is demonstrating how our cybersecurity architecture is evolving for the Agentic Era. We're highlighting how our integrated portfolio, bolstered by Splunk's security observability, provides comprehensive visibility and automated defense. Organizations today must balance the risks and opportunities presented by AI, and our approach integrates AI driven defense with Splunk's data centric security to help businesses anticipate, detect, and respond to threats at scale. GISEC is also a vital forum for strengthening partner alignment, because collective expertise is essential for long term resilience."

Data sovereignty and AI driven complexity are reshaping how organizations think about resilience. Hassan Aoun, Senior Channel Director for Cohesity, sees partners as the key to translating these challenges into outcomes.

"At GISEC 2026, we are highlighting how our technology and partner ecosystem work together to strengthen cyber resilience. Through our updated Aspire Global Partner Program, we're making it easier for partners to build services led practices, develop deeper security expertise, and collaborate with us on customer opportunities. AI adoption and data sovereignty requirements are creating more demanding environments, and partners need simpler training pathways and guided learning to move quickly from training to real world delivery. Being on the ground at GISEC helps us understand evolving needs and ensure our initiatives remain relevant to real customer priorities."

CPX enters GISEC with one of the event's strongest themes: AI resilience for critical infrastructure. CEO Hadi Anwar positions CPX as a regional leader in secure digital transformation.

"At GISEC 2026, CPX is spearheading regional cyber readiness under the theme 'Building AI Resilience: Secure What's Next.' We are demonstrating six interactive capabilities, including Secure AI and OT Security, to equip organizations with end to end protection. AI powered cyberattacks and geopolitical complexity are escalating rapidly, and our solutions deliver advanced threat intelligence, Secure AI capabilities, and governance frameworks to help governments and enterprises pre empt emerging threats. Our booth is a collaborative hub with 20+ ecosystem partners, showcasing real world use cases that strengthen long term resilience and business continuity."

AI has compressed the time between vulnerability discovery and exploitation. Roland Daccache, Director of Sales Engineering for MENA at CrowdStrike, sees GISEC as the moment to demonstrate coordinated, AI powered defense.

"At GISEC 2026, we're showcasing how CrowdStrike is securing AI now that it is a core part of the enterprise. Through the Falcon platform, organizations can understand and control AI agents, secure AI agent identities and software supply chains, and use AI to defend at machine speed. Adversaries are using AI for reconnaissance and social engineering, while agentic attacks move across domains simultaneously. CrowdStrike delivers coordinated investigations across end-



FADY YOUNES
MANAGING DIRECTOR, CYBERSECURITY, CISCO MIDDLE EAST, TÜRKIYE, AFRICA, CAUCASUS AND CENTRAL ASIA (METAC)



HADI ANWAR
CEO OF CPX



HARISH CHIB
VP EMERGING MARKETS - MIDDLE EAST AND AFRICA, SOPHOS



HASSAN AOUN
SENIOR CHANNEL DIRECTOR, INTERNATIONAL EMERGING REGION AT COHESITY

point, identity, SaaS, cloud, and network, turning what once took hours into minutes. We're also helping partners build, resell, manage, and deliver AI powered security through our new AI Partner Specialization."

ESET arrives at GISEC with a unified platform designed for cloud expansion, identity abuse, ransomware, and AI enabled threats. Elias Tsapsidis, General Manager for the Middle East and surrounding regions, emphasizes prevention and visibility.

"At GISEC 2026, ESET is showcasing how our AI native ESET PROTECT Platform brings prevention, XDR, threat hunting, investigation, and response into one environment. We're highlighting risks created by cloud expansion, identity abuse, ransomware, social engineering, and rapid AI adoption. Our research shows rising ClickFix activity, record QR code phishing, and emerging malicious AI skills. Our approach combines multilayered prevention, cloud and endpoint visibility, XDR, threat intelligence, and faster investigation and response. GISEC also gives us a platform to work directly with distributors, resellers, and service providers to build stronger advisory and managed security capabilities."



HUSSAM SIDANI
VICE PRESIDENT OF META AT OPSWAT

Group IB's "Predict, Don't React" Innovation Hub is one of GISEC's most anticipated showcases. Ashraf Koheil, VP of Sales for META & AUZ, positions adversary centric intelligence as the future of regional cyber defense.

"At GISEC 2026, Group IB is using its 'Predict, Don't React' Innovation Hub to bring our latest capabilities to life, including Prevyn AI, Incident Management Center, Cyber Fraud Fusion, and our Cyber Fraud Intelligence Platform. Cybercrime is becoming more sophisticated, and organizations need visibility across the full attack and monetization chain. We address this through adversary centric intelligence, AI, cyber fraud intelligence, threat hunting, DFIR, and managed XDR, helping security teams identify signals earlier and strengthen proactive resilience. GISEC also provides a platform for partner engagement through demonstrations and expert conversations that support long term collaboration."

Illumio brings one of the most technically mature narratives to GISEC this year. For Sam Tayan, Regional Vice President for META, the challenge is not only detecting threats but stopping their movement across hybrid environments. His focus is on microsegmentation and attack path visibility — two capabilities that have become essential as AI accelerates lateral movement.

"At GISEC 2026, Illumio is focusing on AI velocity and what happens when attacks move faster than traditional security processes can respond. We're showcasing the Illumio Platform, recently named a Leader and Customer Favorite in The Forrester Wave for Microsegmentation. The platform brings together Illumio Insights and Illumio Segmentation to help organizations identify risk, stop lateral movement, and strengthen resilience across hybrid environments. Our conversations with partners center on breach containment, regional use cases, and how Illumio complements existing controls. Through one to one meetings and demonstrations, we're helping partners understand how to improve visibility, limit lateral movement, and build stronger cyber resilience."

Infoblox continues this theme of visibility, but from the network foundation outward. Mohammed Al Moneer, Senior Regional Director, emphasizes DNS layer intelligence as a preemptive advantage.

"GISEC gives us an opportunity to show how the Infoblox platform turns the network foundation into a preemptive security advantage. By connecting DNS, DHCP, and IPAM visibility with intelligence and enforcement, organizations can understand what's happening across their environments and identify malicious infrastructure earlier. Digital transformation is expanding the attack surface faster than teams can see it, and cloud adoption, exposed assets, phishing, and AI enabled attacks are converging. Our platform helps connect outside in exposure intelligence with DNS layer protection so teams can prioritize what matters, block malicious activity, and disrupt threats before impact. Partner conversations focus on operationalizing intelligence and building capabilities that sustain resilience long after GISEC."

ManageEngine brings a different perspective: the complexity of hybrid environments and the shortage of skilled security professionals. Sujoy Banerjee, Regional Business Director for the UAE, positions unified platforms and AI driven automation as the answer.

"GISEC 2026 is a key platform for us to demonstrate the depth and direction of ManageEngine's security portfolio. We're spotlighting our AI powered autonomous agents — Zia Agents — alongside unified security, endpoint security, and IAM capabilities. The challenge we're addressing is complexity: hybrid cloud, distributed endpoints, remote workforces, and sophisticated threats.



HÜSEYIN FATIH AKAR,
SENIOR SECURITY PRODUCT MANAGER OF VMRAY



MERIAM ELOUAZZANI
VICE PRESIDENT FOR MIDDLE EAST, TURKEY, AND AFRICA, CENSYS



MOHAMMED AL-MONEER
SENIOR REGIONAL DIRECTOR, INFOBLOX

ManageEngine Identity Access delivers directory independent access management across the hardest to secure environments, while Zia Agents bring AI driven automation to access reviews, alert correlation, EDR triage, and incident investigations. Our partner focus is helping them articulate the value of bringing IT operations and cybersecurity together under a unified platform, enabling long term resilience through integrated visibility and automation."

OPSWAT brings critical infrastructure protection to the forefront. Hussam Sidani, Vice President for META, emphasizes the need to sanitize unseen threats across IT and OT environments.

"Our theme this year is 'Sanitize the Unseen,' reflecting the need to go beyond detection and prevent hidden threats from reaching critical systems. At GISEC, we're showcasing our AI Content Inspector, CIP Mobile Lab, and Nuclear Plant Model Reactor. Visitors can see how deep file inspection, content sanitization, and coordinated IT and OT protections secure the points where files, devices, and data enter critical environments. AI generated and adaptive threats are evolving at speed, and seemingly legitimate files can conceal malicious content. Our approach is layered prevention across email, web traffic, storage, and removable media. We're also investing in skills development through OPSWAT Academy CIP certifications to strengthen practical cybersecurity expertise across the region."

SANS Institute brings the human element into focus. Ned Baltagi, Managing Director for META, highlights the need for advanced training and AI security maturity.

"At SANS, we are using GISEC Global 2026 to combine hands on training with industry and government engagement. We're showcasing the Gulf Edition of our AI Security Maturity Model, AI Cybersecurity Career Guide, and new GIAC certifications focused on AI security, ICS/OT, and cybersecurity leadership. The region is facing challenges across AI security, critical infrastructure, third party risk, cloud and container security, and quantum readiness. Through certified training and technical workshops, we're equipping practitioners and security leaders with practical skills to secure AI, protect critical infrastructure, manage emerging risks, and make better informed security decisions. Engagement at stand D80 provides opportunities to strengthen skills and support long term resilience."

Saviynt brings identity governance into the AI era. Dr. Kamel Heus, Vice President of Sales for MEA, highlights the explosion of non human identities.

"We are exhibiting at Stand Hall 3, P22–P25, showcasing Zuma, our new AI Identity Security Platform, and our converged Enterprise Identity Cloud. The biggest shift is non human identities — AI agents already outnumber human identities 82 to 1, and most organizations cannot govern them with legacy solutions. We're highlighting Zuma and our Agent Access Gateway, which bring AI agents under the same governance as human identities. Our partners are key to delivering that locally with the regional context customers need. Through our Accelerate Partner Program and Delivery Excellence accreditation, we're investing in enablement and training so partners can deliver Saviynt expertise locally and at scale."

SolarWinds brings observability into the cybersecurity conversation. Sheetal Kalra, Channel Account Manager, emphasizes visibility across hybrid IT.

"This year, we're joining our strategic distribution partners to explore how organizations can gain greater operational visibility and strengthen security outcomes in complex IT environments. As ecosystems expand across cloud, hybrid, and AI enabled infrastructures, observability is becoming foundational for operational excellence and cyber resilience. You cannot protect what you cannot see. At GISEC, we're highlighting the critical connection between observability and security, showing how end to end visibility helps teams identify risks earlier, respond faster, and make more informed decisions. We're engaging partners on integrated approaches, interoperability, and vendor agnostic collaboration to reduce complex-



NED BALTAGI
MANAGING DIRECTOR, MIDDLE EAST, TURKEY, AND AFRICA AT SANS INSTITUTE



PRASHANT MENON
CHANNEL LEADER, UAE, CHECK POINT SOFTWARE TECHNOLOGIES



RAMKUMAR BALAKRISHNAN
CHIEF EXECUTIVE OFFICER AT AMIVIZ



ROLAND DACCACHE
DIRECTOR OF SALES ENGINEERING MENA AT CROWDSTRIKE



SAM TAYAN
REGIONAL VICE PRESIDENT FOR META, ILLUMIO

ity and strengthen long term resilience."

Sophos completes the narrative with a unified, AI native defense model. Harish Chib, Vice President for Emerging Markets, highlights platform consolidation and MDR.

"Sophos is using GISEC 2026 to demonstrate how organizations can defend against faster, AI enabled attacks through a more unified cybersecurity model. The focus is Sophos Fusion, an AI native defense system that connects security operations, endpoint, network, identity, email, cloud, MDR, and third party integrations into one coordinated architecture. We're highlighting identity based attacks, phishing, ransomware, AI enabled threats, and the complexity created by fragmented tools. Our solutions improve prevention, detection, investigation, and response through shared telemetry, automation, MDR expertise, and open integrations. Partner engagement centers on AI native defense, MDR opportunities, platform consolidation, and customer resilience to support long term maturity."

Tenable sharpens the region's focus on proactive exposure management and measurable risk reduction. Guy March, VP of Channel Sales – EMEA, emphasizes moving beyond reactive firefighting toward unified, intelligence-driven resilience.

"We will use GISEC 2026 to demonstrate how proactive exposure management will help organizations move beyond reactive firefighting and build measurable, outcome-driven resilience. We will show how unifying visibility across cloud, identity, OT and AI environments will simplify operations, consolidate fragmented tools and align directly with Middle East digital-transformation priorities. As AI accelerates risk and expands attack surfaces, we will highlight how connected exposures create toxic combinations that attackers exploit. Through the Tenable One Exposure Management Platform, we will map relationships across systems, cut through alert noise and pinpoint the chokepoints teams must fix first. We will also work closely with channel partners to operationalize exposure management and elevate long-term cybersecurity maturity across the region."

VMRay closes the loop with deep malware analysis and AI driven SOC efficiency. Hüseyin Fatih Akar, Senior Security Product Manager, emphasizes understanding threats rather than simply detecting them.

"We will be at our partner Shifra's booth, focusing on meaningful conversations and practical showcases. We will discuss what we expect to see in malware and phishing analysis, how threat intelligence will be built from observed behavior, and how AI will genuinely support security operations rather than add noise. Evasive, targeted attacks will arrive at speed and scale, driven by AI and organized criminal operations. Phishing will function as a delivery chain, not a single link, requiring us to go beyond verdicts to understand execution paths, infrastructure, and intent. We will focus on shifting from detection to understanding and on automating routine SOC tasks so analysts can concentrate on deeper work. Accurate, noise-free analysis will make AI-driven workflows trustworthy at scale."

GISEC Global 2026 makes one truth unmistakable: the Middle East is no longer a passive consumer of global cybersecurity innovation — it is shaping the future of cyber defense. Across sovereign AI, microsegmentation, identity governance, observability, OT security, adversary centric intelligence, and partner driven resilience, the region's priorities are clear: anticipate, contain, govern, and collaborate.

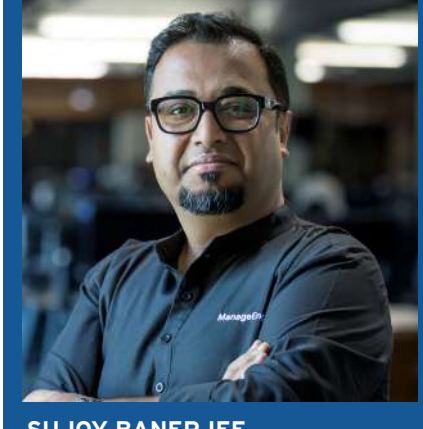
The 18 spokespersons featured in this story represent a cybersecurity ecosystem that is maturing rapidly, driven by regulatory clarity, critical infrastructure stakes, and a willingness to adopt advanced architectures.

Their messages converge on a single point: AI has changed the tempo of cyber risk, and the Middle East is responding with equal speed, discipline, and ambition.

GISEC 2026 is not just an exhibition — it is a declaration. The region is ready for what comes next.



SHEETAL KALRA
CHANNEL ACCOUNT MANAGER - MIDDLE EAST, TURKIYE AND ENGLISH-SPEAKING AFRICA, SOLARWINDS



SUJOY BANERJEE
REGIONAL BUSINESS DIRECTOR FOR THE UAE AT MANAGEENGINE

HID, SOLOINSIGHT AND CTS INTRODUCE INTEGRATED SELF-SERVICE VISITOR CHECK-IN KIOSK

HID announced that its hardware-based HID ATOM document reader and HID U.ARE.U facial recognition module have been integrated with Soloinsight's CloudGate visitor management and physical identity and access management (PIAM) platform to enhance the self-service visitor check-in kiosk from Connected Technology Solutions (CTS). Designed for global enterprises and critical infrastructure environments, the integration enables organizations to verify visitor identities before issuing access credentials while creating a consistent, auditable visitor management process.

Facilities such as hospitals, data centers, offices and logistics hubs often manage hundreds of contractors, vendors and visitors each day, yet most check-in processes verify little more than a name. A visitor can type any name into a tablet or present a photo ID that a receptionist has no way to authenticate, which means the person issued a badge may not be who they claim to be. For regulated or high-risk facilities, that unverified access creates real exposure: unauthorized individuals gaining entry, gaps in the audit trail when an incident occurs and compliance failures when organizations cannot prove who was on site and when. By combining document authentication, facial verification and visitor management into a single solution, the kiosk helps security teams streamline visitor processing, reduce manual identity checks and maintain detailed records for compliance and investigations.



How it works

A host pre-registers their visitor in CloudGate, which sends an email invitation with a QR code to the visitor. At the kiosk, the visitor scans the QR code, then verifies their identity through the HID ATOM document scanner, which reads passports, driver's licenses and mobile IDs. The HID U.ARE.U Face Module runs live face verification and rejects any scan that does not match the identity document or is not a live face. CloudGate confirms check-in, the kiosk prints a visitor pass on the spot and the host is notified. Returning visitors can also be granted a hostless welcome where appropriate.

Following identity verification, CloudGate records each transaction in a centralized visitor record, providing security teams with a complete history of visitor activity that supports investigations, reporting and regulatory compliance.

The kiosk delivers stronger identity assurance with hardware grade document and facial verification, supports any credential in one scan, embeds compliance into every record, enhances existing security investments, and provides US built enterprise grade support.

DELL LAUNCHES NEW 14S LIGHTWEIGHT WINDOWS LAPTOP

Dell Technologies announced the Dell 14S, a lightweight everyday Windows laptop designed for students and young adults who prioritize long battery life, portability, design and value. With a modern aluminum chassis, four expressive color options and up to 21 hours of battery life, the Dell 14S brings features typically associated with premium laptops to a broader audience. It complements the XPS 13, giving customers a choice between an everyday device and Dell's premium ultraportable experience.

Students and young adults have often had to choose between a laptop that looks great, lasts all day or fits their budget. The Dell 14S is built around all three: a design that feels personal, a battery that lasts through a full day, and a build quality that holds up over time — all at a price point accessible to more users.

The Dell 14S comes in four distinct colors — Linen, Dusty Rose, Washed Denim and Velvet Green — each giving the sleek aluminum chassis a different personality. At 13.5 mm thin and 1.15 kg, it is light enough to disappear into a bag yet solid enough for everyday use. The expressive color palette marks a deliberate return to personal design in Dell's consumer lineup, reflecting the belief that everyday technology should feel individual.

With up to 21 hours of Netflix streaming on a single charge, the Dell 14S is built to last through classes, study sessions, work and entertainment without constant recharging. This endurance comes from a 750ED PNCM battery, a denser cell engineered to run cooler and retain capacity over time without adding weight or cost.



Two 16:10 display options meet different priorities: a 2.8K 120 Hz panel for sharp, smooth visuals, and a 2K 60 Hz panel for users who prioritize battery life and value. Both options deliver bright, accurate colors.

Powered by Intel Core 5 and Core 7 Series 3 processors, the Dell 14S handles multitasking across tabs, documents and apps with ease. An FHD camera, far field dual array microphones and stereo speakers support clear video calls, while Wi Fi 6E ensures fast, reliable connectivity. Every configuration includes Windows Hello, two USB C ports with power delivery, HDMI, and a headphone jack — making the Dell 14S ready for the connected demands of modern daily life.

AOC LAUNCHES NEW QD-OLED GAMING MONITOR IN THE MIDDLE EAST

AOC today announced the regional launch of the Q27G40ZDF in the Middle East. The 26.5-inch display features a QD-OLED panel and targets esports players and serious gamers who need speed, color accuracy, and reliability in one package.

The monitor runs at 240Hz with a 0.03ms response time (GtG), which puts it in the same performance class as hardware used in professional tournaments. Motion blur is minimal, and Adaptive-Sync support helps keep screen tearing in check across a wide range of frame rates.

On the visual side, the QD-OLED panel covers 99% of the DCI-P3 color space and supports HDR10. That means deeper blacks, better contrast, and more vivid colors compared to standard IPS or VA panels—useful not just for gaming, but also for media consumption and creative work.



One of the more interesting design choices here is the cooling system. AOC used a graphene film combined with a custom heatsink to manage heat without relying on a fan. The result is a monitor that stays quiet during long sessions while also protecting the panel from thermal stress over time.

AOC also included several software-based tools for gamers. The DialPoint feature gives users a customizable on-screen crosshair for first-person shooters. It also includes a Sniper Scope mode, Dark Boost for visibility in shadowy areas, and Game Color controls that let users adjust saturation levels between 0 and 20.

For those concerned about eye strain, the monitor includes Flicker-Free technology and an anti-blue light solution that filters out harmful wavelengths in the 455nm range.

For connectivity, the Q27G40ZDF offers one HDMI 2.0 port and one DisplayPort 1.4 input. It supports 2560 x 1440 resolution at 240Hz over DisplayPort, and 144Hz over HDMI. The stand allows for tilt adjustment from -5° to 23°, and the monitor is VESA-compatible for wall mounting.

Pricing and Availability

The AOC Gaming monitor Q27G40ZDF is available in the United Arab Emirates with the distributor SDC FZE and can be purchased online. In Saudi Arabia it is available for online purchase with Golden Technologies. All AOC monitors come with a 3-year warranty in the UAE and a 2-year warranty in Saudi Arabia.

ACER LAUNCHES TWO NEW THIN AND LIGHT LAPTOPS

Acer has introduced two new thin and light laptops designed to expand portable performance possibilities: the ultralight Acer Swift Blade 14 and the stylish Acer Swift Air 16, both running Windows 11.

Acer Swift Blade 14

Weighing just 799 g and measuring 12.9 mm thin, the 14 inch Acer Swift Blade 14 (SFB14 53CF) is engineered for mobile productivity and visual driven workflows. It is powered by up to an Intel Core 7 processor 350, paired with 12 GB LPDDR5 memory and up to 1 TB of storage, delivering performance for work, creativity, and entertainment on the go.

The laptop features up to a 3K OLED display with 100% DCI P3 color gamut, a 90% screen to body ratio, ultra slim 4.3 mm bezels, and a 16:10 aspect ratio for immersive visuals. A 50 Wh battery supports all day use, while three USB 3.2 Gen 1 Type C ports and a FHD camera with a privacy switch ensure seamless connectivity. Its chassis blends magnesium aluminum alloy with carbon fiber and comes in marshmallow blue or marshmallow white.

Acer Swift Air 16

The 16 inch Acer Swift Air 16 (SFA16 I31T / SFA16 I31) balances style and performance for users who need versatility. It is powered by up to an Intel Core 7 processor 350 with 40 TOPS and a dedicated NPU, paired with up to 16 GB LPDDR5x memory and up to 512 GB of



upgradable storage. At 13.3 mm thin and 1.5 kg, the laptop features an all aluminum chassis in elemental blue, sage green, or sandstone gold, with a backlit keyboard for productivity in any environment. Its 70 Wh battery supports fast charging to 50% in 30 minutes via a 100W adapter.

For visual driven tasks, the Swift Air 16 offers OLED (100% DCI P3) or IPS (100% sRGB) options, up to WQXGA+ (2880 × 1800) resolution, 500 nits brightness, and up to 120 Hz refresh rate. A multi touch IPS option is also available. Quad speakers with DTS Virtual:X deliver immersive audio, while dual Thunderbolt 4 ports ensure high speed connectivity.

mystartup! WORLD

Welcome to My Startup World – Your Gateway to Startup Success!

Are you a visionary entrepreneur, an ambitious startup, or an investor looking to navigate the dynamic world of innovation? Dive into My Startup World, the premier online news portal dedicated to the startup ecosystem!

✨ Why Choose Us?



Stay Informed

Get the latest news articles and insights that matter to your startup journey.



Inspire & Learn

Explore thought-provoking feature stories that showcase the triumphs and challenges of fellow startups.



Expert Voices

Gain wisdom from exclusive interviews with industry leaders and pioneers who have been where you are.



Thought Leadership

Benefit from expert opinion pieces that provide strategies and tips tailored for startups like yours.

📈 Connect and Grow

Join a thriving community of entrepreneurs, angel investors, and venture capitalists who are passionate about innovation and growth. Whether you're seeking funding or looking to share your story, My Startup World is here to amplify your voice.

🔍 Don't Just Survive - Thrive! 📈

Build your brand and raise awareness in a rapidly evolving marketplace. Leverage our platform to connect, engage, and inspire.

👉 Visit My Startup World Today and Become Part of the Startup Revolution!

security
MIDDLE EAST & AFRICA



STAY AHEAD OF CYBER THREATS.

VISIT SECURITY MEA, YOUR TRUSTED SOURCE FOR NEWS, INSIGHTS, AND STRATEGIES IN CYBERSECURITY.

www.securitymea.com