

# Security **ADVISOR**

MIDDLE EAST



## UAE & SAUDI ARABIA SHAPE MENA SECURITY

# PRINT WITH **PURPOSE**

## **Fujifilm Apeos Series**

offered by MPS Company,  
Where Eco-Friendly meets Efficiency!



+971 45281000 | [info@mps-uae.com](mailto:info@mps-uae.com)





**6** Emirates Health Services and Dell Technologies sign MoU to enhance digital infrastructure in healthcare sector

**44** Pig Butchering scams surge 40% in 2024, expanding to target job seekers, says Chainalysis Report

**18** LEAP 2025 shatters records with US\$14.9 Billion AI investment, solidifying

**48** Cisco Study: CEOs embrace AI, but knowledge gaps threaten strategic decisions and growth

# Secure Your **Digital Future**

Simple. Secure. Resilient.



**Secure Your Enterprise IT Footprint  
For A Safer Digital Journey**



# EDITOR'S NOTE



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

**Sandhya DMello**  
Editor

## UAE AND SAUDI ARABIA DRIVE AI, CYBERSECURITY, AND DIGITAL INNOVATION IN MENA

The Middle East is at the forefront of a digital revolution, with Saudi Arabia and the UAE driving the region's AI, cybersecurity, and digital economy ambitions. This month's issue of Security Advisor Middle East spotlights the landmark KSA Executive Summit 2025, where UAE and Saudi leaders are shaping the future of AI governance and cybersecurity. LEAP 2025's staggering \$14.9 billion AI investment further cements Saudi Arabia's position as a global tech powerhouse, reinforcing the MENA region's commitment to innovation.

AI is not just a buzzword; it is reshaping economies. The UAE's ranking among the top 10 nations in AI enterprise density signals its success in fostering a thriving AI ecosystem. Meanwhile, Abu Dhabi's Hub71 continues to attract high-growth startups, expanding the emirate's role as a global tech hub.

Cyber resilience remains paramount as emerging threats evolve. Reports of rising real estate scams, romance fraud, and IoT-based cyberattacks highlight the urgency

of robust security measures. The Group-IB report on real estate fraud and Chainalysis' findings on pig-butcher scams underscore how cybercriminals exploit digital platforms to orchestrate deception. Encouragingly, ransomware payments saw a 35% drop in 2024, signaling growing enterprise awareness and improved defense mechanisms.

With the UAE's emphasis on children's digital well-being, we also explore the landmark pact between leading tech giants such as Snapchat, Meta, Google, TikTok, and X, signed at the

World Government Summit in Dubai. The need for responsible digital ecosystems has never been greater, and this initiative is a testament to proactive governance.

As we continue to track the convergence of AI, cybersecurity, and enterprise transformation, one thing remains clear: digital resilience is not a choice—it's an imperative. Stay ahead with Security Advisor Middle East as we bring you the latest insights shaping the future of security and innovation.

### AI SET TO RESHAPE ECONOMIES

#### EVENTS



FOUNDER, CPI  
Dominic De Sousa  
(1959-2015)

Published by **CPI**

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

EDITORIAL  
Editor  
Sandhya DMello  
sandhya.dmello@cpimediagroup.com

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

DIGITAL SERVICES  
Web Developer  
Adarsh Snehanjan  
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

Sales Director  
Sabita Miranda  
sabita.miranda@cpimediagroup.com

Online Editor  
Daniel Shepherd  
daniel.shepherd@cpimediagroup.com

© Copyright 2025 CPI  
All rights reserved

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

## CORE42 LAUNCHES AN AI DEVELOPER PLAYGROUND FOR AI INFERENCE-AS-A-SERVICE WITH QUALCOMM IN UAE

**Core42, a G42 company specializing in** sovereign cloud, AI infrastructure, and digital services, announced the launch of the AI Playground in UAE data centers. Built on the Qualcomm® Cloud AI family of accelerators and Qualcomm® AI Inference Suite for Cloud, this free-to-access platform equips developers and AI engineers with ready-to-use high-performance AI applications and agents, tools, and libraries to streamline AI adoption and deployment across cloud and edge devices.

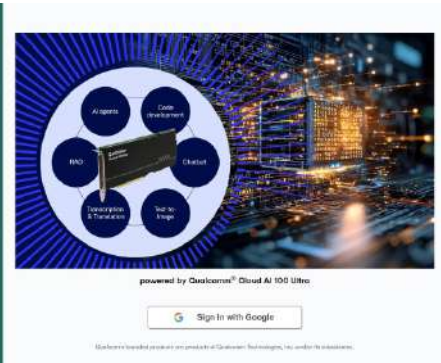
The AI Developer Playground removes infrastructure complexity by integrating AI inference accelerators, standardized APIs, and pre-built generative AI applications to maximize efficiency. As AI adoption accelerates across industries, the need for automation, scalability, and performance optimization has become critical. This platform empowers developers and AI engineers to build, scale, and optimize AI solutions effortlessly, supporting everything from computer vision to generative AI.

“As AI reshapes businesses at an accelerated pace, Core42 is committed to providing the infrastructure that drives this transformation,” said Raghu Chakravarthi, EVP of Engineering at Core42. “By offering the Qualcomm AI Inference Suite, we are making AI more accessible, scalable, and efficient, driving both innovation and sustainability across industries.”



The Qualcomm AI Inference Suite offers a comprehensive set of enterprise-ready AI tools, enabling developers to build AI agents and applications across a range of use cases, including, Chat, Reasoning, Code or Image Generation, Enterprise RAG applications. This cost-effective cloud solution supports Kubernetes and bare-metal container deployments, ensuring integration with popular generative AI models and frameworks. Developers also gain free access to leading open-source models, including Llama-3.3 70B and JAIS30B, with continuous updates to align with evolving AI demands.

“We are proud to collaborate with Core42 to open new frontiers in automation and efficiency. Together, we can enable breakthroughs across enterprises, delivering AI-powered agents for applications as diverse as smart city automation, digital (social media) marketing, and medical AI applications,”



said Rashid Attar, SVP, Cloud Computing, Qualcomm Technologies, Inc. “This solution offers a robust, security-rich, end-to-end platform that can be deployed, empowering developers to reach users without the burden of managing complex infrastructure.”

Core42’s collaboration with Qualcomm Technologies, Inc. through the Qualcomm AI Inference Suite and Cloud AI accelerators grants developers and AI engineers seamless access to advanced AI models and applications, enabling optimal performance while reducing operational costs. By advancing inference-as-a-service, this collaboration empowers developers and AI engineers to stay at the forefront of AI innovation, effortlessly integrating the latest advancements into their workflows.

Developers and AI engineers can now access the Playground: <https://playground.core42.ai>

## EMIRATES HEALTH SERVICES AND DELL TECHNOLOGIES SIGN MOU TO ENHANCE DIGITAL INFRASTRUCTURE IN HEALTHCARE SECTOR

**Emirates Health Services (EHS)** and Dell Technologies have signed a Memorandum of Understanding (MoU) to drive advancements in digital infrastructure by providing EHS with

advanced artificial intelligence (AI) and cybersecurity technologies, paving the way for transformative changes in the UAE’s healthcare system.

The memorandum of understanding

was signed by H.E Mubarak Mubarak Ibrahim, Chief Artificial Intelligence Officer and Acting Executive Director of the Information Sector at Emirates Health Services, and Walid Yehia,



Managing Director - Gulf, at Dell Technologies. Under the terms of the agreement, both EHS and Dell will collaborate across several key areas, including organizing targeted workshops to share best practices in cybersecurity, advancing EHS' AI initiatives, enhancing technical expertise with specialized training sessions and support programs, and providing access to consulting services from experts.

H.E Mubarak Mubarak Ibrahim, Chief Artificial Intelligence Officer and Acting Executive Director of the Information Sector at Emirates Health Services, said:

"At EHS, we are dedicated to advancing the UAE's healthcare sector by aligning with national priorities and visionary goals. By working with Dell, we'll be able to explore new technologies that will elevate service quality and efficiency across our healthcare facilities, while also enhancing accessibility to our services. This is part of our strategy to foster a future-ready healthcare ecosystem that promotes societal well-being and reinforces the UAE's standing as a global leader in healthcare excellence."



Mubarak Mubarak Ibrahim, Chief Artificial Intelligence Officer and Acting Executive Director of the Information Sector, Emirates Health Services, and Walid Yehia, Managing Director – Gulf, Dell Technologies at the MoU signing ceremony.

As innovations in healthcare continue to shape every facet of the patient experience, the collaboration will focus on leveraging advanced technologies that will ultimately streamline patient care processes, improve clinical outcomes, while seamlessly integrating into healthcare operations.

Walid Yehia, Managing Director - Gulf, at Dell Technologies, said: "AI and

cybersecurity are transforming how the healthcare sector operates and delivers critical services. Through our work with organizations like EHS, we strive to empower the UAE healthcare industry with secure, scalable, and cutting-edge solutions to address modern challenges. The MoU sets the stage for scaling innovative solutions that address the evolving demands of the UAE healthcare sector."

## FORTINET DELIVERS UNMATCHED SECURITY AND EFFICIENT NETWORK PERFORMANCE FOR DISTRIBUTED ENTERPRISE WITH NEW NEXT-GEN FIREWALLS

New FortiGate G series next-gen firewalls empower customers to strengthen threat protection and future-proof IT infrastructure

**Fortinet (NASDAQ: FTNT), the global cybersecurity leader driving the convergence of networking and security, today announced the FortiGate 70G, FortiGate 50G, and FortiGate 30G, the latest G series next-generation firewalls (NGFWs) designed to meet the evolving technology and business demands of today's distributed enterprises.**

Powered by Fortinet's proprietary ASIC technology and the unified Fortinet operating system, FortiOS, the FortiGate G series delivers industry-leading security with unmatched performance. These features, combined with advanced



Nirav Shah, Senior Vice President, Products and Solutions at Fortinet.

networking support and FortiGuard AI-Powered Security Services, reduce the risk of successful cyberattacks and allow customers to future-proof IT infrastructure while minimizing operational costs and environmental impact.

"For nearly 25 years, we have set the standard for fortifying enterprise networks," said Nirav Shah, Senior Vice President, Products and Solutions at Fortinet. "By completing the FortiGate G series with the latest ASIC and FortiOS innovation, we give distributed enterprises cutting-edge tools like AI-

powered security services and GenAI for network and security operations centers without compromising performance or sustainability needs. Our customers trust that Fortinet will continue redefining the standard for next-generation firewalls by delivering superior security effectiveness, greater energy efficiency, and unmatched performance for years to come.”

### FortiGate G Series: Industry-Leading Performance with AI-Powered Security

Today’s enterprises are under pressure to scale operations, secure expanding attack surfaces, and manage increasingly sophisticated cyberthreats while reducing

costs and maintaining efficiency. The FortiGate G series is engineered to meet these demands, offering:

- Cutting-edge security with unmatched power efficiency: The FortiGate G series delivers superior protection without compromising performance. For example, the new FortiGate 70G delivers up to 11x higher IPsec VPN and 7x higher firewall throughput than the industry average while consuming 62x fewer watts per Gbps of IPsec VPN throughput and 42x fewer watts per Gbps of firewall throughput.
- Faster identification, containment, and mitigation of threats: FortiGuard

AI-Powered Security Services provides real-time, automated threat detection and response to defend against advanced ransomware, malware, and zero-day exploits.

- FortiAI for enhanced cybersecurity operations: FortiAI, the Fortinet generative AI assistant, helps automate tasks, provides actionable insights, and improves threat detection. FortiGate customers can use FortiAI to support incident analysis, threat remediation, and playbook creation, empowering them to streamline security processes and strengthen their cybersecurity posture.

## NVIDIA DLSS ENHANCES PERFORMANCE IN NEW TITLES

### NVIDIA released DLSS 4, featuring

DLSS Multi Frame Generation for GeForce RTX 50 Series graphics cards and laptops, available in over 75 games and apps. Along with NVIDIA app’s new DLSS 4 overrides, which allow gamers to further enhance their experience by adding DLSS 4 with Multi Frame Generation, or new and improved AI models for supported titles.

Now, the complete suite of DLSS 4 upgrades, including DLSS 4 with Multi Frame Generation, are available in Alan Wake 2, Cyberpunk 2077, and Hogwarts Legacy, and Star Wars™ Outlaws adds support soon. Gamers can enjoy 6 more games that are DLSS-enhanced – Kingdom Come: Deliverance II, The First Berserker: Khazan, NINJA GAIDEN 2 Black, Ambulance Life: A Paramedic Simulator, FINAL FANTASY VII REBIRTH, and Level Zero: Extraction.

NVIDIA RTX technology is delivering the definitive PC experience for GeForce RTX players.

NEXON and Neople’s The First Berserker: Khazan is an upcoming single-player hardcore action RPG from the extensive universe of Dungeon & Fighter (DNF) to millions of players



around the world. Ahead of its March 27th release, gamers can now download a two-level demo from Steam, with progress transferring to the full version upon release. In the demo, all GeForce RTX gamers can activate DLSS Super Resolution, accelerating frame rates, and NVIDIA Reflex, reducing PC latency to make battles even more responsive. Alternatively, gamers can activate DLAA if they have performance to spare, maximizing image quality. Using NVIDIA app’s new DLSS 4 overrides, gamers can also upgrade DLSS Super Resolution

to the new transformer AI model, further enhancing image quality, and activate DLSS Multi Frame Generation, generating up to three additional frames per traditionally rendered frame, for even faster frame rates.

NINJA GAIDEN 2 Black, the remaster of 2008’s Ninja Gaiden II is developed with Unreal Engine 5, and boasts hardware-accelerated ray-traced Lumen lighting, significantly enhancing everything from character visuals to environmental backgrounds, while characters, effects, and lighting have



been completely redesigned to take full advantage of modern technology. GeForce RTX PC gamers can activate DLSS Super Resolution and DLSS Frame Generation to accelerate performance.

Developed by Aesir Interactive and Nacon, Ambulance Life: A Paramedic Simulator is the first simulation game in which gamers experience every aspect of a paramedic's life. Quickly reach the accident site at the wheel of your ambulance and take care of the injured with first aid. At launch, the game will include support for DLSS Super Resolution and DLSS Frame Generation, accelerating performance in the game's large, fictional, ray-traced U.S. city.

FINAL FANTASY VII REBIRTH, the FINAL FANTASY VII remake project, uses the latest technology to bring

FINAL FANTASY VII to a new generation and allows fans to experience the famed story reimagined. The second installment in the project, FINAL FANTASY VII REBIRTH, is out now on PC, and GeForce RTX gamers can accelerate performance using DLSS Super Resolution.

Published by PLAION, Kingdom Come: Deliverance II picks up where its predecessor left off, thrusting players into the shoes of Henry, the steadfast son of a blacksmith, embroiled in a tumultuous tale of vengeance, betrayal, and self-discovery. GeForce RTX gamers can elevate their experience with DLSS Super Resolution, boosting frame rates for even greater immersion in its stunning 15th-century open world. NVIDIA app users can upgrade DLSS

Super Resolution in Kingdom Come: Deliverance II to a new, even better DLSS 4 transformer AI model to further enhance image quality and activate DLAA.

Level Zero: Extraction is a multiplayer extraction horror shooter from Doghowl Games and tinyBuild that blends the heart-pounding tension of asymmetric survival horrors with the high-stakes showdowns of extraction shooters. Playing as an elite PMC mercenary, embark on dangerous raids to extract valuable loot and face off against other players and unpredictable PvE hazards. Level Zero: Extraction has just exited Early Access, and GeForce RTX gamers can accelerate frame rates with DLSS Super Resolution and DLSS Frame Generation.

## IDEX AND NAVDEX 2025 KICKS OFF IN ABU DHABI, MARKING ITS LARGEST AND MOST ADVANCED EDITION

**Under the esteemed patronage of His Highness Sheikh Mohamed bin Zayed Al Nahyan, President of the UAE, the International Defence Exhibition (IDEX) and the Naval Defence and Maritime Security Exhibition (NAVDEX) 2025 officially opened on February 17 at ADNEC Centre Abu Dhabi.**

Organised by ADNEC Group in partnership with the UAE Ministry of Defence and Tawazun Council, this year's edition marks a significant milestone as the largest and most technologically advanced in the event's history. The exhibitions welcome an unprecedented number of exhibitors, featuring 1,565 defence and security companies from 65 countries, a 16% increase from the previous edition.

IDEX 2025 showcases the latest advancements in artificial intelligence, autonomous systems, cybersecurity, and next-generation defence solutions, providing a platform for global

collaboration and innovation. NAVDEX 2025, the region's premier maritime defence exhibition, will feature state-of-the-art naval technologies, live demonstrations, and a dedicated space for international warships at ADNEC Marina.

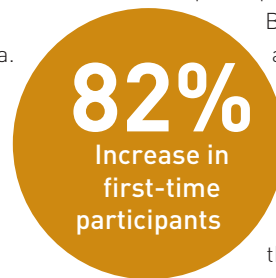
As part of this year's expansion, Hall 14 debuts as a new addition to the exhibition, featuring the CBRNE Hub, a specialised platform dedicated to chemical, biological, radiological, nuclear, and explosives defence solutions. The hub will bring together military leaders, specialists, and 38 companies from 13 countries to discuss cutting-edge innovations in this critical field.

With an expanded exhibition space of 181,501 square metres, the 2025 edition also sees the participation of 41 national pavilions, with the UAE Pavilion

as the largest, spanning 25,000 square metres. Additionally, more than 731 new exhibitors are making their debut, reflecting an 82% increase in first-time participants.

Beyond the exhibition floor, IDEX and NAVDEX 2025 will host a comprehensive conference programme, where defence ministers, policymakers, and industry experts will discuss emerging security threats, defence readiness, and the evolving role of space and cyber technologies.

IDEX and NAVDEX continue to serve as a global platform for fostering strategic partnerships, advancing defence industry growth, and reinforcing international security cooperation. The exhibitions will run until 21 February 2025, bringing together military leaders, government officials, and industry pioneers from around the world.



## QUALYS INTRODUCES MANAGED RISK OPERATION CENTER (MROC) PARTNER ALLIANCE TO SCALE CYBER RISK SERVICES

mROC, powered by Qualys Enterprise TruRisk Management, accelerates revenue paths for partners helping CISOs articulate cyber risk as business risk

**Qualys, Inc, a leading provider of disruptive** cloud-based IT, security and compliance solutions, has announced the Managed Risk Operations Center (mROC) Partner Alliance, allowing select Qualys partners to expand their revenue streams by offering advisory, onboarding, integration, and remediation through a unified managed service to help their clients identify, quantify, assess, and mitigate cyber risks. This provides qualified Qualys Managed Service Solution Partners (MSSPs) the exclusive opportunity to grow their service offerings among Qualys' extensive installed base of enterprise customers.

Organizations often face challenges managing the overwhelming volume of risk findings spread across siloed tools, resulting in inefficiencies and overlooked threats. To solve this, Qualys has transformed Cyber Risk Management with the Risk Operations Center (ROC) powered by Enterprise TruRisk Management (ETM). This innovative solution consolidates diverse risk insights into a unified view, quantifies and communicates cyber risk in terms of Business Value at Risk (potential loss of money, trust, productivity), and automates and orchestrates risk reduction to enhance an organization's security.

Achieving the full potential of the ROC is best achieved via trusted partners who streamline cyber data aggregation through integrations and connectors, apply industry-aligned risk models and quantification, and provide continuous cyber risk monitoring. These experts help CISOs communicate risk to executives, boards, and stakeholders in terms of VAR while ensuring risk is monitored and remediated in alignment with the organization's risk tolerance.

"Given the increasing complexity of the attack surface, Qualys' mROC will be extremely valuable in helping our clients identify and mitigate risk," said Mark Thornberry, SVP, Vendor Marketing at



Sumedh Thakar - CEO at Qualys

GuidePoint Security. "Qualys continues to empower its partners with cutting-edge solutions that enable organizations to stay ahead of evolving threats, enhance operational efficiency, and implement a proactive approach to mitigating risk. We're excited for this evolution."

Through mROC, MSSP partners translate cyber risk into the language of business. These services powered by Qualys ETM foster a quantitative, holistic, and strategic approach to cyber risk management. Partners benefit through:

Enhanced Service Offerings — The mROC Partner Alliance empowers partners to drive growth by elevating services and focusing on a more strategic, value-added approach. New service offerings include:

- **Cyber Risk Advisory Services** — Assess the state of current vulnerability management program and develop a strategic roadmap for ROC implementation. Provide customized cyber risk quantification, estimating the value at risk to align resource allocation with business goals.
- **Onboarding and Integration Services** — Establish a centralized platform that consolidates risk telemetry from disparate tools to deliver a unified asset inventory, continuous vulnerability management, automated workflows

for prioritization and remediation, and executive reporting.

- **Continuous Risk Monitoring Services** — Deliver actionable insights for executive reporting via continuously monitoring risk signals, automating workflows to close visibility gaps, tracking risk trends, and benchmarking against industry standards.
- **Risk Remediation Services** — Design and automate risk reduction programs, including patching and applying compensating controls, by integrating ETM with existing remediation solutions. Deliver expert remediation support with rapid response to zero-day and celebrity vulnerabilities.

Revenue growth — mROC partners can tap into Qualys' extensive installed base to upsell solutions and support the adoption of third-party tools, fostering revenue growth.

No Cost Training and Enablement — mROC Partners gain exclusive access to benefits like in-depth product training, personalized roadmap discussions, technical guidance, and one-on-one risk workshops. Additionally, partners will have the opportunity for strategic co-selling, enabling an accelerated route to market and driving faster customer adoption.

"Establishing a Risk Operations Center as a centralized, proactive cybersecurity management platform is a key strategy for CISOs aiming to systematically reduce risk while enhancing operational efficiency and business resilience," said Sumedh Thakar, president and CEO of Qualys. "With mROC, CISOs have access to an ecosystem of partners who operationalize the ROC and serve as strategic risk advisors. For MSSPs, mROC unlocks a valuable revenue opportunity, empowering them to deliver comprehensive cyber risk management—including risk aggregation, quantification, monitoring, and remediation—powered by Qualys Enterprise TruRisk Management."



تحت الرعاية السامية لصاحب الجلالة الملك محمد السادس  
Under the High Patronage of His Majesty King Mohammed VI



UNDER THE AUTHORITY OF



IN PARTNERSHIP WITH



ORGANISED BY



14 - 16 APRIL 2025 MARRAKECH

# POWERING AFRICA INTO THE GLOBAL AI ECONOMY

AFRICA'S LARGEST TECH AND  
STARTUP EVENT JUST GOT BIGGER

**45,000**  
ATTENDEES

**1,400**  
EXHIBITING & STARTUP  
COMPANIES

**435**  
MEDIA ATTENDEES

**650+**  
GOVERNMENT  
REPRESENTATIVES

**130+**  
COUNTRIES  
REPRESENTED

**340+**  
INVESTORS WITH \$250  
BILLION ASSETS UNDER  
MANAGEMENT

**660+**  
SPEAKERS

**70%**  
OF INVESTORS PLAN  
TO INVEST IN STARTUPS

- AI EVERYTHING MOROCCO (AI X CLOUD X IOT)
- DATA CENTRES **NEW**
- CYBERSECURITY
- TELECOM & NETWORK INFRASTRUCTURE
- DIGITAL CITIES
- E-MOBILITY **NEW**
- GITEX IMPACT (SUSTAINABILITY, CLIMATE TECH, AGRITECH) **NEW**
- HEALTHTECH 5.0
- FUTURE OF BANKING & FINANCE
- NORTH STAR AFRICA - STARTUPS

[gitexafrica.com](https://gitexafrica.com)

in X f @ /gitexafrica



SCAN TO  
GET INVOLVED

# UAE, SAUDI ARABIA DRIVE DIGITAL INNOVATION IN MENA

DUBAI-BASED CPI MEDIA GROUP EXPANDS ITS REGIONAL FOOTPRINT WITH A HIGH-PROFILE SUMMIT IN RIYADH, SPOTLIGHTING SAUDI ARABIA'S AI GOVERNANCE AND CYBERSECURITY LEADERSHIP IN THE MENA DIGITAL ECONOMY.





**D**ubai-headquartered CPI Media Group, a leading media and events company in the Middle East, took a strategic

step forward in regional expansion by successfully making its debut with KSA Executive Summit 2025 in Riyadh on February 13, 2025, hosted by TahawulTech.com, following the conclusion of LEAP 2025.

Held at the VOCO Hotel, situated in the heart of the Kingdom's capital, the conference brought together technology leaders and cybersecurity practitioners from across the Middle East to discuss the evolving landscape of AI, cybersecurity, and emerging technologies.

The event was moderated by CNME Editor Mark Forker, with the first keynote presentation delivered by Ian Winfield, Chief Technology Officer, EMEA – AI and HPC Solutions at Hitachi Vantara.

In his address, Winfield underscored the critical need for robust frameworks and governance to ensure that AI is deployed ethically and responsibly. He highlighted that while AI remains at the center of large-scale investments and corporate strategies, discussions on ethics and governance often receive minimal attention.

"AI was the most used word in 2024, yet there was little mention of governance or ethics, which is a major concern. At Hitachi Vantara, our AI strategy is built on four core pillars—transparency, fairness, privacy and security, and accountability. It is essential to provide clear explanations of AI systems, ensure unbiased decision-making, protect user data, and assign responsibility for AI-driven actions," stated Winfield.

Following the keynote, CNME Editor Mark Forker moderated a panel discussion on Ethical AI and Governance, featuring Ian Winfield and Tahir Latif, Expert AI Regulatory Advisor at Dubai International Financial Centre.





**Mandar Patil**



**Mayuresh Kothari**



**Eng. Naveed Ahmed**

Both panelists expressed their disappointment over the decision of the US and UK governments to refrain from signing a global governance framework for AI at the Global AI Action Summit in Paris.

Latif emphasized that the decision posed a significant challenge to establishing universal AI regulations and noted that the stance of the US government—particularly under a potential Trump administration—was unlikely to shift.

“The UK cited security concerns for its decision, which could be a major setback to its AI Action Plan. Meanwhile, the US argued that such regulations could hinder AI innovation. Under a Trump administration, AI is a strategic priority, and his go-it-alone approach suggests the US is unlikely to engage in global governance efforts anytime soon,” said Latif.

Despite these global challenges, both Latif and Winfield agreed that the Middle East—particularly the UAE and Saudi Arabia—has the financial resources and strategic vision to emerge as a global leader in AI development and governance.

**AI and Cybersecurity: A New Frontier**

The summit continued with a keynote presentation from Ahmad Halabi, Managing Director at Resecurity, who examined AI’s growing impact on cybersecurity ecosystems. His insights seamlessly set the stage for the subsequent panel discussion, titled:

“Cybersecurity – Safeguarding the New Technological Frontier through an AI-Enhanced Cyber Resilience.”

The panel featured distinguished speakers, including:

- **Mandar Patil**, Senior Vice President – International Market & Customer Success, Cyble

- **Mayuresh Kothari**, Technical Director, Secureworks (a Sophos company)
- **Eng. Naveed Ahmed**, Cybersecurity Risk Expert, Saudi Data & AI Authority (SDAIA)
- **Wolfgang Kroj**, General Manager – Sales, Middle East and Africa, Hitachi Vantara
- **Salman Mushtaq Qureshi**, Leading Cybersecurity Expert based in Saudi Arabia

The discussion offered profound insights into emerging threats, the evolving cybersecurity landscape, and the role of AI in cyber resilience.

One of the key takeaways from the session was the assertion by Wolfgang Kroj of Hitachi Vantara that cybersecurity is fundamentally a mindset rather than just a technological challenge.

“Cybersecurity has to become a state of mind. Simply investing in technology without a strategic approach is naïve and impractical. AI and cybersecurity always come back to people and processes—it’s about how we integrate these tools into our overall framework,” remarked Kroj.

The KSA Executive Summit 2025 provided an engaging, educational, and insightful platform for industry leaders, reinforcing the importance of AI governance, cybersecurity resilience, and ethical AI deployment

**IT IS ESSENTIAL TO PROVIDE CLEAR EXPLANATIONS OF AI SYSTEMS, ENSURE UNBIASED DECISION-MAKING, PROTECT USER DATA, AND ASSIGN RESPONSIBILITY FOR AI-DRIVEN ACTIONS**

**IAN WINFIELD, CHIEF TECHNOLOGY OFFICER, EMEA – AI AND HPC SOLUTIONS AT HITACHI VANTARA**



**Salman Mushtaq Qureshi**



**Wolfgang Kroj**



**Tahir Latif**

in shaping the future of technology.

The event underscored how the UAE and Saudi Arabia are leading the MENA region's digital transformation, shaping policies, investments, and initiatives that strengthen AI governance and cybersecurity. Both nations are at the forefront of AI adoption, with Saudi Arabia making strides under Vision 2030 and the UAE having launched its National AI Strategy 2031, aiming to become a global AI hub.

According to IDC, Saudi Arabia's ICT market spending exceeded \$36.6 billion in 2024, making it one of the fastest-growing digital economies in the world. AI investments alone surpassed \$720 million, with projections reaching \$1.9 billion by 2027. Meanwhile, the UAE has invested significantly in AI-driven industries, including smart cities, digital finance, and cybersecurity, with a staggering 70% of businesses in the region adopting AI in some capacity.

The KSA Executive Summit 2025 reinforced the joint commitment of Saudi Arabia and the UAE to accelerate technological innovation across the MENA region.

**Landmark event for digital governance**

The KSA Executive Summit provided a platform for industry leaders,



**Iain Winfield**

policymakers, and technology experts to address the ethical and security implications of AI.

With MENA's cybersecurity market projected to grow at a CAGR of 14.9% by 2028, discussions emphasized the critical role AI plays in proactively addressing evolving cyber risks. The AI adoption is growing and concerns around bias, data privacy, and

transparency have gained prominence.

**CPI Media Group's growing regional presence**

CPI Media Group's expansion into Saudi Arabia with the KSA Executive Summit marked a key milestone in its regional strategy. As a Dubai-based media powerhouse, CPI has a long-standing presence in the UAE, organizing flagship events in sectors such as technology, construction, and business intelligence. The successful launch of KSA Executive Summit 2025 signals CPI's long-term commitment to fostering digital dialogue and collaboration in Saudi Arabia and beyond.

Saudi Arabia and the UAE are accelerating digital transformation through strategic AI investments, cybersecurity initiatives, and regulatory advancements. According to Gartner, by 2026, 60% of Middle Eastern enterprises will fully integrate

**AI AND CYBERSECURITY ALWAYS COME BACK TO PEOPLE AND PROCESSES—IT'S ABOUT HOW WE INTEGRATE THESE TOOLS INTO OUR OVERALL FRAMEWORK**

**WOLFGANG KROJ, GENERAL MANAGER – SALES, MIDDLE EAST AND AFRICA, HITACHI VANTARA**

AI-driven cybersecurity measures, reflecting the growing reliance on AI for digital security.

As AI governance and cybersecurity remain central to regional policies, Saudi Arabia and the UAE's joint leadership in digital transformation will shape the future of technology in MENA. With platforms like the KSA Executive Summit, the two nations are paving the way for ethical AI implementation and robust cyber defense strategies.

A recent survey by global leader Sophos released this month – Kingdom of Saudi Arabia (KSA) Cybersecurity Awareness survey 2024 – revealed that rapid pace of innovation in the cybersecurity landscape makes it challenging for organizations to be prepared for evolving threats and implement cyber controls designed to counter them.

Larger organizations, 76% of the respondents with in-house expertise, are better equipped to manage risks, while smaller ones (21%) often lack the resources, making them more vulnerable to attacks. Thirty-five percent of the respondents stated that the most cited skill gaps are in AI/Machine Learning in cybersecurity followed by cloud security (25%). Across all organizations, quarterly training remains uncommon, with only 12% in medium organizations and 19% in large organizations adopting this frequency.

## KEY FINDINGS

- Phishing reports by employees: Organizations with more than 500 employees have the highest percentage of employees (15%) reporting phishing more than 50 times per month, likely due to advanced monitoring systems and employee training programs
- Organizations with ransomware plan: In organizations with over 500 employees, 89% have implemented a formal ransomware response and recovery plan, demonstrating strong preparedness and recognition of ransomware risks.
- Frequency of cybersecurity training: Small businesses are significantly less likely to provide training, with 61% of small organizations offering no training compared to 20% of medium-sized and just 2% of large organizations
- Budget allocation for cybersecurity from IT: Seventy percent of organizations with more than 500 employees allocate 13% or more of their IT budgets to cybersecurity, showcasing a significant prioritization of protecting complex infrastructures. Sixty-six percent of small organizations allocate less than 10% of their IT budgets to cybersecurity
- Compliance with local data policies: Larger organizations invest more in local compliance due to stricter audits, operational risks, and the sensitive nature of data they manage. Small organizations' preference for global data center policies may stem from cost-effectiveness, easier scalability and fewer regulatory burdens compared to larger counterparts.

"Today's threat landscape is continually evolving, growing more severe and complex, particularly in regions like Saudi Arabia, where digital transformation is rapidly advancing, there is an urgent need to heighten cybersecurity awareness and preparedness," said Chester Wisniewski, global field CTO at Sophos. "Cybercriminals operate without regard for international borders, and our

defenses must adapt accordingly. While ransomware attack rates have declined over the past two years, the impact on victims has increased. To combat these persistent threats, organizations in the Kingdom and beyond must adopt a proactive, human-led approach to threat detection and response, leveraging advanced technology and continuous monitoring to stay ahead of attackers."

As the MENA digital economy continues to thrive, events like the KSA Executive Summit will remain instrumental in driving innovation, regulatory progress, and cross-border collaboration between the UAE, Saudi Arabia, and the broader Middle East. CPI Media Group's expansion into Saudi Arabia is a testament to the growing demand for high-quality industry engagement and strategic insights. The success of the KSA Executive Summit has cemented CPI's position as a leader in technology-driven discussions across the Middle East. 📍

**"TODAY'S THREAT LANDSCAPE IS CONTINUALLY EVOLVING, GROWING MORE SEVERE AND COMPLEX, PARTICULARLY IN REGIONS LIKE SAUDI ARABIA, WHERE DIGITAL TRANSFORMATION IS RAPIDLY ADVANCING, THERE IS AN URGENT NEED TO HEIGHTEN CYBERSECURITY AWARENESS AND PREPAREDNESS,"**  
**CHESTER WISNIEWSKI, GLOBAL FIELD CTO AT SOPHOS**





## Smart Monitoring Solutions

Free Lifetime Video Recording

3 Year Warranty

Free Installation

Free after-sales service

# Keep an eye on your home even when you are away

With Ring Video Doorbells and Security Cameras, you can monitor every corner of your property.

**Starts at AED 20\***



For more information, look up Smart Monitoring at [www.etisalat.ae/smartmonitoring](http://www.etisalat.ae/smartmonitoring)

\*Terms and conditions apply





# LEAP 2025 SHATTERS RECORDS WITH US\$14.9 BILLION AI INVESTMENT, SOLIDIFYING SAUDI ARABIA'S TECH LEADERSHIP

WORLD'S PREMIER TECH ACCELERATOR  
EVENT UNVEILS GROUNDBREAKING  
AI INVESTMENTS, FUTURISTIC  
INNOVATIONS, AND A VISION FOR SAUDI  
ARABIA'S DIGITAL FUTURE.



**L**EAP 2025, the Kingdom’s flagship global tech event, has set a new benchmark for AI investment, announcing a record-breaking US\$14.9 billion in funding deals on its opening day. The monumental commitment underscores Saudi Arabia’s growing dominance as a global artificial intelligence (AI) hub, further advancing its Vision 2030 strategy.

Announced at the Riyadh International Exhibition and Convention Centre in Malham, these investments elevate the Kingdom’s total tech-related infrastructure investments beyond US\$42.4 billion since LEAP’s inception in 2022. Major agreements include a US\$1.5 billion partnership between Groq and Aramco Digital to expand AI-powered inference infrastructure and a US\$2 billion commitment from ALAT and Lenovo to

develop an advanced AI and robotics manufacturing hub. Additionally, Google, Qualcomm, Alibaba Cloud, and Databricks have all revealed major initiatives to boost AI adoption and digital infrastructure in the region.

Delivering a keynote address to inaugurate the event, His Excellency Eng. Abdullah Alswaha, Saudi Minister of Communications and Information Technology (MCIT), emphasized the Kingdom’s role in shaping the future of technology:

“LEAP 2025 is a defining moment because when the Kingdom works, the region works, and the whole world works,” said Alswaha. “Technology has catalyzed Saudi Arabia as the biggest success story in youth and female empowerment in the 21st century. The intelligence age is here, and in partnership with you, we are going to take that leap together.”

**Quantum Computing Breakthroughs and AI-Driven Innovations**

IBM Chairman & CEO Arvind Krishna, who joined Alswaha on the LEAP Main Stage, predicted that quantum computing—a technology set to revolutionize industries from energy and pharmaceuticals to oil and gas—is only “three to five years away” from a major breakthrough. “We’re very excited to already be working on it with some partners in the Kingdom,” Krishna added, hinting at significant Saudi collaborations in quantum research.

LEAP’s Tech Arena, a newly introduced feature at this year’s event, showcased futuristic innovations ranging from virtual boxing to wearable fashion tech. Aaron Sloan, Founder of Engine VR, demonstrated Golden Gloves VR, an AI-driven gamified boxing experience, while Adobe’s TJ Rhodes unveiled Project





Primrose, a groundbreaking smart dress that dynamically alters its design in real time.

"This technology is more than fashion; it's a canvas for new ideas," said Rhodes. "Imagine a world where what you wear reacts to your environment and emotions."

### Saudi Arabia's AI and Data Revolution Continues

The investment momentum carried over to Day Two, as NEOM and DataVolt announced a US\$5 billion deal to develop Saudi Arabia's first sustainable AI data center at Oxagon, the futuristic floating industrial city in the Red Sea. Mobily,

Zoom, and Saudi Arabia Railways (SAR) also unveiled major AI-driven infrastructure projects, reinforcing the Kingdom's ambition to lead in data, cloud computing, and non-terrestrial communications.

### Saudi Gaming Industry Witnesses Unprecedented Growth

Recognizing the US\$220 billion global gaming market, Saudi Arabia is leveraging LEAP 2025 to position itself as a digital entertainment powerhouse. The event saw the launch of the HGM Fund, a US\$300 million investment dedicated to developing Saudi-made video games, starting with WILCO, the Kingdom's first first-person shooter game.

Equinix, a global leader in digital infrastructure, also revealed a US\$1 billion investment in Saudi Arabia's largest data center, promising job creation and industry growth. Meanwhile, Accenture's Technology

**TECHNOLOGY HAS CATALYZED SAUDI ARABIA AS THE BIGGEST SUCCESS STORY IN YOUTH AND FEMALE EMPOWERMENT IN THE 21ST CENTURY. THE INTELLIGENCE AGE IS HERE, AND IN PARTNERSHIP WITH YOU, WE ARE GOING TO TAKE THAT LEAP TOGETHER"**  
**HIS EXCELLENCY ENG. ABDULLAH ALSWAHA, SAUDI MINISTER OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (MCIT**





Vision 2025 report unveiled at the event predicts a future where AI achieves unprecedented autonomy, transforming workplaces and enabling businesses to reinvent themselves at an accelerated pace.

**LEAP 2025 Closes with a US\$820 Million Economic Impact**

As the four-day event concluded, LEAP 2025 shattered records, welcoming 200,000+ industry professionals, 1,800 tech brands, and 1,900 investors with combined Assets Under Management (AUM) exceeding US\$22 trillion—a 400% increase from last year.

Michael Champion, CEO of event co-organizer Tahaluf, highlighted the economic impact of US\$820 million on Riyadh and Saudi Arabia, emphasizing the event’s role in solidifying the Kingdom as a global technology hub.

“Through our events since 2022, we have realized an economic impact of US\$10 billion, set to reach US\$20 billion by 2027,” said Champion. “We are also committing US\$80 million to keep Riyadh as the epicenter of future tech events for the next four years.”

Additionally, LEAP announced its global expansion with the launch of LEAP East, a new tech summit to be held in

Hong Kong in July 2026. The event aims to bridge Asian and Middle Eastern tech ecosystems, fostering deeper collaboration between global innovators.

**PwC, FIFA, and LaLiga Leaders on AI’s Expanding Role**

On the final day, PwC’s Global Chairman Mohamed Kande underscored the growing influence of AI in redefining industries, leadership, and even government operations. He stressed that AI adoption must be met with trust and transparency, warning that “people fear what they don’t understand.”

Meanwhile, Javier Tebas, President of LaLiga, outlined how AI is revolutionizing football, from preventing piracy to enhancing player performance. On LEAP’s Sports Tech stage, Ken Kutaragi, the father of PlayStation, reflected on his journey in gaming and predicted that AI will drive unprecedented industry growth.

With AI, sustainable data centers, and gaming investments at the forefront, LEAP 2025 has cemented Saudi Arabia’s reputation as a tech powerhouse and a global AI innovation hub. As the Kingdom marches towards Vision 2030, its unwavering commitment to digital transformation is set to redefine industries, empower youth, and shape the future of technology worldwide. 🚀







# CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD  
CLEANROOM™ RECOVERY



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



# GOVERNMENT AND PRIVATE ORGANIZATIONS COME TOGETHER TO ENHANCE CHILDREN'S DIGITAL WELLBEING

SNAPCHAT, META, GOOGLE, TIKTOK, X, YANGO, SAMSUNG, E& AND DU SIGN THE PACT

In line with the Year of Community, His Highness Lt. General Sheikh Saif bin Zayed Al Nahyan, Deputy Prime Minister, Minister of the Interior and Chairman of the Digital Wellbeing Council; H.E. Omar Sultan Al Olama, Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications, along with H.E. Sana bint Mohamed Suhail, Minister of Family

Affairs and ECA's Director General, witnessed the signing of the UAE Children's Digital Wellbeing Pact during the World Government Summit in Dubai.

Today, there are serious risks to children's online safety and wellbeing. More than two hours of screen time per day increases likelihood of higher blood pressure and Type 2 Diabetes in children. Moreover, ~33% of children in the UAE

reported being bullied online (2019). Within this context, the Pact is designed to protect children online and it will do this by promoting a safe and appropriate online environment, minimizing exposure of children to harmful content and protecting children from cyberbullying.

H.H. Sheikh Saif bin Zayed Al Nahyan said: "Protecting children in the digital world is a shared responsibility that

requires efforts between various sectors to ensure that we provide a space that balances freedom of access to information with ensuring the safety of children from electronic risks. More and more people are relying on technology in daily life so it has become necessary to establish clear frameworks and effective implementation mechanisms to protect children from harmful content and increasing digital challenges.”

His Highness added that signing the Children’s Digital Wellbeing Pact is in line with national efforts to promote a safe and balanced environment for children in the digital world, in line with the directives of the country’s leadership. The efforts are aimed at building a sustainable digital society that takes into account the needs of future generations.

The Pact, the first of its kind in the region, was facilitated by the Digital Wellbeing Council and the Abu Dhabi Early Childhood Authority, while the Office of International Affairs at the Ministry of Interior, the Telecommunications and Digital Government Regulatory Authority, the Artificial Intelligence, Digital Economy and Remote Work Applications office came onboard as strategic partners for the Pact. Moreover, numerous technology and content platforms,

social media channels, internet and telecommunications service providers also came together and became members of the Pact. They are Snapchat (leading member of the pact for its first year), Meta, Google, TikTok, X, Yango, Samsung, e& and du.

H.H. Sheikh Theyab bin Mohamed bin Zayed Al Nahyan, Chairman of Office of Development and Martyrs Families Affairs and Chairman of the Abu Dhabi Early Childhood Authority, said: “Protecting children and boosting their digital quality of life is a priority to us. Ensuring children’s safety and well-being online directly contributes to building a secure and prosperous society that leverages technology positively. By providing a safe and stimulating digital environment that gives children access to information and educational resources securely, we empower them with greater opportunities to learn and innovate, away from risks associated with the misuse of technology.”

Jawaher Abdelhamid, Regional Head of Public Policy for the Middle East and Africa at Snap Inc., said: “At Snap, we share a deep responsibility to continually strive toward creating a safe experience for our users – particularly the youngest ones. As a reflection of this commitment, we feel proud to undertake a leading role

in the development and execution of the UAE’s first Children’s Digital Wellbeing Pact and look forward to engaging meaningfully with governments, partners and parents on prioritizing the safety and privacy of young Snapchatters in the UAE.”

By developing clear mechanisms to protect children from physical and psychological harm, as well as enhancing supervision of digital content targeting them, the Pact will enhance collaboration among various partners to ensure the highest standards of digital safety for children. The Pact also protects children’s data, ensuring their privacy and safety within the digital ecosystem. This includes promoting transparency through continuous reporting and evaluation mechanisms according to global leading practices. It also focuses on developing effective strategies to reduce the promotion of harmful content, taking into account different age groups.

Moreover, the Pact will support digital literacy programs and educational initiatives that equip children and their parents with the needed skills to browse safely online. The Pact will also facilitate the exchange of expertise and investment in research, to address the emerging risks posed by technological advancements. Finally, the Pact supports exchanging information on advanced technological methods that contribute to providing a safer online environment for children. This includes developing and using effective tools to verify the user’s age before displaying content, establishing leading practices and strategies to enhance user privacy protection, with a particular focus on children’s data, and ensuring full compliance with relevant data protection regulations. It also includes identifying incident response mechanisms and reporting protocols to address emerging cyber threats and immediately manage incidents affecting children. In addition, the Pact will help strengthen efforts to develop policies that enhance children’s digital quality of life. [🔗](#)

**“PROTECTING CHILDREN IN THE DIGITAL WORLD IS A SHARED RESPONSIBILITY THAT REQUIRES EFFORTS BETWEEN VARIOUS SECTORS TO ENSURE THAT WE PROVIDE A SPACE THAT BALANCES FREEDOM OF ACCESS TO INFORMATION WITH ENSURING THE SAFETY OF CHILDREN FROM ELECTRONIC RISKS”**

***SHEIKH SAIF BIN ZAYED AL NAHYAN  
DEPUTY PRIME MINISTER, MINISTER OF THE  
INTERIOR AND CHAIRMAN OF THE DIGITAL  
WELLBEING COUNCIL***





# UAE AMONG TOP 10 COUNTRIES WITH MOST AI COMPANIES PER MILLION POPULATION, GLOBAL AI COMPETITIVENESS INDEX

**SINGAPORE, UAE, AND HONG KONG LEAD GLOBAL AI ENTERPRISE DENSITY RANKINGS**

The UAE has achieved a remarkable position among the top 10 countries with the most AI companies per million population, as revealed in the Global AI Competitiveness Index.

The report, a collaborative effort between the International Finance Forum (IFF) and Deep Knowledge Group, analyzed over 55,000 AI companies worldwide to evaluate the density, financing, and development of AI enterprises globally.

Highlighting its growing prominence in AI enterprise density, the UAE stands alongside innovation hubs such as Singapore and Hong Kong. This milestone reflects the UAE's strategic vision to become a global leader in AI, driven by progressive policies, robust infrastructure, and targeted investments.

Dmitry Kaminskiy, General Partner of Deep Knowledge Group stated: "The UAE's ranking among the top 10 countries for AI companies per capita demonstrates how targeted investments are creating an ecosystem where AI innovation thrives. This is a blueprint for how nations can transform strategic vision into measurable impact."

## Government strategic support and investment

The UAE has consistently demonstrated its commitment to AI at the highest levels. In 2017, the UAE became the first nation to appoint an AI Minister, a groundbreaking move to embed AI at the core of its national strategy. The government's AI Strategy 2031 aims to contribute Dh335 billion (USD 91 billion) to GDP by 2031 and reduce operational costs by 50% through AI innovation.

The UAE has also established the Dh10 billion (\$2.7 billion) Dubai Future Accelerator Fund to support AI innovation projects. Complementing this is the nation's business-friendly environment and zero personal income tax.

Rank	Country/region	Number of enterprises million in population
1	Singapore	162.8
2	Israel	135.2
3	Switzerland	73.6
4	US	61.2
5	Canada	58.3
6	UK	56.5
7	Ireland	50.8
8	Finland	50.0
9	UAE	49.5
10	Hong Kong, China	47.1

#### Talent attraction and development

To support its AI ambitions, the UAE is rapidly building a talent pipeline. Key initiatives include the Golden Visa program, offering 10-year residency to AI professionals, and the establishment of the Mohamed bin Zayed University of Artificial Intelligence (MBZUAI), the world’s first dedicated AI research university. Partnerships with top global universities have further enhanced the UAE’s AI research capabilities, supported by high-value scholarships and advanced research funding. As a

result, the UAE boasts an annual AI talent growth rate of 30%.

#### Infrastructure excellence

The UAE’s world-class digital infrastructure underpins its leadership in AI innovation. With over 90% 5G network coverage, 97.1% internet penetration, and the largest data center cluster in the Middle East, the nation provides an unparalleled environment for AI companies to thrive. Its well-developed smart city infrastructure offers the perfect testing ground for cutting-edge AI applications.

#### UAE’s AI success story: G42

Abu Dhabi-based G42 is a shining example of the UAE’s AI prowess. Specializing in healthcare, finance, and smart city solutions, G42 has become a global leader in AI innovation. In 2024, Microsoft invested \$1.5 billion into the company, forming a partnership to establish AI research institutes in Abu Dhabi to develop “responsible” AI.

G42 also introduced Jais, an open-source Arabic AI language model with 30 billion parameters. Trained on extensive Arabic data and English computer code, Jais highlights G42’s contributions to advancing AI in the region. Currently valued at over \$10 billion, G42 embodies the UAE’s vision of becoming a global AI hub.

With its strategic initiatives, investments, and infrastructure, the UAE is well-positioned to lead the global AI revolution. The Global AI Competitiveness Index highlights the country’s impressive progress and underscores its dedication to shaping a future where AI is a driving force for innovation and economic growth. 📌

**“THE UAE’S RANKING AMONG THE TOP 10 COUNTRIES FOR AI COMPANIES PER CAPITA DEMONSTRATES HOW TARGETED INVESTMENTS ARE CREATING AN ECOSYSTEM WHERE AI INNOVATION THRIVES.”**

***DMITRY KAMINSKIY, GENERAL PARTNER OF DEEP KNOWLEDGE GROUP***



# HUB71 STRENGTHENS ABU DHABI'S THRIVING TECH ECOSYSTEM WITH ITS LATEST COHORT

**C**OHORT 16 STARTUPS HAVE RAISED OVER \$ 145 MILLION (DH532 MILLION), WITH 63 PER CENT OF SELECTED STARTUPS HEADQUARTERED OUTSIDE THE UAE, REINFORCING HUB71'S SUCCESS IN ATTRACTING HIGH-GROWTH INTERNATIONAL STARTUPS

**H**ub71, Abu Dhabi's global tech ecosystem, has welcomed 27 startups as part of Cohort 16 across Hub71's three programs, Access, Hub71+ ClimateTech and Hub71+ Digital Assets. This new addition increases the total number of ventures supported by Hub71 to 357.

The latest cohort includes startups across key priority sectors, reinforcing Hub71's commitment to diversifying Abu Dhabi's economy through technology and innovation.

Collectively, Cohort 16 startups have raised over \$145 million (Dh532 million) in funding, averaging \$4.9 (Dh18 million) million per startup. This achievement

reflects Hub71's track record in attracting high-potential companies that advance technological innovation across Abu Dhabi's priority sectors. By joining Hub71, these startups are establishing their operations in Abu Dhabi, gaining access to a robust network of capital, mentorship, and resources to scale their businesses and drive impactful growth.





Cohort 16 was selected from over 1,300 applications, with 63% of chosen startups headquartered in leading technology markets such as the USA, UK and Germany. Among the notable additions to Hub71's Access program is Vivan Therapeutics, a UK-based precision medicine company pioneering cancer research, using AI and fruit fly models to identify personalized treatments, that has raised \$ 10 million (Dh36 million) in funding.

Meanwhile, Theion, a German startup developing sustainable sulfur-based batteries that store up to three times more energy than traditional batteries will join the Hub71+ ClimateTech program. South Korean startup Redbrick, a cloud-based 3D creation engine that uses AI and blockchain, has raised \$ 16.3 million (Dh59.8 million) in funding and will join the Hub71+ Digital Assets program.

Furthermore, one in three startups

in the cohort is based in the UAE, showcasing the nation's growing status as a global entrepreneurship hub. Notable homegrown startups include Qashio, an award-winning spend management platform that has raised \$ 10 million (Dh 36 million), and Switch Foods, a FoodTech company offering locally produced, affordable plant-based meats. Switch Foods has raised \$ 12.5 million (Dh45.9 million) and launched Abu Dhabi's first plant-based meat production facility, setting a new standard for sustainable food innovation.

Ahmad Ali Alwan, CEO of Hub71, said: "Cohort 16 reinforces the global confidence in Hub71 as a launchpad for transformative ideas from Abu Dhabi. The selection process is highly competitive, reflecting the exceptional caliber of startups in our ecosystem. These companies are advancing innovation across key tech sectors while strengthening Abu Dhabi's position as a

global tech hub."

Additionally, more than half of Cohort 16 consists of Seed and Series A startups. The selected startups operate in nine sectors including FinTech, ClimateTech, HealthTech, EdTech, and Mobility & Logistics, and will play a crucial role in driving the growth of Abu Dhabi's economy.

By joining Hub71 "Access" and Hub71+ programs, startups will be able to tap into a vibrant community of mentors, partners, and investors within Abu Dhabi's technology ecosystem. Gaining access to market opportunities, top talent, and capital significantly enhances startups' prospects of securing commercial deals, attracting investment, and driving market growth.

#### Optional

The 27 startups selected to join Hub71's Cohort 16 include:

#### Access Program

1. Aurem is a central operating system for workplace saving and wealth providers —optimising operations and innovating products in a single configurable platform.
2. Cambio ML provides the "AI data science agent" for enterprises, aggregating and cleaning messy data from data silos.
3. Desert Farms is a science-backed D2C product using camel milk proteins to make a near-identical baby formula to breastmilk.
4. Esports XO connects gamers with tournaments and new games while helping publishers distribute games and telecoms build engaged communities.
5. Fundbot Technologies is a B2B supply chain financing solution that enables banks, buyers, and sellers to connect automating lending and payments.
6. Hotdesk is the Airbnb for Offices, with 2,000+ spaces in 73+ countries. They provide an all-in-one platform offering workspace optimization and hybrid work management software

to help coworking spaces and corporates navigate the future of work.

7. Mithryl's AI platform helps industrial companies automate processes by unifying fragmented systems into context-aware workflows that drive faster, smarter decisions.
8. Nodeshift is a decentralized, no-code AI cloud platform that enables one-click deployment of AI agents and LLMs, providing secure, private, and affordable compute without centralized control or complexity.
9. Onloop an applied AI lab, obsesses over team productivity - powering effortless goal alignment and feedback systems for managers while augmenting human capabilities through mobile-native, agentic workflows.
10. Qashio is a B2B financial management platform offering advanced expense management, customizable SaaS tools, and reward program.
11. Raintech is an operating room voice assistant that improves the quality of care and surgical outcomes by enabling clinicians to focus on patients rather than documentation and admin tasks.
12. Simpleem is Behavior-Analysis AI that predicts human actions with unmatched accuracy and provides tailored guidance on leveraging behavior to improve concrete business outcomes.
13. Skipr is a sovereign agent-centric VPN that delivers the next generation of privacy and security in the age of AI.
14. Taxo integrates with electronic health records (EHRs) to automate medical billing and coding. Its AI-powered solution reduces the time and cost of claims processing by >90%, enabling providers to focus on patient care rather than administrative tasks.
15. Vivan Therapeutics' TuMatch software leverages a proprietary data set and AI/ML to enable rapid, personalized cancer treatment direction.



16. Watermelon Ecosystem is an all-in-one platform that connects F&B suppliers with outlets through a marketplace and procurement system.
17. xMap is a platform that uses AI to transform geospatial data, such as maps, satellite images, and GPS information, into real-time insights for businesses.

**Hub71+ ClimateTech**

1. Airmo delivers actionable, accurate, real-time methane insights and environmental intelligence to the energy sector, regulators, and impact investors.
2. New Path Bio uses precision fermentation to produce nutritious, health-promoting proteins from microbes, eliminating the need for animals, land, water, or climate dependence.
3. Orbillion Bio is a B2B cultivated beef company making tasty, non-GMO beef at commercial scale and cost parity by leveraging advanced computational models and strategic partners.
4. SwitchFoods is a FoodTech startup focused on innovating and producing deliciously healthy, nutritious, and sustainable plant-based meat alternatives tailored to regional

tastes and cooking habits.

5. Theion is a company that develops sustainable sulfur-based batteries that are eco-friendly, cost-effective, and store up to three times more energy than traditional batteries.

**Hub71+ Digital Assets**

1. InvoiceMate is a Blockchain & AI powered platform bridging conventional businesses with crypto liquidity.
2. Redbrick is a cloud-based game and metaverse engine using blockchain and AI to streamline creation and distribution for all skill levels.
3. Rilla Network is a decentralized infrastructure that unlocks the hidden potential of live streaming ecosystems while delivering exponential savings.
4. Sustainable Bitcoin Protocol enables institutional investors to embed verifiable clean energy into their Bitcoin holdings—transforming Bitcoin's distributed energy demand into a catalyst for the global energy transition.
5. 1Money is developing the world's first payment network exclusively designed for stablecoins, and specifically engineered to be the fastest, cheapest, and most compliant. 🔑



# LEAP

09-12 FEBRUARY 2025  
RIYADH, SAUDI ARABIA

# INTO NEW WORLDS

**680+**  
start-ups

**1,000**  
speakers

**1,800+**  
global tech  
brands

**170,000+**  
global attendees

Step into what's next. Secure your ticket now  
[www.onegiantleap.com](http://www.onegiantleap.com)

Co-organised by:



وزارة الاتصالات  
وتقنية المعلومات  
MINISTRY OF COMMUNICATIONS  
AND INFORMATION TECHNOLOGY



الاتحاد السعودي للأمن  
السيبراني والبرمجة والدرز  
SAUDI FEDERATION FOR CYBERSECURITY,  
PROGRAMMING & DRONES

tahajuf  
an  
informa  
company  
تجلف



# LOVE IN THE TIME OF AI — UNVEILING THE DARK SIDE OF DIGITAL ROMANCE

STAY VIGILANT AS ROMANCE SCAMS PEAK DURING VALENTINE'S — SECURE YOUR ONLINE LOVE AND SHOPPING THIS FEBRUARY

People are often blinded by love, but let it not blind you to the extent that you overlook red flags while making online purchases or shopping digitally on Valentine's Day or in month of February.

The surge in e-commerce activity attracts cybercriminals with scams such as phishing, counterfeit websites, and offers that seem too good to be true. It's crucial to verify the authenticity of websites, utilize secure payment methods, and restrict the personal information you share. Always check for reviews and ensure the website uses HTTPS for secure transactions. Being cautious of unsolicited emails and messages is essential to protect your identity and finances during this high-spend period.

## Scams are stealing hearts and bank accounts

Be cautious not to "swipe right" into a scam as Valentine's Day approaches. Researchers at Tenable Inc., the exposure management company, warn that romance scams continue to be the biggest consumer threat today.

"Many of these scammers operate from overseas and don't speak fluent English," said Satnam Narang, senior staff research engineer at Tenable. "AI helps them craft sophisticated, emotionally compelling messages that make their scams more believable and harder to detect."

Romance scams affect people of all ages and backgrounds, but elderly individuals, former military personnel, and those seeking financial arrangements are among the most vulnerable. Scammers deploy various tactics, from impersonating service members using stolen photos to orchestrating fake "sugar mummy and daddy" schemes, luring victims into fraudulent financial transactions. Others entice victims into adult video chats that require paid registrations, generating illicit profits in the process.

The most dangerous form of romance scam today is 'romance baiting,' previously known as pig butchering. In these long-term cons, scammers establish fake relationships to build trust before convincing their victims to invest in bogus cryptocurrency or stock platforms. This method has now overtaken other romance scams in terms of prevalence and financial impact.

"People have lost their life savings to romance scams, and it's heartbreaking," said Narang. "Victims are often blamed for falling for these schemes, but these scams are highly manipulative and exploit vulnerabilities that anyone could have."

Recovering stolen funds is notoriously difficult, particularly when cryptocurrency is involved. To make matters worse, scammers often double down by targeting victims again, posing as recovery agents who promise to retrieve lost funds—for a fee.

Garth Braithwaite, GM Emerging Markets at Gigamon, said: "Too often, we rely on big tech to handle security alone, but staying safe online is a shared responsibility. Each of us must stay alert: cybercriminals devote every moment to finding new ways to breach defenses, especially with the help of generative AI. We can't expect corporate training alone to solve this. People outside office walls rarely see such guidance, leaving many of them exposed. In a world where AI fuels sophisticated romance scams, how are tech companies using it to bolster dating platforms and shield users from new threats? Ultimately, personal awareness is as vital as any company measure."

## Top Technologies Hackers Would 'Love' to Target in 2025

Positive Technologies recently revealed the results of an analytical study into the key technology trends of 2024 and their projected impact on security.

With Valentine's Day approaching, their experts identified five key areas that are driving technological advances or "love interests" cybercriminals can't wait to woo.

### Artificial intelligence (AI)

Positive Technologies predicts that the use of AI in cyberattacks will increase in 2025: AI will be used more frequently in vulnerability scanning tools, data analysis, text recognition, and social engineering tactics.

### Blockchain and digital assets

In 2025, attacks on cryptocurrency holders are expected to increase, with new ways to trick users. Scams to steal digital currencies will become more common, making it harder to protect funds. Fraud schemes involving digital currencies aimed at stealing funds will also become widespread.

### Internet of Things (IoT)

By 2025, the number of attacks on consumer and commercial IoT systems is expected to increase significantly, affecting everything from individual homes to entire cities.

### Cloud technologies

The analysts predict that in 2025, cybercriminals will increasingly target cloud solutions for data theft and extortion. In September, Microsoft researchers reported an attack that compromised hybrid cloud environments. This campaign resulted in data exfiltration, persistent access to the affected infrastructure, and ransomware deployment. It targeted multiple sectors, including government, manufacturing, and transportation.



### Autonomous vehicles

The digitalization of transportation systems is advancing rapidly: the market for autonomous vehicles will grow sixfold by 2032. At the same time, cyberattacks exploiting vulnerabilities in autopilots, sensors, and IoT gateways are on the rise. As we move forward in 2025,

software developers and IT companies are becoming primary targets of attacks.

“This year the effects of software supply chain attacks will likely become more apparent. In attacks on IT companies, we may see a rise in successful incidents, with attackers using compromised developer credentials for initial access. Supply chain attacks continue to be an acute challenge. According to our review of incident investigations, the proportion of attacks where a compromised contractor’s network was used to gain initial access to a target organization has increased from isolated incidents (in 2021–2023) to 15% of all attacks in 2024,” said Ekaterina Snegireva, Senior Analyst at Positive Technologies.

Much of the protection of legitimate users of dating applications comes in the form of warnings suggesting they be mindful if a potential match may intend to scam them, showing a warning once at the start of a conversation thread providing resources on how to spot a potential scam forming.

Aaron Bugal, Field CTO APJ, Sophos, said: “Given that many of these initial conversations are short with the scammer urging the victim to move off



the dating platform – where protections could be applied – and onto messaging platforms uncontrollable by the dating application provider is a key telltale sign that something isn't right, and the user should exercise more caution around who they may be talking with. As such, AI could be adopted to help spot those initial 'lustful lures' on dating applications, especially around this time of year to help detect and weed out fraudulent matches – however, with many legitimate people looking for love and needing to put their best foot forward with a witty and catchy line, could be considered an unwanted advanced by the AI."

With romance scams becoming more sophisticated due to generative AI, tech companies are leveraging AI to enhance safety on dating platforms. AI-driven profile verification, such as video selfie checks, ensures authenticity and reduces fake accounts.

Ezzeldin Hussein, Regional Senior Director, Solution Engineering, SentinelOne, said: "Deepfake detection tools help identify AI-generated images and videos used for deception. AI-powered content moderation analyzes interactions in real-time, flagging suspicious behavior

and preventing scams before they escalate. Platforms also use machine learning algorithms to detect scam-like conversation patterns, alerting users to potential risks. Additionally, companies focus on user education, warning about AI-driven scams and encouraging vigilance. Security firms

provide AI-powered scam detection tools to assess communication authenticity. By integrating these AI safety measures, dating platforms aim to safeguard users from fraudsters exploiting AI for deception, making online dating safer in an era where digital impersonation is becoming increasingly advanced."

Research highlights the rise of AI-driven scams using chatbots and deepfake technology, urging vigilance and offering guidelines to identify fraud. AI-powered tools are being developed to detect scam patterns in messages, alerting users to potential threats. Reverse image search tools help verify online identities, reducing the risk of deception. Awareness campaigns share real scam cases to help users recognize warning signs. Educational content, scam detection tools, and real-time alerts are being integrated to equip users with the knowledge and resources to protect themselves. By promoting digital skepticism and safe online practices, these initiatives aim to prevent fraudsters from exploiting emotions and financial trust in online interactions.

Burcak Soydan, Managing Executive for Middle East at NTT DATA MEA, said: "NTT DATA is actively addressing the surge in





AI-driven fraud, including romance scams, by implementing several key initiatives. NTT DATA emphasizes the importance of user education in combating AI-enhanced scams. They advocate for increased awareness about the sophisticated tactics employed by fraudsters, such as the use of AI to create convincing fake profiles and communications.”

Soydan informed that recognizing the dual role of AI in both perpetrating and preventing scams, NTT DATA promotes the use of Explainable AI. XAI enhances transparency by making AI models more interpretable and accountable, allowing users to understand how AI systems arrive at their decisions. This approach helps in identifying and mitigating biases, thereby reducing the risk of AI being exploited for fraudulent activities.

Dating platforms are integrating advanced machine learning algorithms to detect fraudulent activities. These AI systems analyze user behavior, flagging patterns commonly associated with scams—such as rapid expressions of affection, inconsistencies in shared information, and requests for financial assistance. Natural language processing (NLP) tools

help identify scam-related conversations, triggering alerts when suspicious phrases or requests appear in messages.

Ram Vaidyanathan, Chief IT Security Evangelist, ManageEngine, said: “To combat AI-generated deepfake images and fake profiles, many platforms have implemented facial recognition and image verification technologies. Some require

users to submit short selfie videos for verification, ensuring that the person behind a profile is real. Additionally, multi-factor authentication (MFA) and ID verification have become standard security features, making it harder for scammers to operate undetected.”

#### **User education and awareness**

While AI helps detect scams, educating users remains critical. Dating platforms are launching awareness campaigns, particularly around high-risk periods like Valentine’s Day. In-app warnings, emails, and notifications inform users about common scam tactics, such as sudden financial requests, reluctance to meet via video calls, and inconsistencies in personal stories.

“Many platforms also partner with cybersecurity firms to provide educational resources, including articles, webinars, and interactive quizzes that teach users how to verify identities and recognize red flags. Some apps display real-time safety prompts during conversations, cautioning users if their chat includes suspicious elements. By combining AI-powered fraud detection with proactive user education, dating platforms are can create safer online spaces,” said Vaidyanathan. 📌





Yiyi Miao, Chief Product Officer at OPSWAT

# TO TAME CHAOS OF OUR DIGITAL ENVIRONMENTS, WE MUST SECURE THE ENTIRE SOFTWARE DEVELOPMENT LIFECYCLE

The United Arab Emirates' economic Vision programs have long been seen as roadmaps to a digital future. Even where government

guidelines and whitepapers do not explicitly mention technology, their ambitious goals imply it. The closer we get to Vision 2030's "due date", the more anxious decision makers will be to take control of their digital destinies — to respond with agility and to the expectations of markets and regulators. In doing so, many enterprises will turn to in-house DevOps teams to build their digital experience suites. In theory, that is the only way they can deliver for both consumers and regulators.

It is in that tug-of-war between the desire of customers for superlative experiences and the insistence of regulators on secure workflows, that organizations face their most difficult challenges. Every speedy rollout has the potential to expose the business to vulnerabilities; and every security issue addressed has the potential to complicate workflows for employees and customers. The guiding principle in trying to walk this line is to secure the entire software development lifecycle (SDLC) by performing a left-shift in security strategy — bringing security considerations into earlier SDLC phases — and subsequently ensuring that vulnerability management remains part of every phase of software development thereafter.

If UAE DevOps teams can identify and mitigate threats all the way along the lifecycle, they will have achieved proactive protection, which is a hallmark of cyber-maturity. If they can minimize potential threats while saving time and resources, they will have discovered a recipe for thriving in the digital economy. To get the balance right, we must begin with clear definitions of what new solutions and updates will do, so we can embed best-practice security provisions as implementation gets underway. Frameworks like the Software

Assurance Maturity Model (SAMM) can act as a strong foundation for security and development professionals to collaborate closely on the assessment of business risks associated with software vulnerabilities.

Following these practices, in which security is considered a core ingredient rather than icing on the cake, is a strong start. Software testers must still formulate their scripts in a security-conscious way. Penetration testing and dynamic application security testing (DAST), accompanied by code reviews, can help ensure vulnerabilities have nowhere to hide in the later stages of the cycle. Even when green lights are given, the live production environment must be monitored for any emerging threats.

Security-focused DevOps teams do not have to invent methods from scratch to institute best practices. The tools are already available. Software composition analysis (SCA) and static application security testing (SAST) can automate vulnerability detection by scanning source code and libraries for issues. Tools like PyTM (pythonic threat modeling) and ThreatSpec can even model threats at the design phase; and the Security Knowledge Framework is designed to help developers and software architects think like attackers even if they are not well-versed in cyber security. This is useful in a region that continues to face cybersecurity skills gaps.

These are critical capabilities in the

shift-left approach to DevOps security because of the complexity and expense of ad-hoc remediation. If left to later stages, some vulnerabilities may not be candidates for simple patching and may require months of workshopping and redesign to address. But if security is integrated into the heart of every project, the organization's overall security posture benefits. Not only will it be able to more easily satisfy UAE regulators; it will live up to international standards like ISO 27001. This has lasting, positive implications for its market reputation, especially in industries like finance and healthcare where slips in customer confidence can mean the end of a brand.

#### Supply-chain rein

Keeping a tight rein on the SDLC by treating it as an interconnected whole is a critical step in addressing one particular cyber threat — the supply-chain attack. While some of the more famous examples like SolarWinds and NotPetya lie outside the region, the UAE and GCC have historically presented tempting targets to threat actors, so organizations here must remain cyber-mature to avoid the derailment of economic progress. DevOps teams rely on a supply-chain of third-party open-source libraries. As mentioned previously, tools exist to automatically scan libraries as part of source-code review. Additionally, the Open Web Application Security Project (OWASP) provides an industry-standard

guide specifically for the SDLC. Helpful tips include lists of known vulnerabilities, outdated software, and license risks.

Beyond process and best practice, we must take a look at threat intelligence because it is here that DevOps teams will differentiate themselves in cyber-maturity. Continuous training in high-profile threats will allow them to make better decisions while building applications. They should be aware of Log4Shell, which allows nefarious actors to remotely execute code through a vulnerability in Apache Log4j. Millions of attempts have been made by shadowy groups to compromise the millions of applications and devices exposed to this flaw; and it persists in the wild despite multiple patches from Apache.

Vulnerabilities can even be found in code-parsing tools and deployment suites. Development teams must make good use of code patterns, linters, and testing solutions to ensure code quality. They must include security checks through resources such as tslint or OWASP Dependency-Check. For extra quality assurance, team leaders should consider peer reviews, pre-commit hooks, and automated testing; they should implement formal tracking of third-party libraries; and they should use both automated and manual testing, and pentests, and adopt tools like ZAP for automated Web-attack detection. During release, DevOps teams should review configurations for security flaws, and employ tools like Open Policy Agent, ELK stack, and Prometheus to ensure secure deployment.

#### Taming The Chaos

Vigilance should be the default state of every digital business, and we are now firmly in an era where every business is digital. To please both markets and regulators, enterprises can no longer afford to deploy applications like setting free wild horses. They must tame the experience or risk a fatal hit to their brand. 🐾

**“SECURITY-FOCUSED DEVOPS TEAMS DO NOT HAVE TO INVENT METHODS FROM SCRATCH TO INSTITUTE BEST PRACTICES. THE TOOLS ARE ALREADY AVAILABLE. SOFTWARE COMPOSITION ANALYSIS (SCA) AND STATIC APPLICATION SECURITY TESTING (SAST) CAN AUTOMATE VULNERABILITY DETECTION BY SCANNING SOURCE CODE AND LIBRARIES FOR ISSUES”**



# MITIGATING RANSOMWARE DAMAGE: KEY STEPS FOR CYBER RESILIENCE

**D**eveloping and maintaining an effective incident response plan is essential for mitigating ransomware attacks. This plan outlines roles, responsibilities, and protocols to ensure coordinated action across the organisation. Regular testing through tabletop exercises helps validate the plan's effectiveness and adapt it to evolving threats.

The Middle East has become a prime target for cybercriminals, with ransomware attacks escalating sharply. In the first half of 2024 alone, 45 incidents were reported, approaching the total of 63 incidents recorded throughout the previous year. This significant rise reflects the increasing vulnerability of the region to such attacks. Halcyon emphasizes that a comprehensive plan, along with rigorous testing of recovery procedures, helps organisations strengthen their resilience and ensure swift recovery during cyber incidents.

40% of technology leaders place data protection as the leading investment priority. However awareness of the possibility of attacks is not a guarantee of protection. Half of the 78% of business leaders who claimed their organisations were prepared for attacks still fell victim to ransomware.

## **The Foundation: Incident Response Planning**

Developing and maintaining an effective incident response plan is the cornerstone of mitigating ransomware attacks. Such a plan outlines the roles, responsibilities, and protocols for



**Ray Kafity, Vice President – META at Halcyon**



addressing cybersecurity incidents, ensuring coordinated action across the organisation. Regular testing through tabletop exercises and simulations is essential to validate the plan's effectiveness and identify areas for improvement.

A well-executed incident response plan addresses the following:

- Rapid threat detection and containment.
- Efficient communication among internal teams and external stakeholders.
- Seamless coordination between security, IT, and leadership teams.

By prioritizing regular assessments and updates, organisations can minimize delays and disruptions during actual incidents.

### Key Metrics to Enhance Cyber Resilience

Understanding and optimising critical metrics can significantly improve an organisation's ability to prevent, detect, and respond to ransomware attacks. Here are some essential metrics to monitor:

#### 1. Mean Time to Detect (MTTD)

MTTD measures the average time required to identify a cyber threat. A lower MTTD reflects superior detection capabilities, enabling organisations to recognise anomalies and indicators of compromise (IoCs) promptly. Monitoring and reducing MTTD provides several benefits:

- Prevents attackers from establishing a foothold and moving laterally within the network.
- Highlights the efficiency of Security Information and Event Management (SIEM) systems and security teams.

To achieve a lower MTTD, organisations should:

- Continuously refine detection tools and processes.
- Invest in advanced monitoring technologies.
- Conduct regular personnel training to enhance threat recognition.

#### 2. Mean Time to Respond (MTTR)

MTTR gauges the average time taken to neutralise or mitigate a detected threat.

A lower MTTR ensures that incidents are swiftly contained, reducing potential business disruptions. Organisations can enhance their MTTR by:

- Conducting incident response tabletop exercises to refine protocols.
- Reviewing lessons learned from past incidents to improve strategies.
- Implementing automated response tools for faster threat mitigation.

**40%**  
Technology leaders place data protection as the leading investment priority

#### 3. Incident Response Plan Effectiveness

The true test of an incident response plan lies in its execution during a cyber event. Key indicators of effectiveness include:

- Speed of threat containment.
- Efficiency of communication and coordination.
- Successful execution of recovery procedures.

Regular testing and updates ensure the plan remains relevant and actionable. Organisations should measure the plan's performance during simulations

and real incidents to drive continuous improvement.

**Strengthening the Human Element**

Cybersecurity is not solely about technology; human factors play a pivotal role in defending against threats. Effective training and awareness programs are essential to reducing the risk of human error in cyber incidents.

**1. Role-Based Training**

Training programs should be tailored to the specific responsibilities of different roles within the organisation. For example:

- Software developers require training in secure coding practices.
- Financial executives need awareness of phishing and social engineering tactics.

Tracking metrics such as training completion rates and performance in simulated phishing exercises helps measure program effectiveness.

**2. Cyber Hygiene**

Maintaining robust cyber hygiene is foundational to cybersecurity resilience. Key practices include:

- Regular patch management to address vulnerabilities.
- Continuous vulnerability scanning to identify and remediate risks.
- Adherence to security policies to prevent misconfigurations.

Organisations should establish a strong cyber hygiene framework before investing in advanced technologies, as it serves as the first line of defense against many types of attacks.

**Evaluating and Managing Risk**

The average cost of a data breach in the Middle East region is SAR 29.9 million. It's bound to become more expansive. This is why mitigating cyber is quite essential now. Also, understanding and



managing cyber risk exposure is critical to effective resource allocation and threat mitigation. Organisations should:

- Conduct regular risk assessments to identify high-value assets and vulnerabilities.
- Prioritize mitigation strategies based on the most significant risks.
- Monitor third-party risks to ensure vendors and partners adhere to security best practices.

By quantifying and addressing risk exposure, organisations can focus on protecting their most critical systems and data.

**Optimising Security Controls and Recovery Protocols**

**1. Security Controls Effectiveness**

Organisations must regularly assess the performance of their security controls, such as firewalls, intrusion detection systems (IDS), and malware detection tools. Metrics to monitor include:

- Number of alerts generated by IDS/IPS systems.
- Efficacy of firewall rules.
- Success rates of malware detection.

Continuous evaluation and adjustment based on threat intelligence ensure optimal defense capabilities.

**2. Backup and Recovery Metrics**

Backup and recovery processes ensure data availability during a ransomware attack. Key metrics include:

- Backup success rates.
- Recovery Time Objectives (RTO).
- Recovery Point Objectives (RPO).

Regular testing of backup systems ensures they meet business continuity requirements and can be relied upon during a crisis.

**3. Business Continuity and Disaster Recovery (BCDR)**

Measuring the effectiveness of BCDR plans is crucial for maintaining operations during and after a cyber incident. Regular testing and scenario simulations validate the plans' feasibility and identify areas for improvement. Seamless integration of disaster recovery and business continuity strategies ensures organisational resilience.

Mitigating the potential damage from a ransomware attack requires a holistic approach that combines robust planning, effective training, and continuous improvement of key metrics. Organisations can strengthen their defenses against ransomware by developing a comprehensive incident response plan, enhancing detection and response capabilities, and prioritizing cyber hygiene. 🔒

**A COMPREHENSIVE PLAN, ALONG WITH RIGOROUS TESTING OF RECOVERY PROCEDURES, HELPS ORGANISATIONS STRENGTHEN THEIR RESILIENCE AND ENSURE SWIFT RECOVERY DURING CYBER INCIDENTS**





# Fortify Your Cybersecurity

Fortinet  
Global Cybersecurity Leader

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

Learn more at [fortinet.com](https://fortinet.com)

# OLD FLAWS, NEW FOES: HOW THE MIDDLE EAST IS BATTLING A SURGE IN IOT ATTACKS



**OSAMA ALZOUBI**, MIDDLE EAST & AFRICA VICE PRESIDENT PHOSPHORUS CYBERSECURITY

**T**he Middle East’s rapid adoption of IoT, OT and other cyber-physical system technology has reshaped key industries like energy, manufacturing, and maritime operations. However, this surge in connectivity has also made the region a top target for cyberattacks. In just one year, IoT malware strikes have risen by over 400%, revealing the fragility of outdated systems. These neglected flaws put vital infrastructure at risk, stressing the need for stronger security rules.

At the same time, these concerns go beyond simple technical gaps, pointing to wider political factors that heighten the overall threat.

This issue does not stand alone in the tech realm; it connects with geopolitical conditions. The Middle East’s global role and reliance on oil and gas make it

a prime stage for cyberwarfare. State-backed teams, protest groups, and criminal rings view IoT as a channel for financial sabotage and power plays.

In light of such looming dangers, it becomes clear that technical responses must align with the political context, ensuring a balanced approach to defense.

Global plans like the U.S. ROUTERS Act encourage unified measures to enhance the security of broader network infrastructure devices where a device vulnerability could give attackers broad access to move around networks. Still, the Middle East’s political complexities demand tailored methods that merge fresh ideas, robust security, and cross-border teamwork. How can the region protect its IoT and network infrastructure setups before small weaknesses turn into full-blown risks? Achieving that goal calls for advanced solutions and a grasp of local political realities.

Tackling these challenges requires a firm look at how regional tensions make IoT systems even more fragile.

## **The Geopolitical Threat to IoT in the Middle East**

The Middle East carries strong global influence yet faces ongoing tensions that complicate the spread of new technologies. IoT, OT and other embedded devices offer gains in fields from industrial production to civic services. However, the same networks that boost efficiency can also grant attackers multiple gateways. Cyber-physical system devices are notoriously vulnerable and pose significant security risks – like default credentials, risky configurations, and unpatched firmware. All of which can make it easier for hackers to target IoT devices—including core infrastructure—to harm economies or gain leverage.

By focusing on both technology and the regional power balance, it becomes clearer why these dangers demand a well-planned defense.

Old or poorly configured devices, used in vital sectors, give intruders a chance to move through wider systems after one breach. This mix of political rivalries and vulnerable gear increases the danger across the region.

Given these compounding factors, examining the broader IoT landscape in the Middle East highlights the urgent need to strengthen security measures across the board.

IoT in the Middle East: Current Landscape (Source: <https://energy-utilities.com/forging-a-smarter-path-iiot-applications-in-the-news125968.html>)

### **Adoption Trends**

Cities like Dubai and Riyadh lead in smart city programs, applying IoT and OT to traffic oversight, energy saving, and other urban upgrades. Industries use IoT-driven tasks and cutting-edge logistics to streamline processes. While these projects show IoT's value, safeguards like accurate asset inventory, password and device hardening and vulnerability management, sometimes lag behind.

This gap between swift rollout and lagging protection underlines the necessity of clear standards that keep pace with rapid growth.

### **Current Security Challenges**

Various rules and practices across countries have produced uneven protections, leaving key networks weak. To unify these scattered standards, countries in the area would need to coordinate on strong guidelines—an uphill battle given differing rule. Without a single plan, even the most advanced IoT setups could be turned into liabilities.

This disjointed security posture underscores the importance of regional talks, which can lay the groundwork for a more integrated defense system. CISOs should take a proactive approach by prioritizing resilience over prevention

by implementing strategies that allow them to take advantage of the business benefits presented by IoT and OT devices but minimize the disruption to their operations and protect their critical assets. This includes developing robust plans for accurately identifying, tracking, remediating and managing their assets

### **The Middle East's Critical Need for IoT Security**

#### **Ubiquity of IoT Devices**

IoT underlies major tasks around the Middle East, from factory controls to urban services. This broad usage fine-tunes daily operations but also opens more entry points for cybercriminals. If left unguarded, these areas could face major losses, given how central IoT is to everyday work.

With such an extensive footprint, even one point of failure can reverberate widely, underscoring the importance of prompt and coordinated solutions.

#### **Potential Economic and Operational Losses**

Criminal groups can freeze production lines, disrupt power grids, and block vital services. These actions bring heavy costs, break workflows, and may scare off investors. For a region deeply tied to oil, transport, and manufacturing, the stakes are high.

As a result, leaders must weigh how to reinforce systems and create confidence in the region's ability to handle digital threats.

#### **The Role of Regulations in Strengthening IoT Security**

As the Middle East faces escalating risks from the growing number of IoT and OT devices, regulatory and governing bodies in the region respond to these risks, we are seeing an increase in regulations and guidelines aimed at securing IoT and OT devices. For instance, Saudi Arabia has already introduced comprehensive guidelines addressing these vulnerabilities, reflecting a growing commitment to safeguarding critical infrastructure. These

frameworks are essential as IoT devices, ranging from industrial sensors to smart city components, continue to proliferate, significantly expanding the attack surface for cybercriminals and nation-state actors alike.

By prioritizing regional collaboration and tailored regulations, Middle Eastern countries can not only address current vulnerabilities but also lay the foundation for secure IoT ecosystems that keep pace with technological innovation.

### **Building a Secure IoT Ecosystem**

#### **The Role of Automation and AI in Vulnerability Detection**

Automation and AI can sift through large data quickly, spotting odd behavior and applying fixes right away. This ensures businesses stay alert, cutting down on large-scale breaches. Bringing AI on board is now essential to deal with rising threat levels.

By combining technological innovation with organizational readiness, such tools can give both government and industry players a stronger line of defense. CISO should utilize these technologies to analyze vast amounts of data in real-time, enabling quick detection of emerging threats and vulnerabilities. By detecting and responding to incidents fast, security leads can effectively contain events and minimize their impact to business.

#### **Strategies for the Middle East Moving Forward**

To protect hard-won progress, the Middle East must set uniform security standards, encourage cooperation across borders, and fund both new tools and staff training. Lawmakers could offer tax cuts or official labels for firms that follow strict IoT security rules, calming investor worries and boosting public trust.

Such incentives link economic gains to safety improvements, prompting widespread upgrades without forcing every group to act alone. A focused, collaborative effort will secure the rewards of IoT without risking essential systems. 🔒





# PIG BUTCHERING SCAMS SURGE 40% IN 2024, EXPANDING TO TARGET JOB SEEKERS, SAYS CHAINALYSIS REPORT

EASY ACCESS TO EXTENSIVE VICTIM DATABASES, AI-POWERED SCAMMING TOOLS AND MORE, VIA ONE-STOP-SHOP FRAUD MARKETPLACES, HAS EMPOWERED SCAMMERS, RESULTING IN A 210% YOY INCREASE IN NUMBER OF PIG-BUTCHERING RELATED PAYMENTS

The rise of cryptocurrency has also fuelled a surge in financial fraud, with scammers pocketing at least \$9.9 billion in illicit crypto revenues in 2024. This figure is expected to reach a record \$12.4 billion, according to the latest 2025 Crypto Crime Report by Chainalysis, as further analysis uncovers more fraudulent activity. The report highlights high-yield investment scams (50%) and pig butchering schemes (33%) as the most prevalent forms of crypto fraud, reflecting the increasing sophistication of cybercriminals in exploiting investors.

Interestingly, despite pulling in half of all scam revenue in 2024, high-yield investment scam inflows declined by 36% YoY. On the other hand, pig butchering revenue increased by almost 40% YoY, and the number of deposits to pig butchering scams grew nearly 210% YoY, potentially indicating an expansion of the victim pool. Conversely, the average deposit amount to pig butchering scams declined 55% YoY.

Offering insight into these findings, Jacqueline Burns Koven, Head of Cyber Threat Intelligence at Chainalysis said: "The combination of lower payment amounts and increased deposits could indicate a change in strategy for pig butchering scams. Scammers could be spending less time priming targets, and therefore, receiving smaller payments, in exchange for targeting more victims."

This evolution of scammers' strategies

is further evidenced in the growing number of employment or work-from-home scams that Chainalysis researchers observed. Though employment scam inflows represented less than 1% of total on-chain value that scams received last year, thousands of people have unwittingly paid into fake job platforms.

"On the back of landmark initiatives, such as the UAE government's recent 'Remote Working in the UAE' report, the country's job market can be expected to see a rise in remote and hybrid work opportunities. While the majority of these will be legitimate, scammers will no doubt be keen to take advantage. The tools and techniques they have been honing in recent years with romance scams, can be easily adapted to now trick anxious, perhaps vulnerable, job seekers," Koven stated.

A major contributor to the growth in pig butchering and employment scams is the ongoing 'industrialisation' of the fraud ecosystem, epitomised in the staggering US\$375.9 million in cryptocurrency payments made to scam technology vendors on Huione Guarantee in 2024 alone, one of the most prolific marketplaces for illicit tools and services. When comparing crypto flows from 2021 through 2024 based on a compound annual growth rate, Huione scam infrastructure providers' revenue has increased exponentially, with AI service vendors' revenue growing by 1900%, indicating an explosion in the use of AI technology

to facilitate scams. These AI vendors offer technology that helps scammers impersonate others or generate realistic content that tricks victims.

Through 2024, Chainalysis also tracked nearly US\$95million in crypto payments to data vendors on the marketplace. These vendors sell stolen data such as personally identifiable information (PII) that bad actors can exploit for illicit purposes, often with information on "quick kill" targets i.e. potential victims who are most susceptible to being scammed. "With easy access to comprehensive victim databases, and AI-powered tools, scammers are better equipped than ever. It's time to move past the outdated notion of scammers as unsophisticated opportunists and recognise fraud as the thriving, highly organised ecosystem it is today. Effectively disrupting and dismantling it will require a coordinated effort from regulators, law enforcement, and the private sector," added Koven.

"Both fraud detection and compliance rely on granular, real-time data. Efforts to combat scams must focus on both prevention and enforcement, requiring stronger investigative resources and greater enablement of government agencies and local authorities. As scams continue to evolve, investigators need access to deeper intelligence, faster insights, and specialized expertise to detect and disrupt these emerging threats," Koven concluded. **■**

# GROUP-IB REPORT UNVEILS SURGE IN REAL ESTATE SCAMS ACROSS THE MIDDLE EAST

DISCOVER HOW CYBERCRIMINALS ARE EXPLOITING DIGITAL PLATFORMS TO ORCHESTRATE REAL ESTATE FRAUD, THE IMPACT ON VICTIMS, AND EFFECTIVE STRATEGIES TO COMBAT THESE DECEPTIVE PRACTICES.

Group-IB, a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime, has released a new report exposing the rising of real estate scams in the Middle East. Cybercriminals are exploiting online platforms to deceive victims — often expatriates and individuals relocating to new cities with an urgency to secure a home — into paying for fraudulent property listings, resulting in significant financial losses.

According to the report, the median financial loss per case in the Middle East is approximately \$3,064 with annual losses reaching millions per institution. Real estate scams are

becoming a growing concern in the Middle East, with fraudsters taking advantage of both the increasing reliance on digital platforms and the urgency of individuals securing a home. Group-IB works alongside local authorities and institutions to enhance digital security, leveraging their expertise in fraud prevention and cybersecurity to combat online deceptive practices.

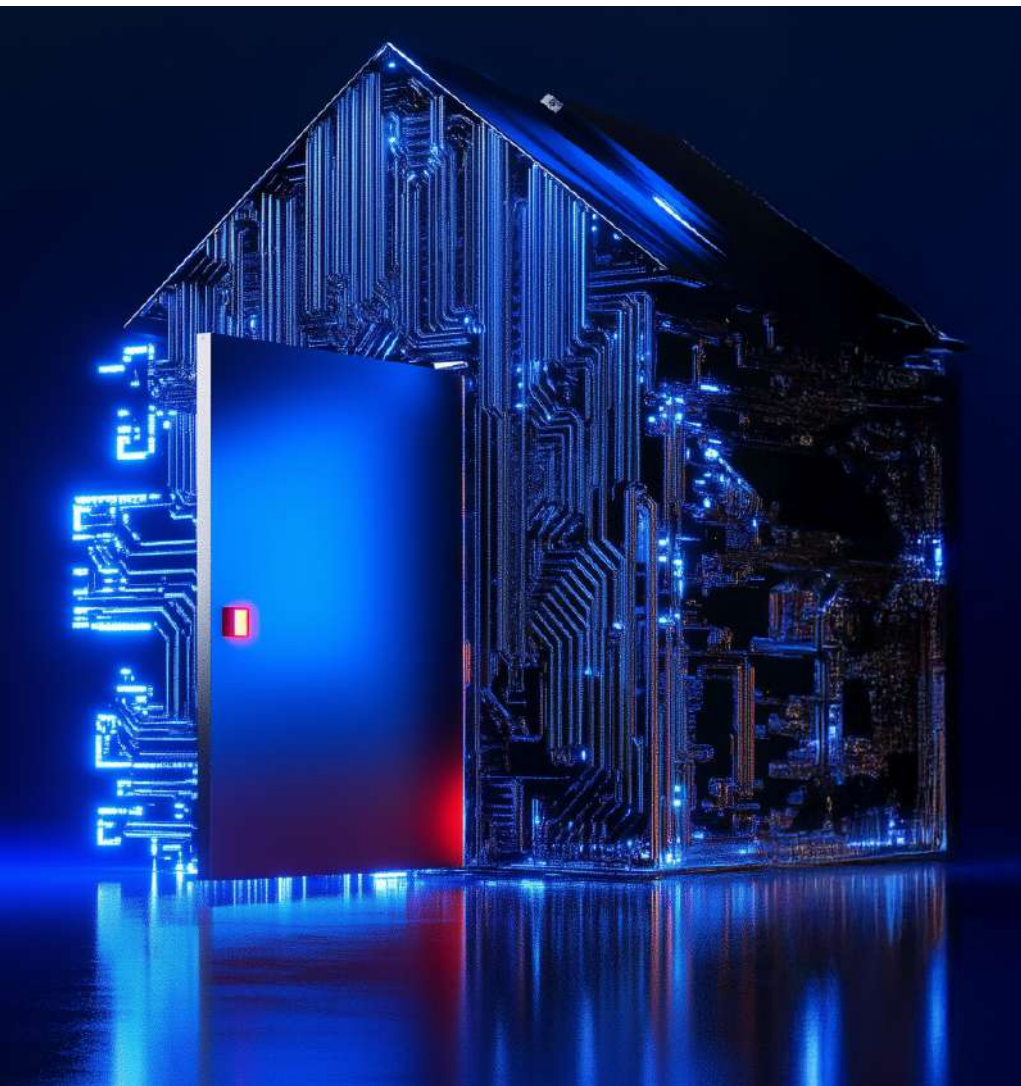
The fraud process begins when a scammer copies an existing property listing and republishes it under their name. Victims are lured in by below-market rental rates and engage with the fraudster via messaging apps like WhatsApp. To establish credibility, the

fraudster sends additional photos, often sourced from the original advertisement, and issues a fake rental contract using a legitimate real estate registration platform. Fraudsters then instruct the victim to transfer funds through electronic wallets or direct bank transfer to a mule account.

Fraudsters often target victims based on their online searches for rental properties, using keywords related to urgent housing needs, expatriate relocation, or below-market rent offers. Scammers rely on high-ranking search results and well-known rental listing platforms to lure victims in.

Based on geohash data uncovered by the report, the scammers seem





to originate from different countries, sometimes using VPNs or GPS spoofing programmes to mask their location.

Real estate scams have severe consequences, affecting both financial institutions and individual victims. These schemes exploit trust and psychological manipulation, leading to significant financial losses that are impossible to recover and potential identity theft as fraudsters often collect sensitive personal data during these transactions.

The report provided recommendations on safeguarding against real estate fraud, emphasizing the importance of verifying property ownership through official documents, understanding local real estate procedures, and visiting the

property in person before making any payments. It also cautioned against pressure tactics that demand immediate payments and stressed the need for thorough research before committing to any transaction.

#### How the Scam works:

Group-IB's Fraud Protection analysts have identified a structured fraud workflow that involves the following key components:

- **Victim** – An individual searching for rental properties, unknowingly targeted by scammers.
- **Fraudster** – A scammer who creates fake property listings and persuades victims to transfer money.

- **Ad Platform** – A popular online marketplace where fraudulent listings are posted.
- **Rental Registration Platform** – A legitimate government system exploited to create fake rental agreements.
- **Mule Bank Account** – A fraudulent account used to receive and launder stolen funds.

#### Real-life Cases:

- **Case 1:** A victim found a rental listing on a well-known platform and contacted the advertiser. The scammer sent a lease agreement through a legitimate regulatory platform, making the offer seem credible. After transferring an initial deposit, the victim was asked for additional payments. When they refused, the scammer vanished.
- **Case 2:** Another victim communicated with a fraudster via WhatsApp, received a contract, and made the payment. Upon attempting to move in, they discovered the actual property owner had no knowledge of the deal.

Group-IB — established in 2003 — is headquartered in Singapore, and with Digital Crime Resistance Centres in the Middle East and Africa, Europe, Central Asia, and the Asia-Pacific. The company analyses and neutralises regional and country-specific cyber threats via its Unified Risk Platform, offering unparalleled defence through its industry-leading Threat Intelligence, Fraud Protection, Digital Risk Protection, Managed Extended Detection and Response (XDR), Business Email Protection, and External Attack Surface Management solutions, catering to government, retail, healthcare, gaming, financial sectors, and beyond.

Group-IB collaborates with international law enforcement agencies like Interpol, Europol, and Afripol to fortify cybersecurity worldwide, and has been awarded by advisory agencies including Aite-Novarica, Gartner, Forrester, Frost & Sullivan, and KuppingerCole. [i](#)



Jeetu Patel, Chief Product Officer, Cisco

## CISCO STUDY: CEOS EMBRACE AI, BUT KNOWLEDGE GAPS THREATEN STRATEGIC DECISIONS AND GROWTH

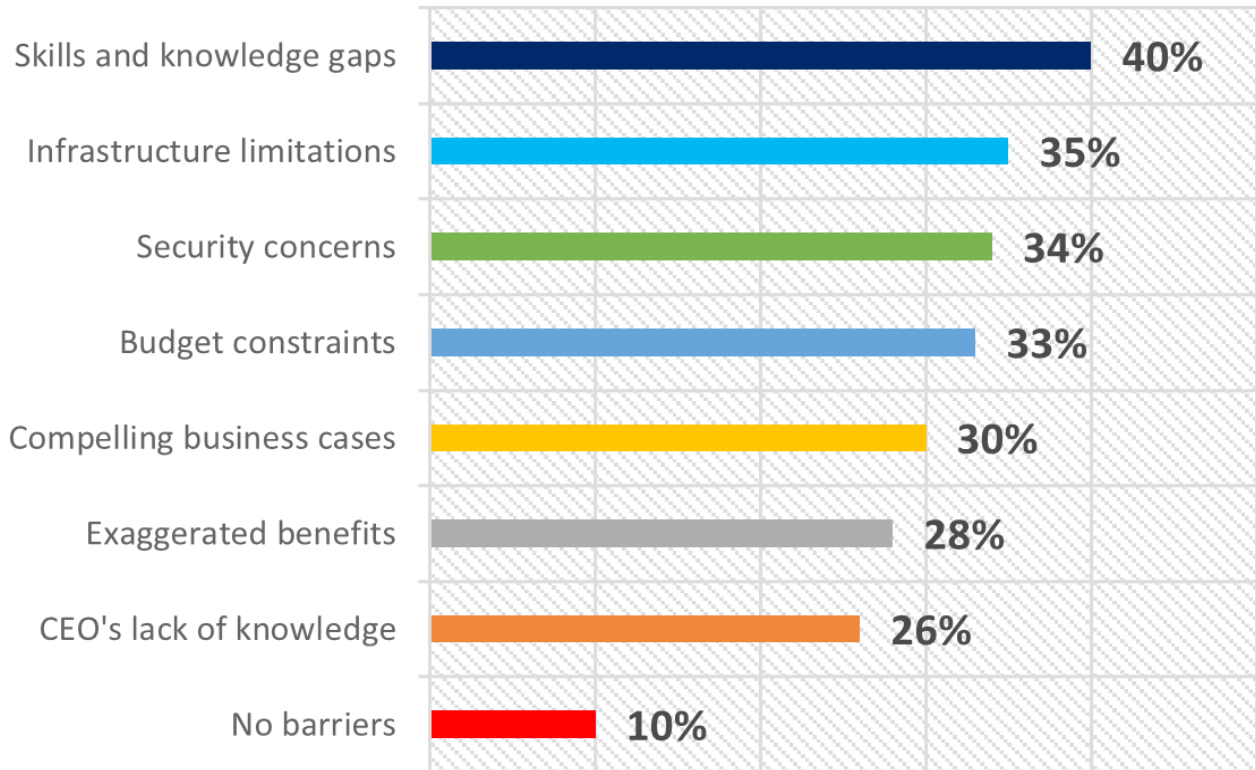
97% OF CEOS PLAN AI INTEGRATION, BUT ONLY 1.7% FEEL FULLY PREPARED. NEW RESEARCH HIGHLIGHTS WHAT'S GETTING IN THE WAY OF PROGRESS – AND HOW CEOS PLAN TO SHIFT AMBITION INTO ACTION.

A new study from Cisco, the worldwide leader in networking and security, reveals a paradox among CEOs: while 4 in 5 recognize AI's potential benefits, and almost all plan to integrate AI into their operations, many (70%) fear gaps in their knowledge will hinder decisions in the boardroom and stifle growth – risking missed opportunities and falling behind competitors. Yet, CEOs are not standing still. With support from their IT leaders and trusted partners, they plan to empowering their people, modernizing infrastructure, and strengthening cybersecurity to sharpen their competitive edge in an AI-driven future.

Cisco's Chief Product Officer, Jeetu Patel, said: "In a dynamic landscape where competition is fierce, speed decides the winners. Leaders who act decisively today to build resilient, future-proofed networks will be the AI-forward leaders driving real value for their business. Eventually there will be only two kinds of companies: those that are AI companies, and those that are irrelevant."

- While 4 out of 5 CEOs recognize AI's potential, many worry gaps in their understanding will impact strategic decisions, risking missed opportunities and falling behind competitors.
- Over 70% fear losing ground due to gaps in IT knowledge or network infrastructure, with more than half already seeing competitive losses from underinvestment in technology.
- CEOs plan to stay ahead by investing in their people, modernizing infrastructure, and strengthening cybersecurity, with 96% relying on trusted partners to future-proof their network for AI.

# CEO Barriers: Getting in the way of AI



## CEOs fear the mounting costs of inaction

Cisco's research shows more than 70% of CEOs are concerned about losing ground to competitors and missing out on opportunities because of IT and infrastructure gaps – fears that are already translating into real losses. Over half of CEOs (53%) worry that a lack of investment in technology is costing them competitive advantage, while two-thirds are concerned about the opportunity costs of not investing more in technology. The costs of inaction aren't hypothetical scenarios. If they don't invest in technology now, CEOs expect higher operating costs, lower profits, reduced productivity, and declining market share.

## The bold act while others fall behind

For the leaders who confront their fears, the rewards will transcend simply "keeping up." CEOs are turning to AI for its transformative potential: driving efficiency (69%), spurring innovation

(68%), and outpacing competitors (54%). But fulfilling that ambition requires CEOs to break down the barriers holding them back from realizing AI's potential: skills shortages, infrastructure gaps, and security risks.

While CEOs focus on the bigger picture, their CIOs and CTOs are often grappling with operational hurdles like the lack of compelling business use cases – a challenge CEOs rank lower. This tension perhaps reflects AI's exploratory phase, where the 82% of CEOs who recognize AI's potential benefits must support bold experimentation in the short term to uncover value in the long term.

Oliver Tuszik, President of Cisco EMEA, highlights the opportunity: "Whole businesses will be revolutionized if they can unlock AI's potential to innovate faster, simplify their operations, and withstand digital disruptions. But no one can do it alone. That's why 96% of CEOs are leaning on trusted partners to make the leap."

## The CEO's Blueprint: People, infrastructure, and cybersecurity

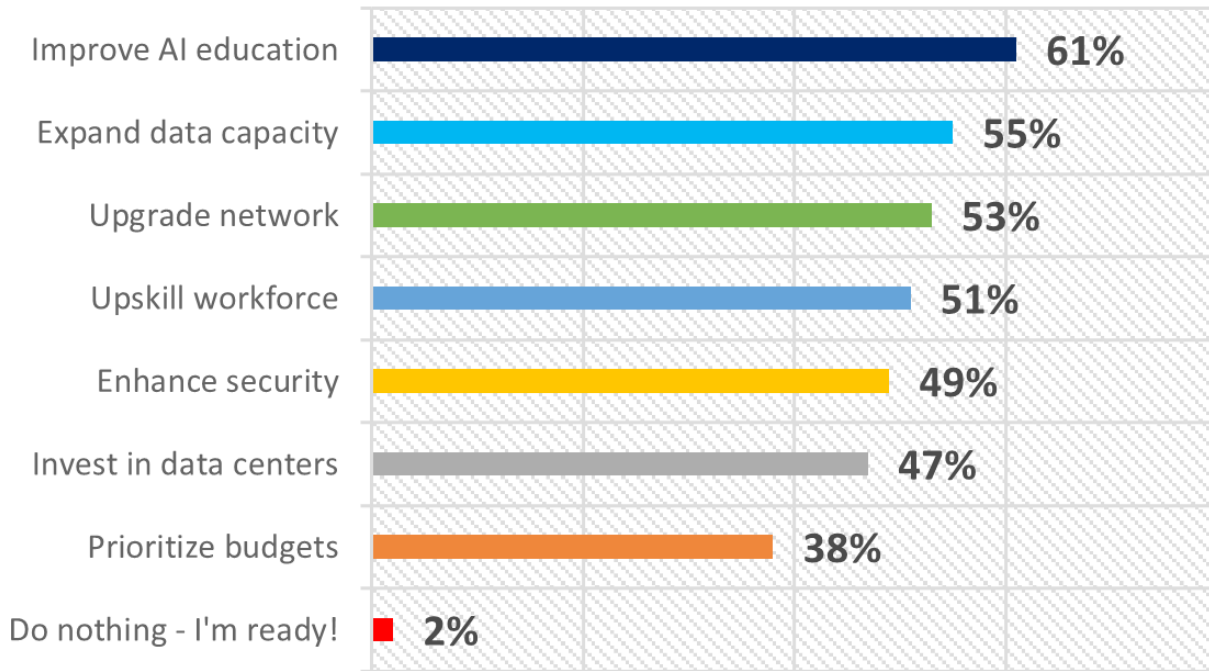
Cisco's research reveals CEOs' plan to turn fear into progress – investing in knowledge and skills, upgrading infrastructure, and enhancing security to prepare for the demands of AI.

Delivering on this blueprint will require decisive technology leadership both within the organisation and through trusted partnerships. CEOs are increasingly looking to their CTOs and CIOs, with nearly 80% recognising their vital role in guiding business and investment decisions. More and more, technology leaders are business leaders who see modern networks and technology not just as tools, but as enablers of growth, resilience, and innovation.

CEOs know they can't deliver on their blueprint without expert support: 96% are turning to trusted partnerships to future-proof their network for AI. With bold technology leadership inside and beyond



# CEO Blueprint: Getting ready for AI




Oliver Tuszik, President of Cisco EMEA

their organizations, the CEOs have the expertise to navigate uncertainties and translate AI’s potential into tangible outcomes.

**Cisco continues to help organizations overcome complexity and create opportunity in the AI era**

Skills shortages, implementation challenges, AI-ready infrastructure, and cybersecurity are top concerns for IT teams and leaders across industries. Cisco’s upcoming announcements aim to address these challenges: closing gaps between security and networking for AI data centres, empowering Service Providers with new revenue-generating tools, and equipping the next generation of AI-forward professionals with enhanced certifications.

The CEO study, conducted by Opinion Matters (24 Dec 2024–2 Jan 2025), surveyed 2,503 CEOs from companies with 250+ employees worldwide. A companion study with 8,065 senior networking leaders will follow in March, exploring the strategic and operational needs of AI-era networking and security. 



معرض و مؤتمر الخليج العالمي لأمن المعلومات

# GISEC

GLOBAL

06 - 08 MAY 2025  
DUBAI WORLD TRADE CENTRE

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



# MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE



ENQUIRE FOR 2025!

OFFICIAL DISTRIBUTION PARTNER



LEAD STRATEGIC PARTNER



DIGITAL TRANSFORMATION PARTNER



STRATEGIC PARTNERS



PLATINUM SPONSORS



GOLD SPONSORS



SILVER SPONSOR



CONTACT US

[gisec@dwtc.com](mailto:gisec@dwtc.com)

+971 4 308 6469

[cyber.gisec.ae](http://cyber.gisec.ae)

#gisecglobal



# HELP AG'S MSS GRADUATE PROGRAM PAVES THE WAY FOR FUTURE EXPERTS

EMPOWERING THE NEXT GENERATION OF CYBERSECURITY LEADERS  
– HELP AG'S MSS GRADUATE PROGRAM



The cybersecurity landscape is evolving rapidly, and the demand for skilled professionals has never been greater. Help AG's MSS Graduate Program, spearheaded by Sunil Sharma, Vice President – Managed Security Services, aims to bridge the talent gap by equipping young graduates with hands-on experience, industry certifications, and mentorship. With a structured, year-long approach, Sharma states that the program transforms aspiring professionals into industry-ready cybersecurity experts. By fostering strong academic partnerships and immersive learning experiences, Help AG is not just addressing current talent shortages but also shaping the future of cybersecurity in the region.

## **What do you aim to achieve through Help AG's MSS Graduate Program?**

With 24 years of cybersecurity experience across seven countries, I've been with Help AG since 2020, leading one of the region's largest Managed Security Services (MSS) teams, comprising over 200 professionals. Over the years, I have witnessed a growing



talent gap in cybersecurity, both globally and regionally.

To address this, we launched the MSS Graduate Program—a structured, year-long initiative designed to identify, train, and mentor young graduates. By aligning their skills with industry needs, we prepare them for full-time roles within our team. The program has received strong industry support and plays a vital role in building a sustainable pipeline of skilled cybersecurity professionals.

### **How does Help AG's MSS Graduate Program facilitate the development of practical cybersecurity skills that can be applied in professional settings?**

The program is structured into distinct phases to provide a comprehensive cybersecurity learning experience. The Back-to-School phase reinforces fundamental cybersecurity concepts, ensuring a strong foundation beyond academic studies. Graduates receive specialized training through Udemy, a strategic partner of Help AG, and hands-on simulations via Immersive Labs. Experienced Help AG mentors provide guidance and regular evaluations to track progress.

In the On-the-Job Training phase, graduates are assigned to streams based on their interests and performance, such as engineering, SOC, and automation. Over six months, they gain hands-on experience, analyze threat alerts, and progressively tackle complex tasks. By the end of this phase, they are well-prepared to contribute effectively to projects and the cybersecurity industry.

### **How does the MSS Graduate Program remain aligned with the evolving cybersecurity landscape?**

To ensure the MSS Graduate Program remains relevant in the rapidly evolving cybersecurity landscape, we integrate the MITRE ATT&CK framework, a globally recognized resource that continuously updates threat models

based on real-world adversarial behaviours. This provides graduates with up-to-date exposure to emerging cybersecurity threats and mitigation strategies. Furthermore, we collaborate with leading vendors to deliver specialized training on the latest tools, technologies, and security solutions. These industry-driven initiatives equip participants with the skills necessary to address current cybersecurity challenges while fostering adaptability for future threats.

### **What challenges do graduates face, and how does the program support them?**

Graduates often struggle with transitioning from academic learning to industry applications and adapting to the fast-paced cybersecurity environment. To address this, the program offers daily check-ins, weekly evaluations, and mentorship from team leaders. Hands-on learning through simulations and shadowing further bridges the gap between theory and practice. The program's flexibility ensures tailored support, fostering confidence and competence in cybersecurity.

### **What is the significance of hands-on experience, and how does the program facilitate it?**

Practical experience is critical in cybersecurity. Help AG collaborates with leading vendors like Immersive Labs to provide trainees with simulated real-world challenges. In addition to internal training, the program supports career placements, allowing graduates to explore opportunities within Help AG and its clients, thereby strengthening the regional cybersecurity talent pool.

### **How do partnerships with academic institutions bridge the gap between academia and industry?**

Help AG actively collaborates with universities such as the University of Wollongong in Dubai and the University of Sharjah to align academic learning

with industry needs. Through career fairs, internships, guest lectures, and curriculum contributions, students gain both theoretical knowledge and practical skills. The initiatives ensure a steady pipeline of industry-ready talent equipped to tackle real-world cybersecurity challenges.

### **Have any program graduates successfully transitioned into client-facing roles?**

The first cohort of the MSS Graduate Program achieved a 100% employment success rate within Help AG. Notably, one graduate led the launch of a new service and became the primary client liaison, earning a monthly performance award among a 550-member team.


Such success stories highlight the program's effectiveness in developing industry-ready professionals.

### **How does Help AG address gaps in traditional cybersecurity education?**

Traditional academia often lags the evolving cybersecurity landscape. Help AG bridges this gap through mentorship, curriculum collaboration, and practical engagements across diverse regions, including India, Oman, UAE, and KSA. As part of the e& group, Help AG fosters young talent through its MSS Graduate Program, hackathons, innovation forums, and open days, ensuring graduates gain industry-relevant expertise.

### **What advice would you give to future cybersecurity leaders?**

To stand out in a competitive job market, aspiring cybersecurity professionals should pursue micro-credentials and industry-recognized certifications alongside their degrees.

Certifications like Cisco CCNA, accessible online, demonstrate specialized skills and a proactive learning mindset. Differentiation comes from continuous upskilling, developing niche expertise, and positioning oneself as a high-value professional in the field. 

# HPE INTRODUCES NEXT-GENERATION PROLIANT SERVERS ENGINEERED FOR ADVANCED SECURITY, AI AUTOMATION AND GREATER PERFORMANCE

HPE PROLIANT COMPUTE GEN12 PORTFOLIO MEETS FEDERAL SECURITY CERTIFICATION STANDARDS, BOOSTS IT PRODUCTIVITY WITH AI-DRIVEN INSIGHTS AND DRIVES 65% POWER SAVINGS



**H**ewlett Packard Enterprise announced eight new HPE ProLiant Compute Gen12 servers, the latest additions to a new generation of enterprise servers that introduce industry-first security capabilities, optimize performance for complex workloads and boost productivity with management features enhanced by artificial intelligence (AI). The new servers will feature upcoming Intel Xeon 6 processors for data center and edge environments.

“Our customers are tackling workloads that are overwhelmingly data-intensive

and growing ever-more demanding,” said Krista Satterthwaite, senior vice president and general manager, Compute at HPE.

“The new HPE ProLiant Compute Gen12 servers give organizations – spanning public sector, enterprise and vertical industries like finance, healthcare and more – the horsepower and management insights they need to thrive while balancing their sustainability goals and managing costs. This is a modern enterprise platform engineered for the hybrid world, designed with innovative security and control capabilities to help companies prevail

over the evolving threat landscape and performance challenges that their legacy hardware cannot address,” added Satterthwaite.

## **Chip-to-cloud and full lifecycle security**

The HPE ProLiant Compute Gen12 portfolio sets a new standard for enterprise security with built-in safeguards at every layer – from the chip to the cloud – and every phase of the server lifecycle. HPE Integrated Lights Out (iLO) 7 introduces an enhanced and dedicated security processor called secure enclave that is engineered from the ground up as

HPE intellectual property. HPE ProLiant Compute servers with HPE iLO 7 will help organizations safeguard against future threats as the first server with quantum computing-resistant readiness and to meet the requirements for a high-level cryptographic security standard, the FIPS 140-3 Level 3 certification .

The chip-enhanced security features of HPE iLO 7 uniquely distinguish HPE ProLiant servers from other vendors. Embedded into the server hardware, secure enclave establishes an unbreakable chain of trust to protect against firmware attacks and creates full line-of-sight from the factory and throughout HPE's trusted supply chain. This extends to the end of the product lifecycle with HPE Onsite Decommission Services which collects equipment and transports it to an authorized sorting and recycling facility.

### **AI-Driven insights improve operations management, automation and power efficiency**

HPE Compute Ops Management is a cloud-based software platform that helps customers secure and automate server environments. Proactive and predictive automation, now enhanced with AI-driven insights, helps organizations improve energy efficiency by forecasting power usage and enabling enterprises to set thresholds to control costs and carbon emissions on a worldwide level. A new global map view simplifies management so customers can instantly identify server health issues across distributed IT environments and multi-vendor toolset integration reduces downtime by up to 4.8 hours per server every year

. Automated on-boarding simplifies server set-up and ongoing management, particularly in remote or branch-office deployments where local IT resources are not available.

All new HPE Compute Ops Management features, including AI-informed insights, new map-based visibility and third-party tool integration, will be available to HPE ProLiant Compute Gen10 servers and newer.

To aid customers evaluating future purchases, a standalone tool called HPE Power Advisor estimates environment performance metrics such as energy costs and greenhouse gas emissions.

### **Servers Optimized for performance, energy efficiency and available with direct liquid cooling**

New additions to the HPE ProLiant Compute Gen12 portfolio are right-sized to address demanding workloads that include AI, data analytics, edge computing, hybrid cloud and virtual desktop infrastructure (VDI) solutions. Addressing the exponential growth in power demands placed on data centers, the HPE ProLiant Compute Gen12 portfolio is engineered to optimize performance, energy efficiency and cost with up to 41% better performance per watt compared to legacy enterprise systems . HPE ProLiant Compute Gen12 servers deliver up to 65% in power savings per year and enable organizations to free up data center capacity with one Gen12 server providing the same compute performance as seven Gen10 servers .

"Partnering with reliable, innovative hardware vendors like HPE helps us meet the evolving needs of our clients

and empower them with comprehensive, workload-optimized IT infrastructure solutions," said William Bell, executive vice president, Products at phoenixNAP. "We were the first customer in the world to order HPE ProLiant Compute Gen12 servers and the benefits of the upgrade were immediate. By delivering these advanced technologies as a service, phoenixNAP enables organizations of all sizes to tackle challenges related to performance, energy efficiency, data security, and infrastructure management at scale."

To meet customer demand for more energy efficient data centers, HPE is offering optional direct liquid cooling (DLC) on Intel-based HPE ProLiant Compute Gen12 one-socket and two-socket rack servers. Liquid removes heat more efficiently than air, removing more than 3,000 times more heat based on volume . HPE has built the world's fastest direct-liquid cooled supercomputers and with more than 300 DLC patents and over 50 years of experience, HPE is a leader in deploying direct liquid-cooled servers and data centers.

### **Availability**

Six of the eight new HPE ProLiant Compute Gen12 servers featuring upcoming Intel Xeon 6 processors will be available Q1 2025. This includes HPE ProLiant Compute DL320, DL340, DL360, DL380, DL380a and ML350 Gen12 servers. HPE Synergy 480 and HPE ProLiant Compute DL580 Gen12 servers are expected Summer 2025.

The HPE ProLiant Compute Gen12 portfolio will be available standalone or via HPE GreenLake, offering scalability, cost efficiency and service agility. These solutions can be purchased through an authorized channel partner. HPE Services helps customers make the most of the HPE ProLiant Compute Gen12 portfolio by providing advisory, professional, operational, managed, financial and asset management assistance to accelerate business operations. **!**

**"OUR CUSTOMERS ARE TACKLING WORKLOADS THAT ARE OVERWHELMINGLY DATA-INTENSIVE AND GROWING EVER-MORE DEMANDING," SAID KRISTA SATTERTHWAITE, SENIOR VICE PRESIDENT AND GENERAL MANAGER, COMPUTE AT HPE.**





Shai Morag, Chief Product Officer, Tenable

# TENABLE STRENGTHENS ITS IDENTITY EXPOSURE CAPABILITIES TO PROTECT AGAINST COMPROMISES

TENABLE IDENTITY EXPOSURE ADDRESSES IDENTITY SPRAWL SECURITY CHALLENGES WITH 360-DEGREE VISIBILITY INTO IDENTITY RISK

Tenable, the exposure management company, announced the launch of Identity 360 and Exposure Center, two new Tenable Identity Exposure capabilities designed to help organizations pinpoint identity risks and take swift, targeted action to prevent identity-based attacks.


Identity management has become fragmented, leading to identity sprawl - a tangled web of accounts, permissions and misconfigurations across disparate platforms. This fragmentation severely limits visibility and risk detection, weakens access controls, and increases the threat of privilege escalation and lateral movement. The combined power

of Identity 360 and Exposure Center simplifies this complexity, delivering unified visibility across identity providers to serve as a single source of truth.

“Compromised identities are at the root of nearly every successful cyberattack,” said Shai Morag, Chief Product Officer, Tenable. “Today, 75% of organizations manage two or more identity solutions,<sup>1</sup> leading to increased complexity around identity security. Tenable Identity Exposure ensures that organizations have full visibility into their identity risks and provides actionable remediation guidance so organizations can swiftly and confidently prevent attacks before they occur.”

**Key functionality available in this release includes:**

- 360-Degree Identity Visibility and Risk Prioritization: Gain a unified view of accounts, weaknesses, entitlements, roles, groups and relationships across Active Directory and Entra ID. Tenable Identity Exposure consolidates this information into comprehensive identity profiles for streamlined risk management.
- Centralized Weakness Management and Streamlined Remediation: Consolidate identity-related weaknesses—including privilege misconfigurations, excessive permissions, stale accounts, default settings, risky trust relationships and unmonitored service accounts—into a single interface, and take action with detailed remediation steps and one-click PowerShell scripts.
- AI-Driven Identity Asset Exposure Score (AES): Identify the most critical identity weaknesses with AI-driven risk scoring and focus remediation efforts on the highest-priority threats.

Tenable Identity Exposure continuously monitors for misconfigurations, attack paths and security weaknesses, empowering organizations to proactively reduce risk and strengthen their security posture. 

# Delinea

Securing identities at every interaction

Seamless, intelligent,  
centralized authorization to better  
secure the modern enterprise



Secure Credentials



Privileged Remote Access



Privilege & Entitlement Elevation



Identity Threat Protection



Identity Governance



Follow us on



delinea.com

# PEOPLELINK APPOINTS TECHBRIDGE MEA AS REGIONAL DISTRIBUTION PARTNER

**T**echBridge Distribution MEA, a leading technology distributor in the Middle East and Africa (MEA), is proud to announce its strategic partnership with PeopleLink, a global leader in audio-visual (AV), Unified Communications, Cloud Collaboration and Software solutions. This partnership will enable TechBridge to distribute PeopleLink’s unified communications solutions across the ME region, further enhancing digital collaboration, communication, and engagement for businesses, educational institutions, healthcare organizations, the retail industry, hospitality, and governments.

Steve Lockie, CEO of TechBridge, said: “We are thrilled to partner with PeopleLink to introduce their award-winning AV solutions to the MEA region. The demand for high-quality, reliable communication tools has never been higher, and our Mobility Division is ready to take their solutions to market and support the growing demand for flexible, scalable AV technology.”

The demand for cutting-edge communication and collaboration tools has surged in the post-pandemic world, with an increasing emphasis on secure, on-premise, end-to-end video solutions to protect regional interests.

Jagadeesh Choppella, Sales Director at PeopleLink, said: “TechBridge’s deep expertise in the MEA market makes it the perfect partner for PeopleLink as we expand our regional presence. Together, we are on a mission to deliver innovative, customized collaboration solutions that elevate interactions through video-enabled communications beyond traditional meeting spaces. Our solutions



are designed to be secure, scalable, and future-proof, ensuring we meet the evolving needs of businesses across the region.”

PeopleLink stands at the forefront of AV, Unified Communications, on-premise video technologies, software, and cloud technologies, offering a comprehensive suite of solutions that cater to organizations of all sizes.

TechBridge’s Mobility Division is uniquely positioned to leverage its vast regional presence and market expertise to bring PeopleLink’s solutions to businesses and institutions across the MEA region.


PeopleLink’s all-in-one video conferencing professional audio systems combines high-definition cameras, impeccable audio devices for every space, and cloud solutions into a single, easy-to-cloud enable and solutions to deploy on-premises.

PeopleLink sets itself apart with its innovative AV and collaboration solutions tailored for various industries, including education, defense, manufacturing, retail, and finance. Their unique solution bundles for classrooms, meeting rooms,

boardrooms, and auditoriums reduce hardware dependencies while enhancing communication and remote collaboration.

Unlike competitors still working on peer-to-peer (P2P) collaboration for the WebRTC platform, PeopleLink has already launched its MCU architecture, enabling multiple participants from different networks and devices to join a single call efficiently.

A key breakthrough is their InstaVC collaboration solution, which integrates seamlessly with hospitality management systems, national ID frameworks, payment gateways, remote healthcare, remote shopping, and digital signage. InstaVC offers a fully customizable experience, allowing businesses to tailor solutions to their specific needs rather than relying on pre-packaged offerings.

PeopleLink also delivers cutting-edge display solutions, featuring interactive flat panels up to 110” with 4K resolution and Active LED panels with pixel pitches of 0.9, 1.5, and 2.5 mm for indoor and outdoor use. These high-quality displays ensure exceptional clarity, responsiveness, and immersive engagement, transforming any space into a dynamic visual environment. 



# Copilot+ PCs

Surface Pro and Surface Laptop deliver the best of AI across devices and the cloud to drive productivity, creativity, innovation, and resilience. To ensure a seamless experience, we built and tested Copilot and Copilot for Microsoft 365 on Surface devices.

## Surface Pro

### Pioneering versatility matched by intelligent power

Unlock high performance in a form factor that redefines what a laptop can do.



The HD front-facing Surface Studio Camera supports powerful Windows Studio Effects.



Employees interact with Copilot effortlessly through touch gestures or inking with Surface Slim Pen on the PixelSense™ Flow touchscreen.



The new Copilot key provides access to Copilot.

On-device AI finds almost anything fast with Recall and empowers collaboration through real-time translation of 40+ languages to English using Live Captions.



Snapdragon®X Elite and Plus processors unlock new levels of speed and efficiency with an industry-leading NPU that drives up to 45 TOPS for seamless on-device AI.



## Surface Laptop

### Transformative design packed with intelligent power

Embrace opportunity with Copilot+ PC performance in a newly sleek profile with a smaller footprint and larger screen real estate.





# PIONEERING CONVERSATIONAL AI AS A SERVICE

## Our Industry Landscape



Retail



Healthcare



Banking



Education



Oil & Gas

Conversational AI Framework | NLP | Text-to-Speech | Generative AI | IDP



SCAN QR



LEARN MORE

