ISSUE 90 | DECEMBER 2024

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

CORO BOLSTERS CYBERSECURITY FOR SMEs AND STARTUPS

EXPLORING CORO'S PROACTIVE CYBERSECURITY SOLUTIONS IN THE DYNAMIC DIGITAL LANDSCAPE OF THE MIDDLE EAST, WITH INSIGHTS FROM **PIERS MORGAN**, SENIOR VICE-PRESIDENT AND GENERAL MANAGER - EMEA

tahawultech.com

cnme
computer news middle east
SUPPLEMENT

D-Link®

MADE IN TAIWAN SWITCH SERIES

Unlocking Network Potential

Layer 3 IGMP filtering and 10G uplink ports

5 years warranty

UPTIME

DGS-3130 Series

Layer 3 Stackable Managed Switches

Designed for small to medium-sized business networks, the unified software incorporates Layer 2 and Layer 3 features, with 10-Gigabit ports, greater port density thanks to physical stacking, all of which enables the DGS-3130 Series to be deployed in a variety of environments and topologies, including Metro Ethernet deployments.

On all GE and RJ-45 access ports

6 KV SURGE PROTECTION

Highly Reliable

Redundant power supply (RPS) support, Ethernet Ring Protection (ERPS) and 6 kV surge protection on all GE and RJ-45 access ports

Feature-Rich Unified Software

Powerful L2 and L3 features such as Static Route, RIP/RIPng and OSPFv2/v3

Scalable and Highly Available

Supports high bandwidth stacking and fault tolerant topologies

Easy Access Control

Support for 802.1X, Web-based Access Control (WAC), and MAC-based Access Control (MAC)

Next-Business-Day Replacement

Register at www.dlinkmea.com/nbd and avail:

3 Years Free Next-Business-Day Replacement
5 Years Warranty Services

D-Link PROTECT

Register the product within 60 days of product purchase

NBD registration applicable to end customer/actual product user only

CONTENTS

Security ADVISOR MIDDLE EAST

EDITOR'S NOTE

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

Sandhya DMello
Editor

2025 CYBERSECURITY OUTLOOK NAVIGATES NEW THREATS AND TECHNOLOGIES IN THE MIDDLE EAST

As 2024 draws to a close, we reflect on a year of profound transformation in the cybersecurity landscape of the Middle East. The rapid digital adoption, spurred by ongoing remote work, enhanced digital services, and the expansive growth of IoT devices, has significantly broadened attack surfaces, making robust cybersecurity measures more crucial than ever.

Throughout the year, we witnessed a notable increase in the sophistication of cyber threats. Ransomware and phishing attacks, now more refined and targeted, have impacted critical sectors including healthcare and finance. In response, nations across the Middle East, particularly the UAE and Saudi Arabia, have strengthened their cybersecurity frameworks, introducing new strategies and regulations to safeguard national security and protect critical information infrastructures.

COMBATTING 2025 CYBER THREATS

This December issue of Security Advisor Middle East explores the dynamic shifts and emerging trends poised to define 2025 in cybersecurity. Articles range from interviews with industry leaders, like Lothar Renner of Cisco, discussing the identity-first approach to security at Black Hat MEA, to strategic insights from SentinelOne and OPSWAT on enhancing cybersecurity measures.

We delve into the evolution of ransomware over 35 years, explore mitigations against AI-driven cybercrime, and examine the strategic importance of data security in shaping a resilient digital infrastructure. Additionally, we look at how AI and machine learning are being leveraged to predict and combat cyber threats more effectively, heralding a shift towards more resilient systems that not only defend but quickly recover from attacks.

As we venture into 2025, the articles within this issue underscore the necessity for continued collaboration between governments, industry leaders, and technology providers. Our collective commitment to cybersecurity must not only persist but intensify, as we strive to safeguard our digital future against increasingly sophisticated threats.

Stay informed and empowered with this issue of Security Advisor Middle East, as we navigate the complexities of cybersecurity together, ensuring a safer tomorrow.

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

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.

CHAINALYSIS ACQUIRES HEXAGATE, ADDS WORLD-CLASS PREVENTION CAPABILITIES

Chainalysis has announced its acquisition of Hexagate, the leading provider of Web3 security solutions that detect and mitigate real-time threats including cyber exploits, hacks, and governance and financial risks. With Hexagate's established position as the top choice for chains, protocols, asset managers, and exchanges to help keep their funds secure, this deal augments Chainalysis' already impressive portfolio of blockchain data solutions.

"I have long believed that in order to advance the Chainalysis mission to build trust in blockchains, we would need to expand our business beyond investigations and into prevention," said Jonathan Levin, Co-Founder and CEO at Chainalysis. "The Hexagate team impressed me with their complete security suite for proactive prevention, including monitoring, mitigation, forensics, and compliance. Together, Chainalysis and Hexagate provide a holistic risk solution that includes prevention, compliance and remediation."

Hexagate leverages machine learning models to identify suspicious patterns and unusual transactions across blockchain networks in real-time. Over the past two years, the company has detected all known hacks – and more than 98% were detected before they occurred. As a result, Hexagate's customers, which include industry leaders like Coinbase and Consensys, have already saved more than US$1billion in customer funds by taking on-chain actions based on real-time notifications and automated responses to potential threats.

Jonathan Levin, Co-Founder and CEO at Chainalysis

Shashank Agrawal, Head of Protocol Security at Coinbase, shared, "Hexagate has become an integral part of on-chain security at Coinbase. Their real-time on-chain threat and risk detection and Base ecosystem monitoring solution for all Base builders has provided us with the broadest coverage for Coinbase and Base, ensuring the safety of our users and reinforcing trust across anything we build or do on-chain."

Such capabilities are only going to become more important for the crypto ecosystem as smart contracts facilitate more value transfer. The growth of stablecoins, enterprise layer 1 and layer 2 protocols, and wallet infrastructure suggests that securing smart contracts will be critical to preventing fund loss among private sector entities, and governments will increasingly seek to monitor smart contracts associated with illicit funds.

"We're thrilled to welcome Hexagate to the team, and to work together toward a safer, more transparent financial system. Web3 is transparent by design, and with the right solutions, it can be the world's safest financial system," concluded Levin.

SOPHOS XDR EXCELS IN MITRE ATT&CK EVALUATIONS: ENTERPRISE

100% of Sophos XDR detections for adversary activities targeting Windows and Linux devices provide rich analytic coverage and achieve the highest possible ratings

Sophos, a global leader of innovative security solutions for defeating cyberattacks, today announced its strong results in the 2024 MITRE ATT&CK Evaluations: Enterprise.

Sophos XDR detected 100% of the adversary behaviors in attack scenarios targeting Windows and Linux platforms, mimicking malware strains from ruthless ransomware-as-a-service gangs LockBit and CL0P. Further, all of Sophos' responses to these ransomware attack scenarios were marked "technique" – the highest possible rating that denotes who, what, when, where, why and how attacks were carried out.

Sophos XDR achieved:

'Analytic coverage' ratings for 99% of sub-steps (79 out of 80) across three comprehensive attack scenarios

Highest possible ('Technique') ratings for 98% of sub-steps (78 out of 80)

Highest possible ('Technique') ratings for 100% of sub-steps in the Windows and Linux ransomware attack scenarios

"Attackers are relentless to innovate techniques to bypass trusted security defenses. This assessment from MITRE helps security buyers evaluate the effectiveness against today's threats," said Simon Reed, chief research and scientific officer at Sophos.

"Sophos is committed to transparency and conducting third party measurement to help security buyers make informed decisions to strengthen their security

Simon Reed
senior vice president, SophosLabs

posture. We're proud of Sophos XDR's ongoing excellence both in industry testing and real-world frontline defenses. We're consistently evolving our solutions, just like attackers are constantly evolving their tactics, so our customers can stop known and unknown threats before they escalate into destructive attacks."

MITRE ATT&CK Evaluations are among the world's most respected independent security tests. This round of MITRE ATT&CK Evaluations: Enterprise evaluated the abilities of 19 vendors in detecting and analyzing attack tactics, techniques, and procedures (TTPs) leveraged by real-world adversarial groups. In this cycle, MITRE also expanded ATT&CK Evaluations to include macOS attacks emulating tactics from the Democratic People's Republic of Korea – where 19 out of 21 Sophos XDR detections were also categorized as "technique" – the highest possible rating.

Sophos XDR combines active adversary mitigations – including industry-first Adaptive Attack Protection that immediately activates heightened defenses when a hands-on-keyboard attack is detected, stopping the attack and providing defenders valuable additional time to respond; anti-ransomware technology; deep learning artificial intelligence; and exploit prevention to prevent and stop attacks. It is powered by Sophos X-Ops threat intelligence, a cross-operational task force of more than 500 security experts within SophosLabs, Sophos SecOps, and SophosAI.

DU PARTNERS WITH CYBERSPACE TECHNOLOGIES TO REVOLUTIONISE BUSINESS MANAGEMENT THROUGH TAIRRA

du, the leading telecom and digital services provider, announced an exclusive partnership with Emirati firm Cyberspace Technologies for Tairra, a business management platform dedicated to optimising operations for teams of varying sizes. The agreement was signed by Fahad Al Hassawi, CEO of du and Abdulla Khalifa Al Shaer Al Mansoori, Managing Partner at Cyberspace Technologies.

Fahad Al Hassawi, CEO of du said: "We are excited to announce our partnership with Tairra, marking a significant step forward in our journey to revolutionise the digital landscape for businesses in the UAE. Our collaboration is founded on a shared vision to simplify complexities in business management through innovative technology. By integrating Tairra's comprehensive suite into our services, we are offering our customers a transformative tool that not only enhances operational efficiency but also elevates the overall customer experience."

Customers will benefit from seamless team coordination, streamlined project management, efficient client relationship management, dynamic chat functionalities, organised file management, suite of productivity tools and a gamified loyalty program – all managed through a user-friendly administrative dashboard.

The collaboration aims to revolutionise business management by offering a comprehensive all-in-one platform that enhances customer experiences and drives innovation. du will introduce Tairra's integrated business collaboration suite to business clientele, consolidating essential tools onto a single platform.

Abdulla Khalifa Al Shaer Al Mansoori, Managing Partner at Cyberspace Technologies, said: " Our platform is designed to meet the dynamic needs of today's businesses, offering tools that streamline operations, boost productivity, and foster team collaboration. We are committed to this collaboration with du, as it aligns with our mission to innovate and deliver solutions that not only support business growth but also enhance the way teams work and interact."

Tairra's flexible hosting options, whether on the cloud or client premises, prioritise data security and compliance. With Tairra's automation capabilities and efficiency enhancements, businesses can optimise workflow, boost productivity and team coordination.

du and Tairra are at the forefront of reshaping the future of business management through cutting-edge technology with a customer-centric approach and empowering businesses with the tools they need to thrive in a rapidly evolving market.

OPSWAT ACQUIRES LEADER IN ADVANCED DATA DIODE TECHNOLOGY TO STRENGTHEN CYBER DEFENSES FOR CRITICAL INFRASTRUCTURE

Acquisition of Fend Incorporated broadens OPSWAT's end-to-end cybersecurity product offerings in the field of Data Diodes and Unidirectional Gateway Solutions, establishing company as one of the most comprehensive providers in the industry

OPSWAT, a global leader in critical infrastructure protection established in the U.S., announced its acquisition of Fend Incorporated. Fend is a pioneering data pipeline and cybersecurity company dedicated to securing operational technology (OT) against cyber threats, ransomware, and other evolving risks. Based in Arlington, Virginia, Fend is known for its expertise in protecting U.S. government agencies, utilities, oil and gas, manufacturing, and other critical industries where air-gapped environments are essential for defense against cyber incidents. The announcement establishes OPSWAT as providing the most comprehensive variety of Data Diodes and Unidirectional Gateways in the industry that utilizes proprietary technology like Multiscanning with up to 30 anti-virus engines, Deep CDR™ for zero-day threats, Sandboxing, and Proactive DLP™ technologies prevent sensitive data leakage.

Fend's data diode technology creates a secure one-way communication channel, allowing data to flow from one network to another while physically blocking reverse transmission. This hardware-based approach is valued in high-security environments like defense, industrial control systems, and critical infrastructure, where preventing external access is paramount. Originally reserved for sensitive applications such as nuclear power plants, data diode technology has evolved to become more accessible and affordable, making it a practical solution for industries that require secure online monitoring and predictive analytics. With benefits such as increased operational efficiency, reduced unexpected downtime, and improved staff productivity, Fend's data diodes offer protection across diverse industrial sectors.

Benny Czarny, CEO and Founder of OPSWAT

"Fend's solutions are a strategic addition to our portfolio, allowing OPSWAT to deliver unparalleled security for customers' most critical assets," said Benny Czarny, CEO and Founder of OPSWAT. "This strategic move broadens OPSWAT's existing product offering that includes high-speed data diodes and unidirectional gateway solutions to mobile, cell-based, cloud-based, and ruggedized products to support more critical infrastructure needs."

"Joining OPSWAT represents a significant opportunity for Fend, allowing us to offer customers an even broader range of cyber defenses," said Colin Dunn, CEO and Founder of Fend. "Together, we can provide unmatched security for critical infrastructure around the globe, ensuring resilience against sophisticated cyber threats."

Trafalgar Capital Partners, an M&A advisor with a focus on the technology, media, and telecommunications industries, helped facilitate the transaction.

"We're proud to have supported Fend Incorporated through this transaction with OPSWAT," said Frantz Casseus, Founder & Managing Director of Trafalgar Capital Partners. "By integrating Fend's pioneering, cutting-edge data diode technology, OPSWAT is poised to deliver unparallelled solutions for secure data transfer and advanced threat protection, enhancing its leadership in critical infrastructure."

OPSWAT's industrial OT offerings significantly expanded with its 2021 acquisition of Bayshore Networks. The acquisition of Fend further enhances OPSWAT's capabilities in both centralized and distributed deployments, providing true cross domain security with connectivity to our MetaDefender Kiosk and MetaDefender Managed File Transfer to help secure solutions for remote assets and smaller facilities, such as water utilities, which have large numbers of endpoints at the edge that still require high security.

Fend's comprehensive connectivity options—accommodating Ethernet, cellular, and even serial connections for older networks—will enable OPSWAT to meet both the demands of emerging technologies such as 5G and Industry 4.0 and the vast landscape of legacy infrastructure around the world. To see the comprehensive options of OPSWAT's variety of data diodes and unidirectional gateways, you can view the product comparison chart here.

This announcement builds on OPSWAT's strategic growth momentum, following its acquisition of InQuest earlier this year.

LANTRONIX PARTNERS WITH TECHBRIDGE DISTRIBUTION MEA TO ELEVATE IOT CONNECTIVITY IN THE MIDDLE EAST

(L-R) Kurt Hoff, vice-president, WW Sales from Lantronix & Steve Lockie, Managing Director of TechBridge.

Lantronix Inc., a global leader in IoT compute and connectivity IoT solutions, recently announced its strategic partnership with TechBridge Distribution MEA.

This collaboration aims to bring Lantronix's progressive IoT and M2M solutions to the rapidly growing Middle Eastern market.

"We are proud to collaborate with TechBridge Distribution MEA," said Kurt Hoff, vice-president, WW Sales from Lantronix. "Our cutting-edge solutions, including our Out-of-Band (OOB) management technology, will enable Middle Eastern businesses to elevate their connectivity and operational resilience. By integrating Lantronix's secure, remote IoT management into TechBridge products, we will help this region's companies reduce downtime and operating costs while delivering technology designed for tomorrow's IoT landscape".

Steve Lockie, Managing Director of TechBridge, added: "This partnership is an excellent fit for our mission to offer premium solutions across the Middle East and Africa. Lantronix's focus on edge intelligence and remote troubleshooting provides a competitive advantage that the region's businesses need. Their OOB solutions particularly align with our goal to offer secure and efficient IoT systems, making us confident in our ability to set new standards in connectivity".

Founded in 1989, Lantronix has built a reputation for delivering ruggedised cellular communication and industrial IoT gateways. Their 30+ years of expertise in industrial automation ensures reliable, scalable, and flexible solutions. Unlike competitors who compromise between cost and functionality, Lantronix excels in offering real-time data monitoring and resilient IoT infrastructure—making their products both affordable and robust.

The partnership with TechBridge MEA strengthens both companies' foothold in the Middle East. TechBridge's Channel focused value-added distribution model and extensive network, combined with Lantronix's leading technologies, promise to address the region's demand for reliable, scalable IoT solutions. The combined strengths of both companies will help businesses reduce costs, improve customer experiences, and launch new business models with greater efficiency.

Successful case studies from Lantronix demonstrate the company's ability to remotely manage industrial assets securely and efficiently, setting them apart from competitors offering either expensive or unreliable solutions. With this partnership, TechBridge Distribution MEA and Lantronix are poised to deliver unparalleled IoT connectivity solutions, enhancing customer experience and operational efficiency across the Middle East

BEYONDTRUST APPOINTS JIM ORTBALS AS SVP OF GLOBAL PARTNER ECOSYSTEMS

- Jim Ortbals brings 25+ years of channel experience to lead BeyondTrust's global partner strategy
- Strategic hire underscores BeyondTrust's ongoing commitment to further develop and execute a global partner strategy to support today's diverse channels and partner business models

BeyondTrust, the global cybersecurity leader protecting Paths to Privilege, has announced the appointment of Jim Ortbals as senior vice-president of Global Partner Ecosystems. With over 25 years of channel leadership across tech giants such as Cisco, VMware, Zscaler and Deep Instinct, Jim brings a track record of building high-performing ecosystems that deliver real results.

"Jim's proven ability to empower partners and drive business growth makes him an ideal leader to take BeyondTrust's partner ecosystem to the next level," said Brent Thurrell, Chief Revenue Officer at BeyondTrust. "His visionary approach to building collaborative alliances and supporting programs aligns perfectly with our mission to protect Paths to Privilege for our customers and partners worldwide."

At BeyondTrust, Jim will spearhead the global channel strategy, emphasizing market share growth through the company's growing global partner ecosystem. BeyondTrust remains committed to advancing its channel momentum by enhancing partner engagement and enablement, utilizing intellectual property, and providing strategic and financial support to partners. These elements are integral to a world-class channel framework and underscore BeyondTrust's dedication to partner success.

"My channel philosophy is to help partners develop innovative and disruptive solutions building upon world-class technology with their own unique set of capabilities to deliver transformative outcomes to our joint customers," said Ortbals. "I'm excited to join the BeyondTrust team and look forward to working closely with our partners to drive meaningful growth and shared success."

INTEL APPOINTS ENG. TAHA KHALIFA AS THE GENERAL MANAGER FOR MIDDLE EAST AND AFRICA

TAHA KHALIFA, GENERAL MANAGER, INTEL-MIDDLE EAST AND AFRICA REGION

Intel announced the appointment of Eng. Taha Khalifa as the General Manager for the Middle East and Africa region. With more than 25 years of experience in the ICT industry, Taha has assumed a range of senior engineering, strategic planning, sales and management roles inside the company in both the US and EMEA. Most recently he was the Client Computing Group Sales Director for Intel in EMEA, leading the execution of Intel's client strategy and growth in the commercial segment.

Taha, who formerly assumed several channel, sales and marketing leadership roles in Middle East, will now lead Intel's operations in a broader region with one of the world's highest digital transformation and economic growth potential. In his new role, Taha will oversee the execution of Intel's strategy across a diverse ecosystem of customers, partners, OEM's and distributors while aligning with governments and industry leaders to advance the region's ICT capabilities and corporate social responsibility efforts. His extensive background and leadership in the region position him well to lead Intel's growth strategy and technology leadership in the Middle East and Africa.

Taha Holds a Bachelor's and a Master's degree in Computer Engineering and an MBA from Arizona State University (US).

SUHAIL HASANAIN APPOINTED REGIONAL SENIOR DIRECTOR FOR NETAPP MEA

HASANAIN WILL ALSO BE LEADING NETAPP'S REGIONAL HEADQUARTERS IN RIYADH

NetApp, the intelligent data infrastructure company, appointed Suhail Hasanain as the new Regional Director for the Middle East and Africa region. In his new role, Suhail will be responsible for driving business growth, fostering strategic collaborations, with continuous development of the ecosystem and delivering exceptional results across all sectors in the region. Additionally, Suhail will lead NetApp's regional headquarters for the Middle East and Africa region in Riyadh, Saudi Arabia, to be officially open on February 1, 2025.

With over 20 years of experience in strategic planning, operational excellence, and leadership, Suhail brings a wealth of expertise to his new position. His in-depth understanding of customer and partner needs, combined with his ability to bring together cross-functional teams, will be instrumental in driving NetApp's success in the Middle East and Africa.

Prior to joining NetApp, Suhail led Dell's multi-cloud offerings in Saudi Arabia, where he successfully negotiated multi-year mega-frame contracts with government entities. His dedication to customer and team excellence has been evident throughout his career, making him a valuable asset to any organization.

As the Regional Senior Director for Middle East and Africa, Suhail will leverage his extensive experience and leadership approach to forge strategic collaborations with regional ecosystem, drive business growth, and ensure that NetApp's solutions and services meet the unique needs of customers in the region. Leading the regional headquarters in Riyadh, Suhail will play a pivotal role in strengthening NetApp's presence and operations in Saudi Arabia.

"We are delighted to welcome Suhail Hasanain to the NetApp team as our new Regional Director for the Middle East and Africa," said Jose Petisco, EEMi Vice-president at NetApp. "Suhail's proven track record, expertise, and passion for delivering exceptional results make him the ideal candidate to lead our operations in this strategic region. He will be base in Riyadh, to further enhance our commitment with customers in Saudi Arabia."

Suhail's appointment reflects NetApp's commitment to attracting top talent and bolstering its leadership team. With his extensive experience and deep understanding of the market, Suhail is well-positioned to drive NetApp's growth and success in the Middle East and Africa.

"We are honored to support the Kingdom's journey towards an AI-driven, diversified economy and help shape a more sustainable, technologically advanced future. This appointment is another testament to our commitment to KSA", added Jose Petisco.

CORO BOLSTERS CYBERSECURITY FOR SMES AND STARTUPS

EXPLORING CORO'S PROACTIVE CYBERSECURITY SOLUTIONS IN THE DYNAMIC DIGITAL LANDSCAPE OF THE MIDDLE EAST, WITH INSIGHTS FROM PIERS MORGAN, SENIOR VICE-PRESIDENT AND GENERAL MANAGER - EMEA

The UAE has positioned itself as a global leader in cybersecurity by proactively adopting cutting-edge solutions to safeguard its burgeoning digital landscape. With a robust regulatory framework and strategic initiatives like the National Cybersecurity Strategy, the UAE prioritizes the protection of its critical infrastructures and business ecosystems. This commitment is reflected in the deployment of advanced technologies such as AI-driven threat detection and blockchain for secure transactions.

The proactive efforts ensure that both large corporations and SMEs operate in a secure environment, effectively minimizing risks and enhancing business continuity in the face of increasing cyber threats.

Piers Morgan, Senior Vice-President and General Manager - EMEA, Coro, spoke to Sandhya D'Mello, Editor, Technology Division, CPI Media Group, on its top priority to address the cybersecurity challenges faced by SMEs and startups and be their cyber-partner to ensure seamless and protected operations.

Coro stands out as one of the most rapidly expanding security solutions tailored for the mid-market, offering comprehensive protection that enables organizations to combat a spectrum of cyber threats including malware, ransomware, phishing, bots, and account takeovers across various platforms—devices, users, and cloud applications.

Over 5,000 businesses rely on Coro for all-encompassing security, unparalleled simplicity in operation, and exceptional cost-effectiveness. Leveraging advanced AI technology, Coro proactively detects and addresses numerous security challenges faced by today's dispersed businesses, allowing IT teams to focus on strategic initiatives rather than managing and troubleshooting security issues.

Your journey in Dubai began 27 years ago, and today, you are in an emirate that is at the forefront of digital transformation. Having witnessed this change firsthand, could you provide insights into how you see this nation leading in the Middle East?
From my perspective, Dubai, UAE, and the entire Middle East are experiencing an exciting time. I remember coming here 25 years ago, staying at the old Hard Rock Cafe where Sheikh Zayed Road actually ended. Since then, I have been returning here three or four times every year, both for business and pleasure. I have many friends and business contacts here, and the vibrancy of the current digital transformation process that many companies are undergoing is truly remarkable. We'll discuss this a bit later, particularly looking at cybersecurity services and how they can protect the established and emerging companies that we see developing all the time in this region. So yes, for me, I love coming here and hope that continues.

Considering the increasing digital transformation in the Middle East, how critical is cybersecurity today? You could explain it from a B2C or even a B2B point of view.?
I think it encompasses all B2B, B2C, even C2B. We see it in the newspapers, online every single day, around the globe. The bad guys, the threat actors, are constantly looking for weaknesses, particularly in certain markets. We at Coro like to think that we are protecting many of those organizations as we specialize within the SME and SMB market spaces. Cybersecurity is needed by everybody here in the UAE or across the Middle East, in Europe, in North America, out in Asia Pacific.

CORO
StorIT
Making C...security Easy ...ness
Coro cybersecurity r... a click of a button.
N...
One pane of glass, o... driven data engine.
One security p... es you need.

We're seeing requirements from both a regulatory perspective and a compliance perspective, and that is now filtering down to both startup companies and small to medium corporate organizations or businesses. We see it every day, and despite recent downturns in economies, cybersecurity is still absolutely relevant.

Is Coro planning to open an office in the region?
I joined Coro recently, and my responsibility is to expand the EMEA region. As a part of our phase one growth program, we will be establishing a presence and opening offices here. However, it's not crucial for us to have a physical office here, as we have excellent partners and distributors.
Through my personal experience and the teams that we're establishing in the region, we are well-connected and 100% committed to investing in both personnel and technology in this region, while introducing our services. We have already achieved a degree of success in a mini road show that I've been participating in over the last couple of weeks. Our team has just been at Black Hat in Riyadh, and we attended Gitex this year. We plan to attend GISEC next year.

I'm very excited by this region and what it has to offer, but more importantly, by how we can introduce our cost-effective, flexible, modular-based cybersecurity solutions that will be very helpful for the SMB customers in the Middle East and North Africa that I mentioned earlier.

Can you name top three markets that have contributed to Coro's growth journey out of the Mena region?
The UAE presents a nascent market opportunity, as our establishment is still underway. Coro, as a business, has experienced substantial global growth within the last three years, with a year-on-year revenue increase ranging between 300% and 400%. We are disrupting the traditional cybersecurity market; our offerings are novel to partners, distributors, and customers alike. Differentiation and simplicity are paramount; cybersecurity can often be convoluted and misunderstood. We aim to eliminate this complexity within our target markets. Our single-based user platform and single pane of glass management system provide streamlined access, offering customers both choice and a unified management solution.

300
to 400% growth trajectory projected year-over-year at the end of 2024

WE AT CORO ARE COMMITTED TO BEING MORE THAN JUST A SERVICE PROVIDER; WE AIM TO BE A CYBER-PARTNER FOR SMES AND STARTUPS, ENSURING THEY CAN OPERATE SEAMLESSLY AND SECURELY. THIS IS VITAL AS BOTH THE FREQUENCY AND SOPHISTICATION OF CYBER THREATS INCREASE GLOBALLY.

How many channel partners or resellers are you currently leading, and what specific strategies do you employ to manage these relationships?
As we are still in the early stages, we are actively signing up channel partners on a daily basis through our strong relationships here, especially with StorIT. We engage with various types of partners including MSPs, MSSPs, value-added resellers, ISVs, and system integrators. We tailor our cybersecurity solutions to meet the specific needs of their businesses and offer their customers a range of options, from endpoint agents to comprehensive services like email security, SASE, EDR, NDR, and XDR. Our approach is to work closely with these channel partners who understand their customers' needs better than anyone. One standout partner in the UAE is MMA InfoSec, a high-growth company that provides full managed services and security operations centers. However, our focus isn't limited to a single partner; it's about leveraging the entire ecosystem to ensure our services are understood and valued in the market. Additionally, we aim to simplify the security landscape for these companies, many of which have been overwhelmed with multiple security tools generating thousands of alerts. With the Coro platform, we can reduce these to a manageable number, making it easier for SMBs without large IT teams or CISOs to handle their security needs effectively.

Can you explain how Coro's Cyber Security Platform, specifically tailored for SMEs, differs from solutions designed for larger enterprises?
Since we entered the market in 2015, the initial years were dedicated to research and development, crafting our platform and services, and establishing a clear roadmap. One key observation we've made is that the needs of SMEs (Small and Medium-sized Enterprises) are often overlooked by many cyber service providers who typically target larger corporate accounts. They attempt to fit enterprise-grade security solutions into the SME context, which doesn't always align with the actual needs of smaller businesses.

SMEs, especially in our region, are mostly companies with up to 500 users,

sometimes even 350 in terms of endpoint or agent count. Our approach at Coro is to simplify the cybersecurity process for these businesses, which often do not have extensive in-house expertise. We offer an "a la carte" menu of 14 different cyber modules, allowing SMEs to select and combine different solutions or opt for specific bundled offerings according to their needs. This flexibility allows us to tailor our solutions to be both scale-appropriate and budget-friendly, providing a competitive commercial proposition that resonates with the specific dynamics and capacities of SMEs.

In essence, we're disrupting the traditional cybersecurity market by offering a platform that is not only effective but also adaptable to the unique challenges and constraints faced by SMEs, ensuring that they are no longer the 'forgotten' group in cyber defense strategies.

In today's complex digital landscape, with an overwhelming array of cybersecurity solutions, what are your top three tips for entrepreneurs in the SMB sector to navigate these choices effectively?

Navigating the cybersecurity landscape as an entrepreneur, especially within the SMB sector, can indeed be daunting given the rapid evolution of technologies like AI and generative AI. Here are three crucial tips to help entrepreneurs make informed decisions:

Understand Your Unique Needs: Every business has its own specific requirements and vulnerabilities. It's essential to thoroughly assess your business model, data sensitivity, and potential risks. Understanding these elements helps in choosing cybersecurity solutions that are not just popular but truly pertinent to protecting your specific assets.

Stay Educated and Informed: The cybersecurity landscape is dynamic, with new threats and solutions emerging regularly. Entrepreneurs should invest time in continuous learning about new threats and cybersecurity trends. This knowledge is critical in making informed decisions rather than relying solely on CIOs or CISOs.

Leverage Expertise: While it's important for entrepreneurs to be informed, collaborating with experienced cybersecurity providers can alleviate much of the burden. Providers like us offer flexibility and adaptability in our services, allowing businesses to focus on their core operations while we handle the complexities of cybersecurity. We guide our customers through the process, ensuring they are cyber-aware and their employees are trained on the significance of cybersecurity.

With these tips, entrepreneurs can better manage their cybersecurity needs, ensuring their ventures are protected against the prevalent threats that unfortunately see many startups falter in their initial years.

Could you elaborate on the Coro Academy and its offerings, particularly how it supports organizations in educating their staff on cybersecurity?

Coro Academy is an integral part of our approach to cybersecurity, designed to offer comprehensive educational resources for organizations. With over 25 years of experience in the industry, we've recognized the need for specialized cybersecurity education tailored to specific organizational needs.

At Coro Academy, we offer a variety of modules focused on cyber awareness training. We start by assessing an organization's existing cybersecurity infrastructure to identify any gaps. Based on this assessment, we provide targeted training and knowledge enhancement sessions to secure these vulnerabilities. Our training modules are crafted to address everything from basic cyber hygiene to advanced security protocols.

Moreover, the Coro Academy team operates globally, delivering these educational resources both in-person and through online modules. We also provide certifications for both technical skills and commercial go-to-market strategies, primarily aimed at our channel partners. As our business evolves, these certifications become increasingly relevant, especially in regions where demonstrating expertise through credentials is highly valued.

Overall, Coro Academy aims to empower organizations by equipping their staff with the necessary skills and knowledge to maintain robust cybersecurity measures, thus enhancing their overall security posture.

What advancements and innovations can Coro's customers anticipate in the platform in the upcoming years?

Looking ahead, Coro is committed to continuously enhancing our cybersecurity platform, ensuring it remains at the forefront of technology and service delivery. Our platform is designed to be a dynamic learning system, constantly evolving through both human oversight and artificial intelligence (AI) capabilities. The AI component is crucial, as it continuously absorbs and processes information, improving with every interaction and data point it encounters.

In the coming years, we plan to further develop our services within the platform and extend these advancements to various global markets through our eco-systems. This development is not just about keeping pace with the market but leading it by simplifying interactions and being easy to do business with—a contrast to the complex and often dictatorial approaches seen elsewhere in the industry.

Our approach involves actively listening to and learning from our customers' experiences and feedback. This information is invaluable as we refine our processes and enhance the AI's learning capabilities within the central Coro platform. By integrating these insights, our platform can better adapt, learn, and deliver tailored and flexible solutions that meet the evolving needs of our growing customer base. This strategy ensures that our platform not only responds to current cybersecurity challenges but also anticipates future needs, thereby providing robust, proactive protection for our clients.

Can you share a memorable case study where the Coro platform notably impacted a client, particularly in a crisis scenario, without needing to specify the client's name?

Absolutely, I'd be happy to share a general example that underscores the adaptability and effectiveness of the Coro platform across various industries. We serve around 20,000 customers globally, spanning sectors like healthcare, manufacturing, retail, financial services, and automotive, among others. Our goal is to avoid being confined to any single sector, emphasizing our solution's flexibility.

One case that particularly stands out involves a crisis scenario in the SMB space, where our platform demonstrated its robust capabilities. We encountered a situation where thousands of alerts overwhelmed an IT manager, waking them at 3:30 am with fears of a network crash or a ransomware attack. Upon intervention, it turned out many of these alerts were false positives—just noise. Our platform not only resolved these issues but also adjusted our service level agreements to ensure that IT managers could rest easier, knowing their systems were monitored and protected efficiently.

Our solution's intuitive design allows for rapid deployment, with modules capable of being set up in as little as two minutes. This swift response time, combined with our commitment to cost-effective and scalable cybersecurity, ensures that our clients can rely on us to handle the 'heavy lifting' of cybersecurity, allowing them to focus on their core business functions. This approach not only helps in immediate crisis management but also builds a foundation for ongoing security and peace of mind.

How do you anticipate the end of 2024 in terms of growth compared to 2023, particularly within this region?
Looking forward to the close of 2024, we are optimistic about our growth trajectory, projecting an impressive year-over-year increase of at least 300 to 400% globally. This growth is not just in numbers but also reflects our deepened commitment and investment in specific regions, including significant efforts here. We have dedicated considerable resources—time, personnel, and financial—to this area, reflecting our strong belief in its potential.

As we approach the end of the year and look towards the future, our focus remains on strengthening our market presence. We are finalizing foundational aspects of our operations and have established solid routes to market. Additionally, we've launched a new channel program tailored to this region, designed to engage and support channel partners who are interested in collaborating with us. We encourage potential partners to join this program, through which we aim to provide substantial support, investment opportunities, and avenues to monetize our services together. This strategy underscores our commitment to not only expanding our footprint but also enhancing our collaborative efforts to achieve sustained growth and success in the region.

Do you have a message for our readers and potential partners?
Absolutely! I encourage everyone to explore what Coro has to offer, especially if you're grappling with the complexities of cybersecurity. Our platform is designed to simplify cybersecurity while delivering corporate-grade service, making it ideal for small to medium enterprises that may not have dedicated IT teams or CISOs. But it's also robust enough for larger companies that face numerous cybersecurity challenges.

I am particularly enthusiastic about this region and the potential it holds. I look forward to continuing to engage with local businesses, listening to their needs, and understanding the challenges they face. For channel partners and corporate customers interested in collaborating, I invite you to reach out. Let's forge partnerships that not only address your cybersecurity needs but also allow us to make a significant impact together in the market.

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

SENTINELONE CHARTS STRATEGIC PATH FOR 2025 WITH ENHANCED CYBERSECURITY INITIATIVES

EXPLORING SENTINELONE'S STRATEGIC ADAPTATIONS AND TECHNOLOGICAL ADVANCEMENTS IN RESPONSE TO THE DYNAMIC CYBERSECURITY MARKET CONDITIONS OF 2024.

In 2024, SentinelOne faced a cybersecurity environment marked by both formidable challenges and unprecedented opportunities. Meriam ElOuazzani, Senior Regional Director, META, SentinelOne spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, on how from adapting to evolving threats to advancing their technological capabilities, the company has actively shaped its strategies to not only meet current demands but also set the stage for 2025. This proactive approach has been crucial in reinforcing their commitment to innovation and customer support, particularly through initiatives like the autonomous SOC and enhancements to their Singularity Platform.

Can you discuss the dual nature of challenges and opportunities SentinelOne faced in the cybersecurity market in 2024, and how these experiences are shaping your strategic initiatives for 2025?

The year 2024 has presented both challenges and significant opportunities, particularly within the cybersecurity market. We have encountered a range of issues, from evolving threats to direct attacks, and we understand the daily challenges our customers face. It is essential that we consider what support we can offer, whether as consultants helping to devise robust cybersecurity strategies or by enabling our partners and distributors to enhance their services.

Looking ahead to 2025, we see a landscape full of opportunities due to the groundwork SentinelOne has laid to bolster digital transformation and meet cybersecurity needs. We are already planning major initiatives and making commitments for the upcoming year with a focus on advancing technology, addressing customer needs, and empowering our channel and partners.

The cybersecurity field is exhilarating; it is constantly evolving. Every day brings new developments, and every few months, we announce updates or innovations to our offerings. For instance, we envisioned an autonomous SOC, and within five months, we began implementing that vision. Our customers' drive for innovation spurs us to continue innovating and finding ways to remain relevant. This dynamism is thrilling, and I appreciate being a part of it—especially at SentinelOne, where we are making a substantial impact with our technology. We have a lot to offer, and sharing this with our customers is profoundly rewarding.

What did you showcase at Black Hat Middle East this year?
Black Hat MEA provided a valuable opportunity to network and explore collaborations. We showcased our AI-driven approach and solutions, emphasizing our autonomous SOC and its benefits. Additionally, we introduced new capabilities of Purple AI and updates to our Singularity Platform, highlighting our Singularity Hyperautomation and Singularity AI SIEM.

Have you encountered situations where you had to challenge prevailing attitudes? For instance, clients may be hesitant to adopt new solutions due to concerns about the return on investment or the perceived necessity. How do you manage these objections?
Initially, customers may feel overwhelmed by the number of AI-based security solutions available. They may be unsure of how to prioritize and implement these solutions and how to measure ROI. Some customers may also be resistant to changing their existing cybersecurity strategy, while others may not see the need for a comprehensive strategy.

We guide customers to understand the necessity of a multi-layered security approach that utilizes multiple technologies to protect different surfaces. We emphasize that protection alone is not enough and that detection and response are also critical components of a successful cybersecurity strategy.

We work with customers to develop and implement a cybersecurity strategy that is tailored to their specific needs. Our technology is modular, so customers can start with any service and expand as they grow. We also offer flexible solutions to accommodate different customer needs and budgets.

With SentinelOne's strong presence in the Middle East and Africa, which markets do you see as the top three drivers in the region?
The Gulf is very important to us. We look at Saudi Arabia and the UAE as transformational markets, but we're also seeing strong growth in other regions. These markets are facing significant cybersecurity challenges, and we see increased activity from threat actors, particularly in Africa. This has heightened customers' awareness of the need to build secure infrastructures for their organizations. Additionally, we see great opportunities in Kuwait and Qatar. We're expanding rapidly in the Middle East, as well as in Turkey and Africa.

Could you identify the top three economic sectors where you observe significant adoption of cybersecurity solutions to enhance proactive operations and security?
Cybersecurity is primarily a data problem. What I mean by that is the amount of data, how we need to correlate it, and the noise that comes with it. There's also a lack of integrations - though across the IT and security fields, we are still working on many integrations - and the need for more automation. The real problem is how to handle data, particularly when customers have large amounts of it, combined with the need to ensure privacy and protect that data.

These customers are top priorities for any cybersecurity company. What's different now is which industries are prioritizing cybersecurity. We see a significant need for cybersecurity transformation in government, oil and gas, banking, and healthcare. We have customers across all these industries.

Cybersecurity has become a primary focus because organizations now have their brand, data, and privacy to protect. They need to implement a cybersecurity strategy and execute it. Security is no longer optional - it's a must. It's no longer a choice but a part of every CIO's or CTO's strategy to ensure data and privacy are properly managed.

Can you explain how SentinelOne's Singularity Hyperautomation simplifies security workflows and automates responses?
The autonomous SOC, announced five months ago, facilitates threat hunting and enables security analysts to identify threats and respond automatically through Singularity Hyperautomation, an intelligent, no-code technology. By using automation to create workflows and queries, and Purple AI to write simple queries, analysts can focus on more advanced tasks. This allows customers to stay ahead of threats, make strategic decisions, identify and act on true positives, reduce false positives, and ensure better asset compliance and monitoring, enabling faster response to targeted threats.

At OneConnect Dubai, you mentioned that cybersecurity is now a battlefield of "AI versus AI." How does SentinelOne navigate this landscape?
AI is used by both cybersecurity companies and threat actors, making the field a battle of AI vs AI. Companies must stay ahead by constantly improving technology. Protection alone is not enough; visibility is also crucial for identifying and recovering from threats quickly. The Singularity Platform offers a multi-layered security approach, including EDR, XDR, endpoint protection, identity protection, cloud security, and AI SIIM. The platform provides advanced technologies in a simple way, with various services to support customer teams. While not everyone is in the IT and security business, everyone has data to protect, and innovative solutions are key to staying ahead of threat actors.

> **EVERY DAY IN CYBERSECURITY IS EXHILARATING; IT'S A REALM WHERE INNOVATION IS NOT JUST ENCOURAGED BUT ESSENTIAL FOR SURVIVAL**
>
> *MERIAM ELOUAZZANI, SENIOR REGIONAL DIRECTOR, META, SENTINELONE*

KNOW YOUR IDENTITY

CNME EDITOR MARK FORKER SPOKE TO LOTHAR RENNER, MANAGING DIRECTOR, SECURITY SALES AND ENGINEERING AT CISCO EMEA, AHEAD OF THEIR PARTICIPATION AT BLACK HAT MEA IN RIYADH LAST MONTH, TO LEARN MORE ABOUT WHY THE US TECHNOLOGY BEHEMOTH IS ADVOCATING FOR AN 'IDENTITY-FIRST APPROACH TO SECURITY, THE NEW VARIANTS EMERGING WITHIN RANSOMWARE, THE IMPORTANT ROLE THE CISCO NETWORKING ACADEMY WILL PLAY IN ADDRESSING THE GLARING SKILLS GAP GLOBALLY – AND THE ROLE OF GEN AI IN THE CYBERSECURITY LANDSCAPE.

CISCO EMPLOYS A MULTI-LAYERED APPROACH THAT INTEGRATES ADVANCED AUTOMATION CAPABILITIES WITH STRATEGIC HUMAN INTERVENTION TO ENSURE ROBUST AND EFFECTIVE INCIDENT MANAGEMENT.

Lothar Renner is one of the most respected and revered sales leaders in the cybersecurity ecosystem globally having spent almost a quarter of century at Cisco.

CNME Editor Mark Forker caught up with Lothar Renner for the first time since the pair spoke face-to-face at GISEC 2024 in April.

Such is the nature of the technology sector, there has been huge changes across the industry in the six months that have elapsed since the pair last spoke.

Renner was in Riyadh for Black Hat MEA, which is the region's flagship cybersecurity conference.

So, there was no better time to pick Renner's brains on the challenges currently engulfing the cybersecurity world.

Ahead of the interview, Cisco's Talos IR Trends Report for Q3 had just been published, and that's where we kickstarted our conversation.

Renner stressed the need for enterprises to adopt an 'identity-first' approach to security.

"Identity is the fabric that connects humans, devices and applications in the workplace, and has become an easy target for modern cybersecurity attacks. Organizations need to adopt an identity-first approach to security, which among other things allows them to evolve from just asking 'can' a user access a system to continuously assessing whether a user 'should' be able to do what they are doing once they are authenticated. That really is the key, the mindset needs to shift, businesses really need to determine regardless of authentication processes, who really needs the access to their systems," said Renner.

There are many reasons why Cisco has sustained its success over such a long period of time, but one of the key market differentiators over the years for them has been their ability to simplify.

When it comes to security, Cisco are in the business of simplification.

"That's why in Cisco Live EMEA last year, we unveiled new innovations within the Cisco Security Cloud to simplify security: Cisco Identity Intelligence and continued innovation in AI capabilities are the latest milestones towards its vision of a unified, AI-driven, cross-domain security platform. Cisco Identity Intelligence brings together identity, networking and security to better protect organizations' complex identity stack against increasingly sophisticated attacker techniques," said Renner.

Identity attacks may be in vogue when it comes to cybersecurity, but ransomware remains a huge problem, and as Renner points out the report from Cisco Talos indicates that new variants of ransomware attacks have emerged.

"As part of a years-long trend in greater democratization of ransomware adversaries, we continue to see new variants and ransomware operations emerge. A third of these engagements involved exploitation of known vulnerabilities that are consistently leveraged by ransomware operators/affiliates to deploy ransomware, according to public reporting. Some of those vulnerabilities carried CVE numbers from 2023 - which means we in the industry need to get better at vulnerability management and patching. At the same time, we need to prepare ourselves for the incident to happen, which is why we need the creation of incident response plans and playbooks," said Renner.

The issue when it comes to the skills shortage is a huge problem that many business leaders across the global IT and technology industry have been bemoaning over the last number of years.

Unfortunately, it appears that the situation will likely become more of a challenge before it gets better.

A lack of skills in relation to AI has been well documented, but there is a real crisis when it comes to talent in the cybersecurity industry globally.

However, Renner believes Cisco's Networking Academy can go a long way to plugging the gaps that currently exist.

It is a global problem. Four million professionals are urgently needed to plug the talent gap in the global cybersecurity industry. Attracting, training and retraining cybersecurity professionals is key to helping organizations and society stay safe online. At Cisco, we are dedicated to equipping professionals with the skills necessary to enhance their careers and bridge the skills gap. Cisco Networking Academy is one of the world's longest standing IT-skills-to-jobs programs that partners with learning institutions worldwide. Specifically in the Middle East and Africa region, since the inception of Cisco Networking Academy, we have trained more than 4.3 million learners on digital skills, with focus on cybersecurity and networking. In Cisco's 2024 fiscal year alone, more than 1.1 million students were trained across 2,000+ academies in the region," said Renner.

There have been seismic changes across the Middle East region when it comes to digitalization.

The sheers speed and scale of the transformation programs, particularly in the UAE and the KSA are unprecedented globally.

However, as a consequence of all of that transformation, the term 'cybersecurity readiness' has come under the microscope more and more across the Middle East.

In order to help nations across the Gulf accelerate their transformation, Cisco is leveraging their expertise in security to help them protect their key assets.

Renner highlighted how their One Platform vision was taking shape.

"For security to be both simplified and strengthened, it needs an AI-driven, comprehensive platform that seamlessly integrates with an organization's IT infrastructure. This vision aims to address the complexities of modern cybersecurity challenges by providing a holistic, intelligent, and automated approach to threat detection, response, and management. We are increasing our focus on cybersecurity in the region with the acceleration of digitization we're witnessing in most of the Middle East nations. Early this year, we have launched a new local cloud data centre in the UAE for our Duo multifactor authentication (MFA) and secure access solution, that support businesses of all sizes in strengthening their cybersecurity posture and improving connection performance," said Renner.

Cisco's cybersecurity readiness index for the UAE and the KSA showed that a high number of respondents have suffered a cyberattack.

Renner highlighted his belief that a multi-layered approach is the best tactic to adopt to combat modern cyberattacks.

"According to Cisco's Cybersecurity Readiness Index in UAE and KSA: 65% of UAE respondents and 67% of KSA respondents already experienced a cybersecurity incident in the past year. In today's rapidly evolving threat landscape solely relying on human-scale defence is no longer enough. Comprehensive security calls for machine-scale capabilities. Cisco employs a multi-layered approach that integrates advanced automation capabilities with strategic human intervention to ensure robust and effective incident management," said Renner.

In relation to Gen AI, Renner concluded a brilliant exchange by declaring that attackers are constantly developing new strategies and tools – whilst he stressed the need for organizations to stay ahead of these threats by enhancing their cybersecurity posture.

"Our latest innovation, the Cisco Hypershield: is designed to power and protect the engine of the AI revolution, which is AI-scale data centres and clouds. Backed by Talos – Threat Intelligence: 800 billion security events observed per day, 200+ vulnerabilities discovered per year. Cisco is committed to equipping our customers with the tools, products, solutions and services they need to stay protected at all times, amidst a threat landscape that is continually evolving," said Renner.

ORGANIZATIONS NEED TO ADOPT AN IDENTITY-FIRST APPROACH TO SECURITY, WHICH AMONG OTHER THINGS ALLOWS THEM TO EVOLVE FROM JUST ASKING 'CAN' A USER ACCESS A SYSTEM TO CONTINUOUSLY ASSESSING WHETHER A USER 'SHOULD' BE ABLE TO DO WHAT THEY ARE DOING ONCE THEY ARE AUTHENTICATED.

THE FUTURE OF IDENTITY SECURITY: AI-DRIVEN INNOVATIONS RESHAPE IAM LANDSCAPE

DISCOVER HOW GENERATIVE AI AND EMERGING TECHNOLOGIES ARE SETTING THE STAGE FOR THE NEXT ERA OF IDENTITY AND ACCESS MANAGEMENT.

Identity and Access Management (IAM) is maturing, and the integration of Artificial Intelligence (AI) is becoming a necessity. With the landscape of identity security evolving rapidly, organizations are increasingly adopting AI-driven solutions to streamline and secure their operations.

P. Sathyamurthy, Sales Director, IDM Technologies LLC spoke to Sandhya D'Mello, Technology Editor, CPI Media Group, on how innovations like passwordless authentication, zero-trust frameworks, and AI-enhanced threat detection are pivotal as businesses look towards 2025 and beyond. This shift promises a more efficient, secure, and user-friendly approach to managing digital identities, making AI integral to the future of cybersecurity.

Identity and Access Management (IAM) has reached a high level of maturity in recent years. Could you share your insights on what the future holds for Identity Security?

As the identity Security landscape evolves at an unprecedented pace, staying ahead of emerging trends is crucial for organizations seeking to proactively bolster their defenses. In this regard, I see a good percentage of organizations utilizing generative AI, will significantly improve the user experience and efficiency of their IAM controls. We will also see a rise in adoptions like passwordless authentication, zero-trust security, AI-powered threat detection, cloud identity security, and managing IoT machine identities.

Looking ahead to 2025 and beyond, what key trends do you anticipate will shape the landscape of Identity Security?

In my opinion, AI will consolidate data from a wide array of sources, such as user access logs, device metadata, network traffic, and application interactions, by creating a comprehensive dataset for analysis. Then AI will establish detailed profiles for users and devices by analyzing historical data. This profiling will help distinguish between regular and irregular behaviors. Whereby AI will assess the context of access requests (like time of day, location, device type, etc.) to determine the risk levels. If there are higher-risk contexts, it triggers more stringent authentication methods. Finally, upon identifying potential threats, AI can automatically implement countermeasures, such as revoking access, initiating password resets, or isolating affected systems, thereby minimizing response time.

What are the critical elements necessary for successful AI adoption within IAM frameworks?

The key elements for a successful and effective AI in IAM strategies are integrating data from multiple sources, providing a holistic view of user and entity behaviors across the network, and enabling better threat detection. However, beyond identifying anomalies, predictive analytics forecast potential security incidents by recognizing early warning signs, and allowing preemptive actions. Also, continuously monitoring not just users but also devices and other entities within the network, to detect subtle signs of potential compromise. By implementing dynamic risk assessment processes that adjust based on real-time data, ensures that security measures are appropriately scaled to the assessed risk level. Furthermore, utilizing AI to automate routine security tasks and responses, frees up human resources to focus on more complex security issues, and ensures consistent and swift reactions to threats.

How can AI transform Identity Security for organizations? Are there specific enhancements or capabilities that AI brings to the table?

By incorporating AI in IAM, organizations can analyze behavior and detect anomalies in real-time, allowing for the early identification of potential security threats. AI will improve the accuracy of threat detection, reducing the number of false positives and allowing security teams to focus on genuine threats. AI also enables seamless and secure access through adaptive authentication, reducing friction for legitimate users. Whereby ensuring regulatory compliance by providing detailed logs and reports of all access events. Finally, AI-driven IAM solutions can effectively scale with the organization's growth, managing an increasing number of identities and access points.

Which client sectors or verticals are most in need of integrating AI into their IAM solutions, and why?

Though any organization will benefit from using AI in IAM, I see the sectors that will adopt early and take advantage the most are financial institutions, healthcare, governments, and large enterprises, to name a few.

Given the shift towards digital transformation, are clients ready to migrate their IAM services to the cloud? What are the perceived benefits or challenges in making this transition?

The Identity Security solutions are mature, and enterprises globally and regionally are adopting them. As more cloud-native IAM and PAM vendors commit to the region, the readiness of regional cloud DCs will enable enterprises to decide and move to the cloud confidently. Though we are still early in this migration process, I encourage enterprises to step into the cloud-native journey without concern.

6 MIDDLE EAST CYBERSECURITY PREDICTIONS FOR 2025, BY QUALYS

RICHARD SEIERSEN, CHIEF RISK TECHNOLOGY OFFICER, QUALYS

Oceans of clouds, containers, endpoints, IoT devices, first- and third-party networks — for the modern Middle East security team, there is a lot to watch and a lot to do. As 2025 dawns, the CISO must question the status quo and ask themselves how things need to change in the coming year. Is AI a risk that requires a new security strategy? Could it also be the answer to facing down a threat landscape that is scaling up in terms of both volume and stealth capabilities? Would AI play the role of traffic cop, analyst, auditor, advisor? And what of the human factor? Will AI replace security professionals or augment their efforts?

Below, I try to answer some of these questions and others with six predictions that I believe will shape regional cybersecurity in 2025.

Prediction 1: The increasing use of AI will not alter the basics of cybersecurity strategies

While several regional enterprises are looking for the next best AI solution in an effort to fight fire with fire, I am reminded of the famous Alphonse Karr quote, "The more things change, the more they stay the same." As such, a better question is, "What do businesses stand to lose (i.e. what is the value at risk) from AI abuse and misuse?" And what portion of this risk can be addressed with current security capabilities? For example, is securing an AI agent from threats like spoofing, tampering, information disclosure, denial of service, or escalation of privileges actually novel? Does it require new investments to build up a dedicated "AI" security stack? Similarly, consider that AI models consist of open-source and first-party code deployed on premises, in the cloud, or both. Infrastructure, software-pipeline, and supply-chain security practices still apply. So again, the question is, do we really need a complete security rethink?

My recommendation is that security teams proactively address these evolving threats by developing robust threat models and establishing guardrails — essentially, "secure by default" solutions. Ultimately, the key challenge lies in balancing the desire for rapid digital transformation with the imperative of safeguarding enterprise assets against potential AI-related abuses.

Prediction 2: The 'human factor' will be key to guarding against the increase in hackers leveraging AI for offensive attacks

AI will enable bad actors to do what they have always done, but faster. Just like defenders, they will use AI to automate software development and expedite the analysis of reams of data to discover plausible vulnerabilities and select and execute exploits.

One critical area for improvement lies in addressing human vulnerabilities, often referred to as "layer 8" in cybersecurity. Since humans are easily spoofed, it's essential to implement stronger forms of multi-factor authentication and privileged access management. These measures can help mitigate risks associated with social engineering and wire fraud, which are likely to increase as attackers utilize AI for more sophisticated tactics.

Prediction 3: In the next five years, AI-driven cybersecurity will enhance operational efficiency for defenders, but the human element will remain crucial in interpreting data and making decisions

Over the next five years, we can expect significant improvements in operational and capital efficiency for defenders, as AI continues to automate routine tasks and streamline processes. This will free security practitioners to focus on more complex challenges, particularly those involving "irreducible uncertainty" — situations where the risk cannot be fully understood through empirical data.

As the deterministic aspects of cybersecurity are automated, the role of experts will increasingly shift toward decision-making in uncertain scenarios. AI will aid in modeling these risks, but the effectiveness of these models will heavily depend on the expertise and assumptions of the security professionals using them. This means that while AI will enhance analytical capabilities, the human element will remain critical in interpreting data and making informed choices among plausible alternatives. Security professionals will continue to play a vital role in navigating complexities and uncertainties, underscoring the importance of their expertise in the evolving landscape of AI-driven cybersecurity.

Prediction 4: Automation and orchestration will grow in importance in 2025 to centralize risk telemetry across cloud, endpoints, and IoT devices

Landing all your risk telemetry into one place will become common. Many organizations are already aggregating IT, OT and cloud-native risk data into security data lakes, including asset state and changes over time, along with threat and vulnerability intelligence. Note that telemetry consumption is not the same as risk measurement. At a minimum, assets must be normalized, and scores must be rationalized. From there, automation will enable organizations to measure operational efficiency in controlling attack surfaces and implement "policy-as-code" using AI copilots. AI-driven tools will drive down risk in both a capital and operationally efficient manner.

Prediction 5: Cyber risk quantification (CRQ) will be a core organizational practice for most CISOs in the next five years

Measuring risk is a core capability, not a product. As cybersecurity maturity grows, the integration of financial metrics with technical security data will become critical. The industry calls this "cyber-risk quantification" (CRQ), but I call it cybersecurity risk management. You can't extract quantitative measurement from the broader domain of cybersecurity risk management — they are one and the same. The good news is that the majority of CISOs will have CRQ capabilities in 2025 — in part or wholly integrated into their cybersecurity risk management programs.

Prediction 6: The relationship between CISOs, the C-suite, and boards will evolve toward more strategic collaboration, driven by a focus on economic and operational efficiency

The CISO that focuses on economic and operational efficiency will be fast friends with business focused leaders. The modern CISO will see risk management as minimizing business impact without breaking the bank. It's that simple in theory. In practice, the CISO must do this in a structured manner that is explainable to business stakeholders and executable by operators, which goes back to measurement as a career skill and core security capability. Clear, measurable communication will be essential, allowing CISOs to translate complex security strategies into actionable insights for business leaders. In short, our relationship with business folks who are focused on winning will be improved to the extent we adopt the right concepts, objects and methods of measurement. This approach will foster stronger partnerships with the C-suite, enhancing decision-making and driving business outcomes, while managing cyber risk effectively.

Resolution revolution

The transition to a new year is often punctuated by resolutions, which are invariably commitments to "do better". CISOs' resolutions for 2025 will involve cultural shifts in risk management and collaboration between security and other functions, from IT to the C-suite. To "do better", security leaders must focus on business-oriented measures backed by data, and holistic solutions that help target resources where they can make the greatest impact.

EXPLORING AND MITIGATING AI-DRIVEN CYBERCRIME

DEREK MANKY, CHIEF SECURITY STRATEGIST & GLOBAL VP THREAT INTELLIGENCE | BOARD ADVISOR, THREAT ALLIANCES AT FORTIGUARD LABS

From the boardroom to your go-to news podcast, conversations about the availability of and use cases for AI are everywhere. It's no surprise why AI innovations and their surrounding excitement are ubiquitous: AI has undoubtedly improved society in many ways, ranging from increasing business efficiencies to generating better outcomes in sectors like healthcare and education.

Cybersecurity practitioners benefit from AI, using this technology to enhance threat detection and response times by automating anomaly and vulnerability detection. Teams also use AI-driven cybersecurity tools to predict and prevent attacks by analyzing patterns and adopting evolving threats.

Conversely, the growing cybercrime market is thriving on cheap and accessible wins. As AI evolves, it's already lowering the barrier to entry for aspiring cybercriminals, increasing access to the tactics and intelligence needed to execute successful attacks regardless of an adversary's knowledge. In addition to enhancing accessibility, AI enables malicious actors to create more believable phishing threats, complete with context-aware and regionalized language.

The AI-Enabled Cybercrime Project

While defenders navigate a changing threat landscape in which attackers continually identify new ways to harness AI for their benefit, collaborating across public sectors, industries, and borders is crucial to developing new strategies and practices to combat AI-driven cybercrime. Fortinet is proud to work with the UC Berkeley Center for Long-Term Cybersecurity (CLTC), the Berkeley Risk and Security Lab (BRSL), and other public and private sector organizations on a new effort: AI-Enabled Cybercrime: Exploring Risks, Building Awareness, and Guiding Policy Responses. CLTC was established in 2015 as a research and collaboration hub at the University of California, Berkeley, and serves as a convening platform and bridge between academic research and the needs of decision-makers in government, industry, and civil society relating to the future of security. BRSL at UC Berkeley's Goldman School of Public Policy is an academic research institute focused on the intersection of technology and security. The lab conducts analytical research and designs and fields wargames.

This latest effort, AI-Enabled Cybercrime, is a structured set of tabletop exercises (TTXs), surveys, workshops, and interviews that will take place over the next nine months, engaging subject matter experts worldwide and sharing findings in a public-facing report and follow-on presentations. The project will simulate real-world scenarios to uncover the dynamics of AI-powered cybercrime and develop forward-looking defense strategies. This effort will help decision-makers in policy and industry navigate the changing nature of cybersecurity, support the development of proactive AI-enabled cybercrime prevention strategies, and inform public policy decisions.

The initiative begins December 17 with a scenario-based TTX conducted at UC Berkeley. Cybersecurity professionals, academic experts, local government officials, and law enforcement representatives will explore generative AI tools like those used to create believable phishing scams and how they catalyze cybercrime.

Follow-up workshops are planned in Singapore and Israel in the first half of next year. The cumulative findings from these workshops will be shared in a public report scheduled for release in the summer of 2025.

Partnering with UC Berkeley to Strengthen Our Collective Defenses

In addition to the AI-Enabled Cybercrime initiative, Fortinet has worked with UC Berkeley's CLTC on other projects to help entities worldwide prepare for future cybersecurity challenges. Last year, Fortinet collaborated with the CLTC and other organizations on its Cybersecurity Futures 2030 effort to help leaders across the public and private sectors examine future-focused scenarios and consider how digital security will change in the coming years.

The Cybersecurity Futures 2030 inaugural report, Cybersecurity Futures 2030: New Foundations, which was published last December, includes insights from six global workshops with insights on how technological, political, economic, and environmental changes will impact the future of cybersecurity for governments and organizations and how leaders should start to prepare. Fortinet participated in the Washington, D.C. working session, taking part in a hands-on workshop that included analysis across different geographies and scenario planning for 2030.

Collaboration Is Table Stakes for Disrupting Global Cybercrime

As our adversaries take advantage of new technologies and we assess and adjust our strategies, it's clear that partnerships strengthen our collective ability to navigate the evolving threat landscape proactively. Ongoing cooperation across industries and borders is a vital component of successfully dismantling sophisticated cybercrime operations, and there are many powerful examples of existing collaborations that are already combatting cybercrime in a meaningful way.

Dismantling cybercrime operations and adversaries' attack infrastructure is everyone's responsibility; no organization can achieve this alone. By working together and regularly sharing intelligence and response strategies, we can force cybercriminals to start over, rebuild, and shift their tactics, disrupting their activities and making our digital world safer.

BY **FADY YOUNES**, MANAGING DIRECTOR FOR CYBERSECURITY AT CISCO MIDDLE EAST, AFRICA, TÜRKIYE, ROMANIA AND CIS

35 YEARS OF RANSOMWARE: EVOLUTION AND LESSONS

December 2024 marks the 35th anniversary of ransomware and 20 years since modern criminal ransomware first emerged. Over these decades, ransomware has transformed from basic attacks to complex global crimes. This moment invites a reflection on its history and future implications.

Ransomware began in December 1989 with the AIDS Trojan, which encrypted file names and demanded payment via floppy disks. Its impact was limited due to technological constraints. By 1996, researchers predicted "cryptoviruses" that would use encryption for extortion, highlighting the importance of robust antivirus protection and regular data backups.

Rise of Criminal Ransomware

The first major ransomware attack, GPCode, appeared in 2004, targeting Russian users through malicious email attachments. Initially using weak encryption, attackers soon adopted secure public-key encryption, complicating decryption. Collecting payments was a challenge, as methods like bank transfers risked revealing attacker identities.

The advent of virtual currencies addressed this issue, enabling anonymous transactions. Cryptocurrencies like Bitcoin allowed attackers to securely and anonymously collect payments. CryptoLocker, launched in 2013, was one of the first campaigns to successfully utilize Bitcoin, setting the stage for future operations.

Professionalization of Ransomware

With secure payment methods established, ransomware operations became professionalized. An ecosystem emerged, dividing tasks between developers, who created sophisticated malware, and affiliates, who distributed it via spam campaigns, botnets, or social engineering. This collaboration facilitated large-scale, efficient attacks.

In 2016, ransomware operators shifted their focus from individuals to institutions. The SamSam ransomware exemplified this by attacking organizational networks and demanding hefty ransoms. This strategy proved particularly lucrative in sectors like healthcare, where downtime could threaten lives, encouraging swift payments.

Current Threat Landscape

High-profile incidents, such as WannaCry in 2017, showcased ransomware's destructive potential. WannaCry affected systems by encrypting files but was ineffective as a profit-making tool due to its inability to track payments. Similarly, 2017's NotPetya, designed to wipe data, acted as destructive malware rather than true ransomware.

November 2019 saw the introduction of double extortion with Maze ransomware, which involved stealing data before encryption. This tactic pressured organizations to both decrypt files and prevent data leaks, adding reputational and regulatory risks to the victim's burden.

Human and Operational Impact

Ransomware's impact extends beyond financial losses, disrupting essential services and causing operational chaos. IT teams work under intense pressure to restore systems, risking burnout. For businesses, reputational damage and compliance penalties add to the long-term costs. These consequences highlight ransomware's far-reaching effects.

Lessons Learned and Future Preparations

The IT landscape has changed significantly since ransomware's inception. Enhanced software engineering and faster patching cycles have reduced vulnerabilities. However, human error remains a major entry point, with password breaches and phishing used as prevalent attack vectors.

Despite challenges, there is optimism. Law enforcement has arrested major ransomware operators and dismantled their infrastructure. Advances in antivirus and endpoint protection have improved detection and response capabilities. In addition, modern systems can flag suspicious activities, like unauthorized encryption attempts.

The most effective defense remains robust offline backups, allowing data restoration without ransom payments. However, the ongoing threat of ransomware underlines the failure to widely adopt effective backup strategies.

Looking Ahead

As cyber threats continue to escalate globally – specially with the AI revolution, the UAE faces unique challenges that necessitate robust defense mechanisms. The nation's rapid technological advancements render it a prime target for cyberattacks.

The Cisco Cybersecurity Readiness Index for 2024 reveals that 65% of UAE organizations experienced a cybersecurity incident in the past year, while 85% believe that a security incident is likely to disrupt their business in the next 12 to 24 months.

Encouragingly, the findings indicate a significant increase in cybersecurity investment plans among UAE organizations. An impressive 99% of respondents are planning to boost their cybersecurity budgets in the upcoming year, and 68% intend to significantly upgrade their IT infrastructure to address security challenges within the next 12 to 24 months, according to the same Cisco Cybersecurity Readiness Index for 2024.

The UAE has gained global recognition for its proactive stance against cybercrimes and attacks. According to the Global Security Index 2024, released in September 2024, the nation ranks among the highest-tier countries. The UAE demonstrates a firm commitment to cybersecurity through its National Cybersecurity Strategy, the UAE Cybersecurity Council, and partnerships with global law enforcement entities, all aimed at safeguarding critical infrastructure against cybercrime.

In an advanced digital economy like that of the UAE, proactive measures—such as employee education, advanced endpoint protection, and offline backups—are essential for effective mitigation of cyber threats.

MIDDLE EAST FIRMS BOOST CYBERSECURITY BY EQUIPPING EMPLOYEES WITH ESSENTIAL TRAINING

AMID GROWING CYBER THREATS, ACRONIS MSP ACADEMY UNVEILS KEY COMPETITIVE ADVANTAGE FOR BUSINESSES PRIORITIZING EMPLOYEE TRAINING

Acronis, a global leader in cybersecurity and data protection, has reported that partners who completed training and certification under the Acronis Academy program experienced higher revenue growth from product sales and fewer IT support requests from customers than non-certified partners. These findings are based on certification training data and sales metrics achieved by its partners.

Acronis launched the MSP Academy in 2023 to offer specialized MSP training, supporting the growing base of managed service providers. Data from their certification training revealed that partners who completed certification training saw an average 60% increase in revenue and a 40% reduction in incident resolution reports.

"The Acronis MSP Academy modules cover essential areas including managed services, cybersecurity, and marketing, all of which are particularly relevant to the growing demands in the Middle East," says Ziad Nasr, General Manager of Acronis Middle East.

"By completing these courses, MSPs in the region can enhance their expertise in cybersecurity, deliver exceptional services to clients, and strengthen their reputation in a rapidly evolving market," added Nasr.

Over 155,000 vulnerable assets have been identified within the UAE, according to recent reports from the UAE Cybersecurity Council. This alarming figure reflects the growing cybersecurity risks in the Middle East, driven by geopolitical factors, increased migration, and the region's expanding digital presence. In addition to these vulnerabilities, advanced threats like ransomware are rising. In 2024, Saudi Arabia reported 11 ransomware incidents

in 2024, up from 10 in 2023, Lebanon saw an increase from 2 to 7 cases, and Oman reported 4. These incidents highlight the urgent need for comprehensive cybersecurity education.

Human error is a major contributor to cyberattacks, yet a recent PwC survey reveals that only 37% of organizations in the Middle East have implemented strong training and awareness programs for their employees.

In 2025, emerging cyber threats like deepfake technology and AI-generated phishing emails are expected to evolve, with attackers increasingly exploiting vulnerabilities as businesses and government agencies rely more on digital communication. Cybercriminals may impersonate executives or government officials using deepfake audio or video, making these attacks difficult to detect. These advanced threats are often beyond public awareness and can only be effectively identified if proper training and awareness programs are in place to help individuals recognize and defend against them.

COURSERA 2025 JOB SKILLS REPORT: GENAI AND BUSINESS SKILLS DRIVE UAE WORKFORCE COMPETITIVENESS

KAIS ZRIBI, COURSERA'S GENERAL MANAGER FOR THE MIDDLE EAST AND AFRICA,

Coursera, a leading global online learning platform, has released its 2025 Job Skills Report, highlighting how the rapid adoption of generative AI (GenAI) is reshaping industries and redefining in-demand skills. The report reveals that UAE learners are prioritizing GenAI and business skills to stay competitive and adapt to the region's evolving labor market.

GenAI is the fastest-growing skill

Drawing on insights from five million enterprise learners and over 7,000 institutional customers, the report identifies GenAI as the fastest-growing skill globally, with course enrollments increasing by 866% year-over-year. In the UAE, this trend is evident, with GenAI skills leading the list for learners and reflecting the country's ambition to become a global AI leader. This is further

Generative AI skills surged by 866% year-over-year on the platform

AI skills doubled in enrollments year-over-year

Demand for **risk management** and **cybersecurity skills** is skyrocketing

Data ethics is among the fastest-growing skills on Coursera for employees, driven by the need to responsibly manage and analyze customer data

Project management skills saw a sharp rise in demand, jumping 70 spots on the fastest-growing skills list

coursera

underscored by the UAE's ranking among the top five countries in Stanford HAI's Global AI Vibrancy Tool.

AI and advanced technologies are projected to contribute nearly 14% of the UAE's GDP by 2030. The country's early investments in AI have laid a strong foundation for growth, though challenges remain. A recent SAP YouGov survey revealed that 43% of UAE IT decision-makers cite a lack of skilled employees as a key obstacle to AI implementation. This presents a significant opportunity, with 84% of UAE companies planning to hire specialized AI talent within the next 15 months.

Globally, AI is expected to add US$15.7 trillion to the economy by 2030, while 70% of graduates advocate for GenAI training. Higher education institutions have a unique opportunity to expand AI-focused programs. Popular courses like computer vision, PyTorch, and machine learning have seen enrollments double year-over-year. However, gender disparities persist; women accounted for only 28% of AI course enrollments in 2024, emphasizing the need for inclusive education and workplace policies to ensure diversity in technology.

UAE learners excel in business skills

Coursera's 2025 Job Skills Report also identifies business skills as a key area of focus for UAE learners. Skills such as compliance reporting, auditing, workforce development, human capital management, and forecasting rank among the top priorities. These capabilities reflect the UAE's standing as a regional and global business hub, where organizations increasingly rely on data-driven insights and effective management practices to maintain their competitive edge.

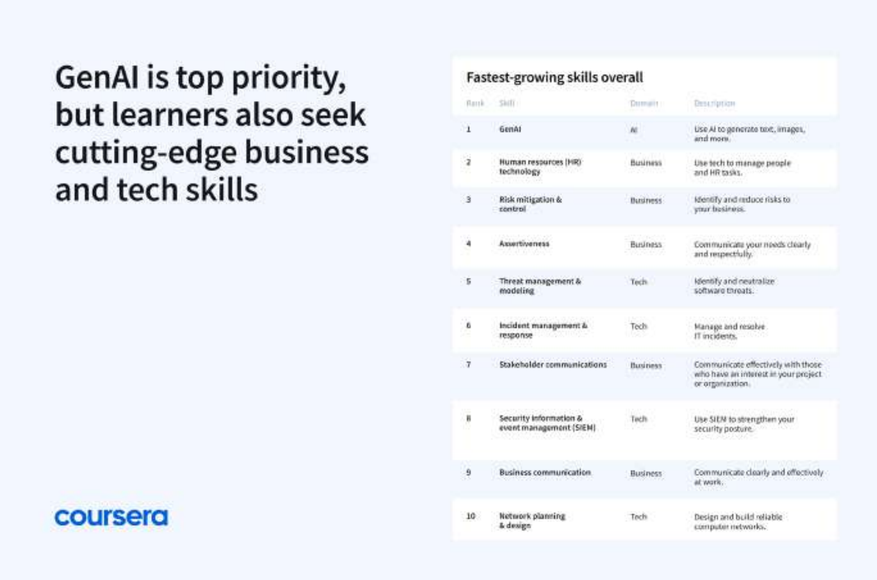
The UAE's emphasis on business acumen is closely tied to its ambitious economic goals, including its push to attract multinational corporations and foster entrepreneurship. By mastering these high-demand skills, UAE learners are equipping themselves to support the country's long-term economic growth and resilience.

Kais Zribi, Coursera's General Manager for the Middle East and Africa, said: "The UAE's visionary digital transformation and leadership in AI require a workforce adept in both technical and business skills. By focusing on GenAI and essential business competencies, UAE learners are positioning themselves to drive innovation and competitiveness in a rapidly evolving market. Coursera remains committed to supporting the UAE's workforce with the tools and resources needed to achieve these ambitious goals."

Cybersecurity: a global priority

Globally, cybersecurity and risk management skills rank among the top fastest-growing tech skills, as businesses respond to a 75% increase in cyberattacks in Q3 2024. While cybersecurity is not the top focus for UAE learners, the country has made notable strides in this domain. Public sector entities in the UAE face and thwart an average of 50,000 cybersecurity attacks daily, with the UAE Cybersecurity Council preventing 71 million attacks.

To enhance digital resilience, the UAE has introduced policies focused on cloud computing, data security, IoT security, and cybersecurity operations. Supported by a growing cybersecurity market valued at US$1.5 billion in 2023 and projected to grow by 12.7% through 2028, these efforts underscore the need for ongoing workforce development in cybersecurity to address evolving challenges.



GenAI is top priority, but learners also seek cutting-edge business and tech skills

Fastest-growing skills overall

Rank	Skill	Domain	Description
1	GenAI	AI	Use AI to generate text, images, and more.
2	Human resources (HR) technology	Business	Use tech to manage people and HR tasks.
3	Risk mitigation & control	Business	Identify and reduce risks to your business.
4	Assertiveness	Business	Communicate your needs clearly and respectfully.
5	Threat management & modeling	Tech	Identify and neutralize software threats.
6	Incident management & response	Tech	Manage and resolve IT incidents.
7	Stakeholder communications	Business	Communicate effectively with those who have an interest in your project or organization.
8	Security information & event management (SIEM)	Tech	Use SIEM to strengthen your security posture.
9	Business communication	Business	Communicate clearly and effectively at work.
10	Network planning & design	Tech	Design and build reliable computer networks.

coursera

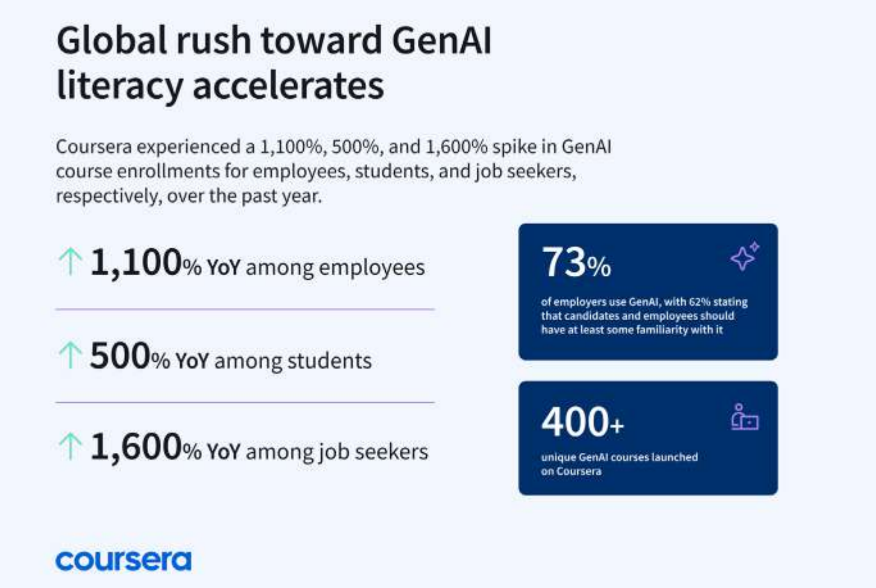
Bridging gaps in data ethics

Data ethics is among the fastest-growing skills on Coursera, driven by the need for employees to responsibly manage and analyze customer data. Despite its importance, there is a notable gap in interest among students and job seekers. This presents a key opportunity for higher education institutions to enhance curricula, as 60% of data leaders identify data governance as a critical concern. A Deloitte survey found that 78% of organizations prioritize "safe and secure" AI use as a top ethical principle.

The UAE has been proactive in addressing these challenges through initiatives like the Ethical Charter for Development and Use of AI, launched as part of the UAE's AI Strategy 2031. Learners who upskill in data ethics and governance will position themselves competitively for future roles in this critical field.

The Value of human skills

The report also emphasizes the importance of human skills in the workplace. Assertiveness and Communication ranked among the top 10 skills in 2024. However, while 84% of managers expect new hires to communicate effectively and contribute to meetings, 71% of Gen Z workers report challenges in doing so. Interestingly, younger students are prioritizing green skills, with sustainability-focused areas like waste management and business continuity appearing in the top 10 skills for students. While ESG-related skills are increasingly important, the report suggests that Gen Z workers should also focus on core human skills to better meet employer expectations and thrive in team-oriented environments.



Global rush toward GenAI literacy accelerates

Coursera experienced a 1,100%, 500%, and 1,600% spike in GenAI course enrollments for employees, students, and job seekers, respectively, over the past year.

↑ 1,100% YoY among employees

↑ 500% YoY among students

↑ 1,600% YoY among job seekers

73% of employers use GenAI, with 62% stating that candidates should have at least some familiarity with it

400+ unique GenAI courses launched on Coursera

coursera

Upskilling the workforce

With 9.4 million Coursera learners in the Middle East and North Africa, Arabic has emerged as the top language job seekers are learning in, after English. To meet this growing demand, Coursera has leveraged AI and machine learning to translate over 4,900 courses into 23 languages, including Arabic, enabling learners to enhance their skills, improve employability, and advance their careers.

As the UAE accelerates its AI adoption, developing a workforce equipped with both technical and human skills is essential to maintaining its status as a regional and global innovation hub. By championing education and embracing innovation, the UAE not only prepares its workforce for the future but also reinforces its role as a global leader in technology and business excellence.

10 CYBERSECURITY TRENDS THAT THE CRITICAL INFRASTRUCTURE SECTOR SHOULD KEEP AN EYE ON IN 2025

SERTAN SELCUK,
VP FOR METAP & CIS,
OPSWAT

As we head into 2025, the United Arab Emirates (UAE) looks forward to yet another year of innovation that takes us yet another step closer to the fulfillment of Vision 2030. As business leaders flesh out strategies for investment, operations, and recruitment, they will try to anticipate the unexpected. In 2024, the UAE Cyber Security Council identified 155,000 vulnerable assets, with two in five critical vulnerabilities remaining unaddressed for over five years. Let 2025 be the year we fight to secure our economic future. Below are 10 predictions about cybersecurity for the coming year that should help focus the defenders' actions.

1. Fighting AI fire with AI fire

Cheaper AI has lowered entry hurdles for threat actors. In some cases, this has been done by plugging technical knowledge gaps for attackers; in others, AI has provided more grammatically and aesthetically convincing phishing messages, increasing the likelihood of success in credentials theft. The same tools can be leveraged by potential targets to bolster their cyber defenses, but so far, we see UAE organizations often lagging behind their adversaries' adoption. In 2025, we believe this trend will begin to reverse itself, with business and technology leaders collaborating on ways to focus cyber investments where they will have the greatest impact.

2. A return to basics
Both because of increases in the sophistication and volume of attacks and because of the lack of skills and resources in the cybersecurity function (significant budget will now be swallowed by AI), UAE businesses will focus more on the basics in 2025. They will prioritize critical sites and assets, prioritizing segmentation to segregate their crown jewels. With the right strategy, the enterprise can secure the environment while preserving its ability to glean actionable business insights. To accomplish this, it will rely on one-way data transfers using data diodes, backed by traditional scanning policies for inbound removable media and mobile devices.

3. Constant vigilance
As the cost of machine learning continues to fall and phishing campaigns become more convincing, UAE enterprises should brace for an increase in attacks on employees' devices. Where its people have long been an organization's greatest cyber-vulnerability, they remain its greatest potential weapon. This year, we will see a greater focus on awareness training and novel detection controls to protect against AI-powered social engineering.

4. Securing the supply chain
The targeting of the latticework of vendors, suppliers, distributors, and other partners that make up the modern business environment will continue in 2025. As OT becomes ever more vulnerable because of its merger with IT, the energy, utilities, and manufacturing sectors will become points of concern. Threat actors will target suppliers or subcontractors to compromise critical infrastructure. Since these attacks represent existential threats to the economy at large and to public health and safety, we expect to see an escalation in investment in their protection in 2025.

5. Accountability to regulators
At a GITEX Global 2024 panel, it was pointed out that amid the explosion in advanced technologies like AI, attackers still commonly exploit basic vulnerabilities with basic infiltration methods. Outdated software is a persistent vulnerability for organizations, and this could be the year when UAE businesses recognize the risks, not only to operations but to their legal standing with regulators. Unfortunately, investments in awareness training have not been enough to prevent people from falling for social engineering. To address their compliance shortfalls, businesses must intensify their training efforts, tailoring each lesson to the learner, and making sure it is immersive enough to ensure retention.

6. The cloud crisis
When OT-heavy organizations adopt cloud technologies for flexibility and scalability, they expand their attack surfaces. This transition calls for strong network perimeter security protocols. Cloud-connected devices must communicate with host services through data diodes for secure, one-way data transfer. Where remote access to OT environments is necessary, other secure pathways should be used that are tailored to specific OT tasks and use the least-privilege principle. In 2025, we expect to see increased adoption of such cloud-aware solutions.

7. Ransomware, of course
According to the UAE Cyber Security Council, half of all cyberattacks in the country are ransomware attacks. It is expected to continue this year, signifying the need for preventative measures such as staff awareness and N-tier backup facilities.

8. A return to premises
As we already mentioned, the cloud is vulnerable. Consequently, businesses worldwide are moving their data from cloud storage solutions to on-premises setups. Inspired by high-profile incidents such as the 2023 MOVEit attacks, we expect this migration to continue through the coming year as UAE organizations dial back their reliance on third parties.

9. Securing Web apps
The rise of the multi-cloud environment has brought with it new vulnerabilities. In 2025, organizations will look to multi-layered defenses recommended by the Open Worldwide Application Security Project (OWASP) to secure Web apps. Many organizations have relegated security to an afterthought when adopting AI tools. This may be because best practice standards have yet to emerge on the tools or practices that most effectively protect enterprises as they use AI. This leads to vulnerabilities being overlooked, including those in Web apps.

10. Consolidation of vendors
The art of cybersecurity continues to be non-holistic among regional businesses. Companies work with point solutions, each geared towards a specific area, such as endpoints or networks. This leads to data silos and an open field for attackers who understand how to decipher their attacks so no one tool can detect a breach. As such, the visibility of the security team is compromised. In 2025, we expect to see UAE enterprises prioritize vendor consolidation, not only to cut costs but to give the SOC a single pane view of the attack surface.

Rays of hope
Yes, attackers are becoming more sophisticated. Yes, they use AI. And yes, we can expect the volume of campaigns to increase. The UAE enterprises do not face this fight unarmed. By returning to the drawing board on protections and training, and by turning to pragmatism on budgets and resourcing, UAE business leaders can prepare for the 2025 cyber battlefield without breaking the bank.

2025 PREDICTIONS: WEBASSEMBLY, AGENTIC AI, DATA CLASSIFICATION, AI GATEWAYS AND SMALL LANGUAGE MODELS

More than ever, enterprises are grappling with a hybrid IT estate spread across public cloud, on-premises, and edge computing. This poses significant challenges in terms of standardizing security, delivery, and operations across disparate environments.

Against this ever-changing backdrop, what are they key trends to look out for in 2025? We assembled an elite team of F5 experts to learn more.

2025 Technology #1: WebAssembly

Oscar Spencer, Principal Engineer, F5

WebAssembly (Wasm) offers a path to portability across the hybrid multicloud estate, delivering the ability to deploy and run applications anywhere a Wasm runtime can operate.

But Wasm is more than just a manifestation of the promise for cross-portability of code. It offers performance and security-related benefits while opening new possibilities for enriching the functionality of browser-based applications.

In 2025, WebAssembly in the browser isn't expected to undergo drastic changes. The main developments are happening outside of the browser with the release of WASI (WebAssembly System Interface) Preview 3. This update introduces async and streams, solving a major issue with streaming data in various contexts, such as proxies. WASI Preview 3 provides efficient methods for handling data movement in and out of Wasm modules and enables fine-tuned control over data handling.

Additionally, the introduction of async will enhance composability between languages, allowing for seamless interactions between async and sync code, especially beneficial for Wasm-native languages. As WASI standards stabilize, we can expect a significant increase in Wasm adoption, providing developers with robust tooling and a reliable platform for building on these advancements.

Assuming Wasm can solve some of the issues inherent in previous technologies, it would shift the portability problems 95% of organizations struggle with today to other critical layers of the IT tech stack, such as operations.

Racing to meet that challenge is generative AI and the increasingly real future that is AIOps. This fantastical view of operations—changes and policies driven by AI-based analysis informed by full-stack observability—is closer to reality everyday thanks to the incredible evolutionary speed of generative AI.

2025 Technology #2: Agentic AI

Laurent Quérel, F5 Distinguished Engineer

Autonomous coding agents are poised to revolutionize software development by automating key tasks such as code generation, testing, and optimization. These agents will significantly streamline the development process, reducing manual effort and speeding up project timelines. Meanwhile, the emergence of Large Multimodal Agents (LMAs) will extend AI capabilities beyond text-based search to more complex interactions.

As AI agents reshape the internet, we will see the development of agent-specific browsing infrastructure, designed to facilitate secure and efficient interactions with websites. This could disrupt industries like e-commerce by automating complex web tasks, leading to more personalized and interactive online experiences.

However, as these agents become more integrated into daily life, new security protocols and regulations will be essential to manage concerns related to AI authentication, data privacy, and potential misuse.

By 2028, it is expected that a significant portion of enterprise software will incorporate AI agents, transforming work processes and enabling real-time decision-making through faster token generation in iterative workflows. This evolution will also lead to the creation of new tools and platforms for agent-driven web development.

The truth is that to fully exploit the advantages of AI, you need data—and a lot of it. That's a significant challenge given that nearly half (47%) of organizations admit to having no data strategy for AI in place. The amount of data held by an organization—structured, unstructured, and real-time metrics—is mind-boggling. Simply cataloging that data requires a significant investment.

2025 Technology #3: Data classification

James Hendergart, Sr. Dir. Technology Research, F5

Roughly 80% of enterprise data is unstructured. Looking ahead, generative AI models will become the preferred method for detecting and classifying unstructured enterprise data, offering accuracy rates above 95%. These models will become more efficient over time, requiring less computational power and enabling faster inference times. Solutions like Data Security Posture Management (DSPM), Data Loss Prevention (DLP), and Data Access Governance will increasingly rely on sensitive data detection and classification as a foundation for delivering a range of security services. As network and data delivery services converge, platform consolidation will drive vendors to enhance their offerings, aiming to capture market share by providing comprehensive, cost-effective, and easy-to-use platforms that meet evolving enterprise needs.

The shared desire across organizations to harness generative AI for everything from productivity to workflow automation to content creation is leading to the introduction of a new application architectural pattern as organizations begin to deploy AI capabilities. This pattern expands the traditional three tiers of focus—client, server, and data—to incorporate a new AI tier, where inferencing is deployed.

2025 Technology #4: AI gateways

Ken Arora, F5 Distinguished Engineer

AI gateways are emerging as the natural evolution of API gateways, specifically tailored to address the needs of AI applications. Similar to how Cloud Access Security Brokers (CASBs) specialize in securing enterprise SaaS apps, AI gateways will focus on unique challenges like hallucinations, bias, and jailbreaking, which often result in undesired data disclosures. As AI applications gain more autonomy, gateways will also need to provide robust visibility, governance, and supply chain security, ensuring the integrity of the training datasets and third-party models, which are now potential attack vectors.

Additionally, as AI apps grow, issues like distributed denial-of-service (DDoS) attacks and cost management become critical, given the high operational expense of AI applications compared to traditional ones. Moreover, increased data sharing with AI apps for tasks like summarization and pattern analysis will require more sophisticated data leakage protection.

In the future, AI gateways will need to support both reverse and forward proxies, with forward proxies playing a critical role in the short term as AI consumption outpaces AI production. Middle proxies will also be essential in managing interactions between components within AI applications, such as between vector databases and large language models (LLMs).

The changing nature of threats will also require a shift in how we approach security. With many clients becoming automated agents acting on behalf of humans, the current bot protection models will evolve to discriminate between legitimate and malicious bots. AI gateways will need to incorporate advanced policies like delegated authentication, behavioral analysis, and least privilege enforcement, borrowing from zero trust principles. This will include risk-aware policies and enhanced visibility, ensuring that AI-driven security breaches are contained effectively while maintaining robust governance.

Most pressing are the ability to not only address traditional security concerns around data (exfiltration, leakage) but ethical issues with hallucinations and bias. No one is surprised to see the latter ranked as significant risks in nearly every survey on the subject.

2025 Technology #5: Small Language Models

Lori MacVittie, F5 Distinguished Engineer

Given the issues with hallucinations and bias, it would be unthinkable to ignore the growing use of retrieval-augmented generation (RAG) and Small Language Models (SLMs). RAG has rapidly become a foundational architecture pattern for generative AI..

Organizations not already integrating retrieval augmented generation (RAG) into their AI strategies are missing out on significant improvements in data accuracy and relevancy, especially for tasks requiring real-time information retrieval and contextual responses. But as the use cases for generative AI broaden, organizations are discovering that RAG alone cannot solve some problems.

The growing limitations of LLMs, particularly their lack of precision when dealing with domain-specific or organization-specific knowledge, are accelerating the adoption of small language models. While LLMs are incredibly powerful in general knowledge applications, they often falter when tasked with delivering accurate, nuanced information in specialized fields. This gap is where SLMs shine, as they are tailored to specific knowledge areas, enabling them to deliver more reliable and focused outputs. Additionally, SLMs require significantly fewer resources in terms of power and computing cycles, making them a more cost-effective solution for businesses that do not need the vast capabilities of an LLM for every use case.

SLMs currently tend to be industry-specific , often trained on sectors such as healthcare or law. Although these models are limited to narrower domains, they are much more feasible to train and deploy than LLMs, both in terms of cost and complexity. As more organizations seek solutions that better align with their specialized data needs. SLMs are expected to replace LLMs in situations where retrieval-augmented generation methods alone cannot fully mitigate hallucinations. Over time, we anticipate that SLMs will increasingly dominate use cases where high accuracy and efficiency are paramount, offering organizations a more precise and resource-efficient alternative to LLMs.

Looking ahead: beyond transformers

Kunal Anand, Chief Innovation Officer

Transformer models, while powerful, have limitations in scalability, memory usage, and performance, especially as the size of AI models increases.

As a result, a new paradigm is emerging: converging novel neural network architectures with revolutionary optimization techniques that promise to democratize AI deployment across various applications and devices.

The AI community is already witnessing early signs of post-transformer innovations in neural network design. These new architectures aim to address the fundamental limitations of current transformer models while maintaining or improving their remarkable capabilities in understanding and generating content.

Among the most promising developments is the emergence of highly optimized models, particularly 1-bit large language models. These innovations offer dramatic reductions in memory requirements and computational overhead while maintaining model performance despite reduced precision.

The impact of these developments will cascade through the AI ecosystem. Models that once demanded substantial computational resources and memory will operate efficiently with significantly lower overhead. This optimization will trigger a shift in computing architecture, with GPUs potentially becoming specialized for training and fine-tuning tasks while CPUs handle inference workloads with newfound capability.

These changes will catalyze a second wave of effects centered on democratization and sustainability. As resource requirements decrease, AI deployment will become accessible to various applications and devices. Furthermore, infrastructure costs will drop substantially, enabling edge computing capabilities that were previously impractical. Simultaneously, the reduced computational intensity will yield environmental benefits through lower energy consumption and a smaller carbon footprint, making AI operations more sustainable.

These developments will enable unprecedented capabilities in edge devices, improvements in real-time processing, and cost-effective AI integration across industries. The computing landscape will evolve toward hybrid solutions that combine different processing architectures optimized for specific workloads, creating a more efficient and versatile AI infrastructure.

TECHNOLOGY PARTNERS ANTICIPATE SIGNIFICANT REVENUE SHIFT TO AI IN THE UAE

INDUSTRY LEADERS FORESEE SUBSTANTIAL TRANSFORMATIONS DRIVEN BY INFRASTRUCTURE, CYBERSECURITY, AND CUSTOMER EXPERIENCE

Cisco, the worldwide leader in networking and security, released findings from its new Cisco Global AI Partners Study. The study, titled Bridging the Customer AI Readiness Gap – The opportunities ahead for partners, revealed that IT partners around the world are anticipating a transformative wave of AI technology demand that will drive the majority of their revenue over the next four to five years. According to the study, more than a quarter (26%) of partners surveyed in the UAE believe that as much as 76-100% of their revenue will come from AI-related technologies during this period.

The study highlights that 43% of partners in the UAE believe the demand for AI-related technology investments will grow by more than 75% in the next four to five years. The partners surveyed for the report highlighted infrastructure (26%), cybersecurity (26%), and sustainability management (11%) as the top three drivers of AI technology demand in the coming years. As AI demand surges, partners in the UAE also foresee a

significant shift in their revenue mix. In the short-term, 37% anticipate AI will contribute to 26-50% of their revenue a year from now, while in the long run that contribution is expected to become even higher.

"As AI becomes a cornerstone of business transformation in the UAE and broader region, it's essential for our partners to be equipped with the skills and tools needed to lead this shift," said Ossama Eldeeb, Regional Director for the Partner Organization in the Middle East and Africa, Cisco. "The study's findings reveal substantial opportunities for partners to drive AI adoption and support businesses in harnessing the full potential of AI. By investing in readiness and innovation, Cisco and our partners are prepared to deliver impactful solutions that align with the region's ambitions and technological advancements."

The Cisco Global AI Partners Study, a double-blind survey of over 1,500 IT partners across 29 markets, assesses partners' capabilities in the age of AI. These findings align with the Cisco AI Readiness Index, which found that companies globally lack readiness for AI adoption, revealing gaps in infrastructure, data management, governance, and talent. Built on the insights from the Index, the Cisco Global AI Partners Study reinforces the crucial role partners play in helping customers achieve AI readiness.

Partners Show Confidence and Invest in Overcoming Challenges

The findings indicate a robust confidence among partners in their knowledge and understanding of various aspects related to AI technologies. The assessment focused on several specific solutions and capabilities for AI deployment across the four pillars of infrastructure, data, governance, and talent.

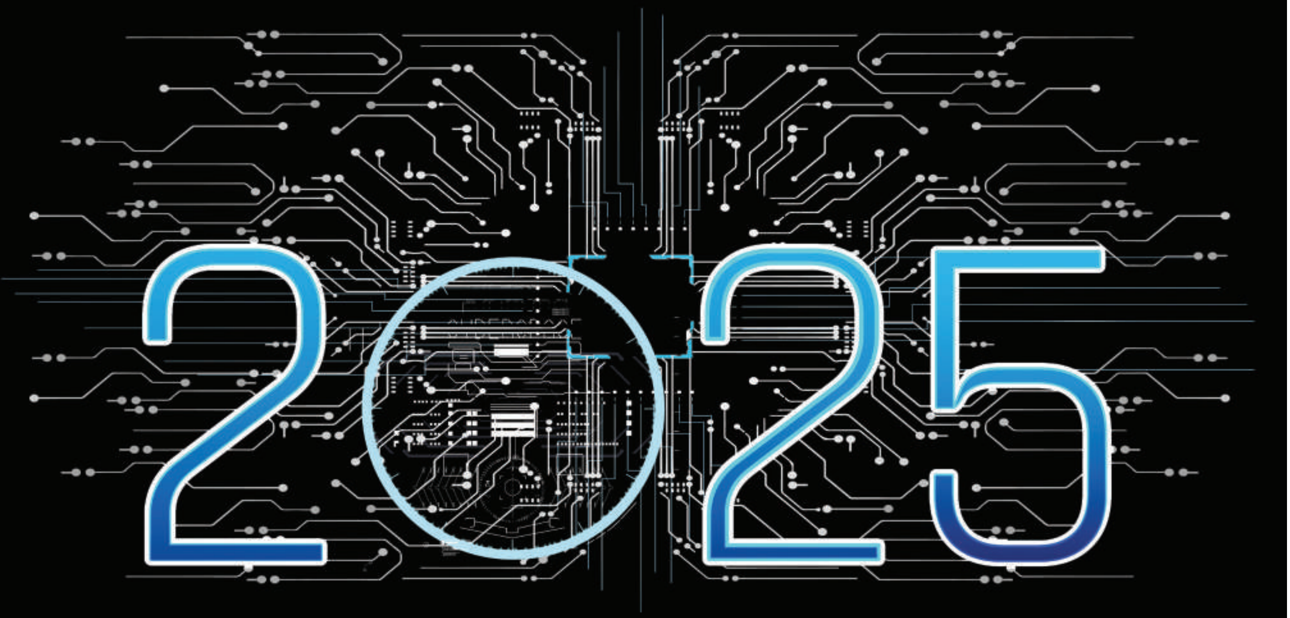
- 26% of partners in the UAE believe that 76-100% of their revenue will come from AI technologies over the next 4-5 years.
- Partners identified infrastructure, cybersecurity, and customer experience as the primary drivers of AI technology demand, presenting the greatest revenue opportunities.
- Partners show confidence about their knowledge and understanding in helping customers deploy AI solutions and are investing in upskilling.

These capabilities include:

- Building scalable and adaptable AI-ready infrastructure;
- Ensuring sufficient GPU resources for ongoing projects;
- Assessing and maintaining latency and throughput of data centers;
- Understanding data sets, data sovereignty and privacy laws across different regions/countries.

While partners show strong confidence in their knowledge and understanding of deploying AI technologies, they also understand the challenges they need to address to maximise the opportunities ahead. The biggest ones are inexperience in deploying new technologies (69%), lack of knowledge of systems and processes (51%), and a lack of available technologies (46%). To address these challenges, partners are already heavily investing in upskilling existing employees in AI-related competencies, with almost 74% conducting either internal trainings or inviting external vendors to provide specialized training.

CYBERSECURITY



NAVIGATING EMERGING THREATS AND TECHNOLOGIES

EXPLORING THE TOP THREE CYBERSECURITY TRENDS OF 2025, INDUSTRY LEADERS SHARE INSIGHTS ON AI-DRIVEN SECURITY, ZERO TRUST ARCHITECTURE, AND THE IMPERATIVE OF POST-QUANTUM CRYPTOGRAPHY.

The cybersecurity landscape is rapidly evolving, driven by technological advancements and increasingly sophisticated threats. Industry leaders outline the pivotal trends set to shape cybersecurity strategies. The trends include the rise of AI-driven security measures, widespread adoption of Zero Trust frameworks, and advancements in quantum-resistant cryptography. The article delves into how these trends are expected to fortify digital defenses and transform cybersecurity practices across industries, ensuring enhanced protection in an interconnected world.

SentinelOne

Ezzeldin Hussein, Regional Senior Director, Solution Engineering, SentinelOne

In 2025, three major cybersecurity trends will shape the industry. First, AI-driven security automation will dominate, enabling faster threat detection, response, and predictive analytics to counter evolving threats. Second, Zero Trust adoption will accelerate as organizations prioritize identity-centric architectures to protect hybrid and multi-cloud environments. Lastly, post-quantum cryptography will gain momentum as enterprises prepare to safeguard data against future quantum-driven decryption threats. These trends reflect the growing need for proactive, resilient, and future-proof security solutions to combat increasingly sophisticated attacks while ensuring compliance and operational continuity in an interconnected digital landscape.

Cloud Box Technologies

Avinash Gujje, Practice Head, Cloud Box Technologies

The cybersecurity space in 2025 will bring opportunities and challenges, with these top three trends leading the way.

Firstly, AI-driven threat detection and response will dominate, powered by sophisticated and evolving machine learning algorithms capable of identifying anomalies and predicting potential threats. As organizations increasingly adopt hybrid work environments, zero-trust architecture will see a significant rise in demand, ensuring continuous authentication of users, devices, and applications to minimize risks. Finally, escalating cybersecurity threats will push governments to enforce stricter data protection regulations, similar to GDPR, compelling companies to integrate security practices into their core business operations. Eventually, this will shape a more secure digital future.

ManageEngine

Rajesh Ganesan, President, ManageEngine

Some of the cybersecurity priorities organizations need to focus in 2025 are:

1. **Democratizing Cybersecurity**

Cybersecurity now extends beyond top management, making democratization vital to manage risks at all levels. This will support shared responsibility, proactive defense, cost savings, efficiency, and innovation. To achieve this, continuous security engagement programs and self-service tools should be looked at to enhance best practices.

2. **Distributed Governance Model for Compliance**

Adoption of a distributed governance model for compliance will help prioritize and manage rising regulatory complexities and audits. A central compliance team can help to manage oversight, while departments handle execution will be a good way to embed compliance into daily operations. This will also ensure practical, business-aligned controls.

3. **Scaling up AI in Cybersecurity**

2025 is set to be a big year for investing in AI for defense becomes crucial. Investing in augmented AI is also becoming increasingly important to significantly enhance employee productivity.

Tenable

Maher Jadallah, Vice President, Middle East & North Africa, Tenable

2024 has seen an increase in cyber threats across UAE: In the UAE we have seen an increase in both ransomware and attacks targeting critical infrastructure. Threat actors are increasingly focusing on vital sectors such as energy and water, threatening national security. We've also witnessed an increase in attacks by groups that are backed by certain governments, targeting companies and government institutions. AI techniques have also been used to improve the effectiveness of attacks, such as analyzing data and hacking systems faster.

AI adoption will increase in UAE: Many security teams still bear the scars from Bring Your Own Device (BYOD) and Shadow IT. Today, it's Shadow AI that's causing sleepless nights as organisations look to harness the possibilities AI offers. For the security team, it's a race to introduce practices and policies that negate the risk to the business, such as vulnerability detection and remediation, containing data leakage and reining in unauthorised AI use. With new AI instances daily, if not hourly, its imperative organisations can confidently expose and close AI risk, without inhibiting business operations.

To Secure Critical Infrastructure Everything is Important: We're seeing threat actors increasingly target organisations deemed as 'critical infrastructure'. In today's complex landscape, the distinction between Information Technology that runs our businesses and Operational Technology that underpins our critical infrastructure is less important than how we manage and secure these systems. Security leaders must protect and secure the entire network and critical infrastructure that encompasses an interconnected web of IT, operational technology (OT) and internet-of-things (IoT) systems.

These trends point to the need to enhance cybersecurity and invest in modern technologies. The inability to remediate everything, everywhere, all at once will make context king. Organisations that prioritise understanding the greatest risk to their business and the most critical vulnerabilities will win. This contextual approach will redefine vulnerability management as exposure management, enabling cybersecurity teams to act strategically, swiftly, and with greater precision to mitigate threats effectively.

Nozomi Networks

Anton Shipulin, Industrial Cybersecurity Evangelist, Nozomi Networks

In 2025, we can expect an increase in AI/ML-enabled cyberattacks targeting critical infrastructure and new attacks on AI/ML-based OT/IoT cyber-physical systems in smart city projects. Additionally, the cybersecurity of space infrastructure – including satellites and ground systems – and industries across sectors that rely heavily on space-based communications and services, is becoming a pressing concern as these systems are vulnerable to specific threats. Lastly, as the attack surface increases and our critical infrastructure continues to be a target for cyberattacks, we will see big cybersecurity players begin to dip their toes into the pool of OT. Whether through M&A, product development or other means of entry, the OT market is ripe for growth.

Sophos

John Shier, field CTO, Sophos

Generative AI will continue to play a dual role in cybersecurity by 2025. On one hand, it will be leveraged by cybercriminals to craft increasingly sophisticated and targeted phishing campaigns, automate malware generation, and evade traditional detection methods. On the other hand, it will be a powerful ally for cybersecurity professionals, helping to identify threats faster, improve anomaly detection, and streamline incident response. At Sophos, we are investing heavily in integrating AI-driven defenses into our products to stay ahead of this evolving threat landscape.

There are a number of emerging threats leveraging AI technology that are intensifying in the pace and sophistication of attacks. Security experts say the largest threat they see from GenAI is not a new tactic or technique, but an acceleration of existing methods used by cybercriminals and nation-state hackers.

SANS Institute

Ned Baltagi, Managing Director, Middle East, Africa, and Turkey, at SANS Institute

In 2025, three key cybersecurity trends will dominate. First, quantum-resistant cryptography will emerge as businesses prepare for quantum computing's potential to break classical encryption, driving demand for training on new cryptographic standards. Second, AI and machine learning will play dual roles in offense and defense, requiring specialized skills to interpret insights, govern ethical use, and ensure human oversight. Lastly, DevSecOps will expand as organizations integrate security into development processes, with cloud-native tools safeguarding containers and serverless architectures. Advanced identity and access management, especially aligned with zero-trust principles, will also be critical to counter insider threats and secure digital ecosystems.

AI, DATA SECURITY, AND CISO SHIFTS: TOP CYBERSECURITY TRENDS TO WATCH IN 2025

Looking ahead to 2025, the cybersecurity landscape continues to evolve at a breakneck pace as threat actors continue to perfect their craft. They are using artificial intelligence (AI) to create code and more convincing lures (especially in languages that have traditionally been a barrier for entry), automate attacks, and target people with greater precision. At the same time, they are increasingly turning their attention back to us, as individual consumers, using social media and messaging apps as a testing ground before moving to larger organizations.

But it's not just the attack vectors that are evolving. Organizations are also faced with navigating the complexities of digital identity management, multicloud environments and new data strategies. As data becomes more decentralized, and with new regulations pushing for tighter control over digital identities and sensitive information, ensuring the right tools are in place to secure data across a sprawl of applications and environments is quickly becoming a priority for security teams.

So, what might lie ahead in 2025?

Our experts peer into their crystal balls to offer their top cybersecurity predictions for the year ahead, shedding light on the trends and technologies that will define the next wave of security challenges and solutions.

Threat Actors Will Exploit AI by Manipulating Private Data

We are witnessing a fascinating convergence in the AI realm, as models become increasingly capable and semi-autonomous AI agents integrate into automated workflows. This evolution opens intriguing possibilities for threat actors to serve their own interests, specifically in terms of how they might manipulate private data used by LLMs (Large Language Models). As AI agents depend increasingly on private data in emails, SaaS document repositories, and similar sources for context, securing these threat vectors will become even more critical.

In 2025, we will start to see initial attempts by threat actors to manipulate private data sources. For example, we may see threat actors purposely trick AI by contaminating private data used by LLMs—such as deliberately manipulating emails or documents with false or misleading information—to confuse AI or make it do something harmful. This development will require heightened vigilance and advanced security measures to ensure that AI isn't fooled by bad information.

Daniel Rapp, Chief AI and Data Officer

2025: The Age of "Decision-Making Machines" through AI

Generative AI will move beyond content generation to become the decision-making engine behind countless business processes, from HR to marketing to DevOps. In 2025, AI will become an indispensable developers' "apprentice", doing everything from automating bug fixes, to testing and code optimization. The trend towards using AI-assisted development tools will accelerate in the next year, bridge skill gaps, reduce error rates, and help developers keep pace with the faster release cycles of DevOps. AI will also supercharge DevOps by predicting bottlenecks and preemptively suggesting optimizations. This will transform DevOps pipelines into "predictive production lines" and create workflows that fix issues before they impact production.

Ravi Ithal, Group General Manager, DSPM R&D and Product Management

Under Scrutiny, AI Will Become an Essential Part of How We Do Business

A few years ago, cloud computing, mobile and zero-trust were just the buzzwords of the day, but now they are very much a part of the fabric of how organizations do business. AI technologies, and especially Generative AI, are being scrutinized more from a buyer's perspective, with many considering them a third-party risk. CISOs are now in the hot seat and must try to get their hands around both the 'risk vs. reward' and the materiality of risk when it comes to AI tools. CISOs are asking exactly how employees are using AI to understand where they may be putting sensitive information at risk. As a result, there will be increased scrutiny around how LLMs are powering AI tools. Just like food packaging labels (which first surfaced back in the 60's and 70's) tell us what ingredients are used in the creation of a food product, today's CISOs will increasingly ask, "what's in this AI tool, and how do we know it's manufactured and secured correctly?"

Patrick Joyce, Global Resident Chief Information Security Officer (CISO)

The New Battlefield: Geopolitics Will Shape Cyber Espionage and the Rise of Regional Cyber Powers

2024 has demonstrated that state-aligned cyber espionage operations are deeply intertwined with geopolitical dynamics. In 2025, APT operations will continue mirroring global and regional conflicts. The cyber espionage campaigns preceding these conflicts will not be limited to large nations historically seen as mature cyber actors but will proliferate to a variety of actors focused on regional conflicts seeking the asymmetric advantage cyber provides.

Additionally, state-aligned adversaries will use cyber operations to support other national goals, like spreading propaganda or generating income. Targeted threat actors will likely leverage the continued balkanization of the internet to attempt to deliver their malicious payloads.

Joshua Miller, Staff Threat Researcher

Consumers Will be Testing Ground for Scamming Operations

In the early stages of fraud in the cyber or digital arena, individual consumers were the target; now, after two decades of evolution of the cybercrime ecosystem, we see ransomware operators "big game hunting" enterprise businesses for tens of millions of dollars.

Over time, layered defenses and security awareness have hardened organizations against many of the everyday threats. As a result, we have seen an uptick in actors once again leaning on individual consumers for their paydays. Pig butchering and sophisticated job scams are two examples that focus on social engineering outside of a corporate environment.

We will see a resurgence in the number of less sophisticated threat actors leveraging alternative communication channels, such as social media and encrypted messaging apps, to focus on fleecing individuals outside of enterprise visibility.

Selena Larson, Staff Threat Researcher

The "How" of the Threat Actor Landscape is Evolving Faster Than the "What"

The end game for cybercriminals hasn't evolved much over the past several years; their attacks remain financially motivated, with Business Email Compromise (BEC) designed to drive fraudulent wire transfers or gift card purchases. Ransomware and data extortion attacks still follow an initial compromise by malware or a legitimate remote management tool.

So, while the ultimate goal of making money hasn't changed, how attacks are conducted to get that money is evolving at a rapid pace. The steps and methods cybercriminals employ to entice a victim to download malware or issue a payment to a bogus "supplier" now involve more advanced and complex tactics and techniques in their attack chain.

Over the past year, financially motivated threat actors have socially engineered e-mail threads with responses from multiple compromised or spoofed accounts, used "ClickFix" techniques to run live Powershell, and abused legitimate services—like Cloudflare —to add complexity and variety to their attack chains.

We predict that the path from the initial click (or response to the first stage payload) will continue to become increasingly targeted and convoluted this year to throw defenders, and especially automated solutions, off their scent.

Daniel Blackford, Head of Threat Research

Smishing Goes Visual: MMS-Based Cyberattacks Will Flourish in 2025

MMS (Multimedia Messaging Service)-based abuse, consisting of messages that use images and/or graphics to trick mobile device users into providing confidential information or fall for scams, is a burgeoning attack vector that will expand rapidly in 2025. Built on the same foundation as SMS, MMS enables the sending of images, videos, and audio, making it a powerful tool for attackers to craft more engaging and convincing scams. Cybercriminals will embed malicious links within messages containing images or video content to impersonate legitimate businesses or services, luring users into divulging sensitive data. Mobile users are often unaware that they are using MMS, as it blends seamlessly with traditional SMS, creating a perfect storm for exploitation.

Stuart Jones, Director, Cloudmark Division

6 KEY TECHNOLOGY TRENDS AFFECTING THE SECURITY SECTOR IN 2025

JOHAN PAULSSON, CTO, AXIS COMMUNICATIONS, MATS THULIN, DIRECTOR CORE TECHNOLOGIES, AXIS COMMUNICATIONS, AND THOMAS EKDAHL, ENGINEERING MANAGER, AXIS COMMUNICATIONS

We’ve once again reached the time of year when we look ahead to some of the technology trends that will affect the security sector over the coming 12 months. The pace of change is as fast as ever.

Some of the trends are evolutions of those we’ve seen in previous years. An obvious one is the continued interest in how AI will be applied in our sector, and we’ve highlighted some of the new considerations that will need to be addressed moving forwards. Others are new, or even a resurgence of topics we may not have focused on for a while.

National and regional legislators will once again try to keep pace with technological innovation. AI, cybersecurity, privacy, the need for resilience in critical entities… All these (and more) will be the focus of proposed and new regulation. We haven’t highlighted this as a specific trend, but it’s no less a priority and something every organization will need to respond to.

We believe that within all of these trends lies significant opportunity for the sector. For our customers that means enhanced capabilities, more flexibility, greater efficiency and increased value.

Hybrid solutions: the foundation for freedom of choice

In previous years we’ve highlighted how hybrid architectures – those making best use of edge, cloud, and on-premise technologies – have become the de facto choice for security solutions.

The drivers for the choice of architecture will be unique to every organization, taking into account technological, legal, ethical and governance concerns and requirements. The environment is evolving quickly, and therefore freedom of choice is imperative.

Hybrid solutions give freedom of choice to store video, look at video or manage devices etc. Either by combining edge, cloud, and on-premise technologies to get an optimal total system solution or utilizing its flexibility choose the instance you prefer.

Whether demanded by emerging local and regional regulations or concerns over control of data, cost, or energy efficiency, hybrid solutions will continue to offer the greatest flexibility in creating architectures to best suit specific organizational needs and allow a system to be scaled.

AI evolution alongside AI efficiency

Development within the field of AI continues to race ahead. Deep learning technologies are the bread and butter of most analytics solutions within the security sector, while newer generative AI technologies are rapidly maturing. There is still a lot of hype in certain areas but real applications of generative AI in the security sector are becoming available. Each step of evolution brings with it a new set of opportunities, but also ethical, legal, and corporate considerations.

Generative AI models are large and require much compute capacity to execute, which creates a debate in how to balance the cost of AI (both in terms of financial investment, but also in terms of energy use and environmental impact) with its value. A lot of effort is being put into reducing the size of the models while maintaining the quality of results. The increased use of AI technologies only reinforces hybrid architectures as the standard.

The various 'flavors' of AI – from deep learning-based object recognition to generative AI – either demand or benefit from being applied at different places in the value chain, and in specific environments. Generative AI can assist operators in interacting with security solutions in natural language but, for the foreseeable future at least, require significant processing power. Conversely, deep learning-based analytics such as enhanced object recognition can be performed within surveillance cameras themselves.

Eventually this will enable generative models to be, at least partly, run on cameras with high-quality results. At the same time the models are improving in quality with regards to ethical aspects, bias, hallucinations, and the risk of making the wrong decisions.

Over time there is a big opportunity to dramatically change the efficiency and effectiveness of security operations. Algorithms will be able to understand what is happening in a scene and react to anomalies, based on the analysis on different types of input data, including but not limited to visual information. Input data will come from radar, audio, and numerous other sensors. This will create solutions that enable increasingly proactive capabilities and generate valuable insights in security scenarios for long term planning.

Beyond safety and security becomes real

The application of increasingly advanced computer vision, audio, access control and other connected technologies continues to serve security and safety use cases. Greater accuracy of analytics through the application of AI – particularly in object recognition – means that incidents can be responded to more quickly and effectively than ever before.

What is also clear is that the data generated by sensors of all types – video, audio, environmental, and more – can benefit numerous use case beyond the traditional. While still a relatively small part of the market, we expect to see an acceleration of applications aligned to operational efficiency and business intelligence.

This trend highlights the opportunities for increased collaboration across customer organizations. Technology being sourced or specified for one use case could well be used in another area of a business's operations. For instance, data being created by video cameras employed principally for security purposes can be analyzed over time to improve customer or employee experience, sustainability, or process efficiency.

Through the high-quality hardware platforms available, the pace of development and innovation is astounding. Hardware vendors that foster an open and collaborative ecosystem of application developers and system integrators will bring greatest value to customers most quickly.

The "rebirth" of image quality

It may be counterintuitive to suggest that a focus on image quality is a trend in the sector, where many would assume it's always been a priority (which, of course, it has). The trend is in how the images from visual sensors are being used, and with that the increased opportunities that better image quality brings.

The paradigm shifts when we consider that images are now often being initially viewed and analyzed by computers rather than humans, and that images are being viewed continuously, rather than when an incident of interest has taken place.

Advances in analytics and AI mean that a higher resolution image will inevitably lead to a better result, whatever the use case. Object recognition will be more accurate and more detailed data (and metadata) created. The drive towards even better image quality has been reignited.

With this has come opportunities for efficiency as well as effectiveness. A single camera producing much higher image quality can cover as large an area as multiple cameras would have been needed for previously. Higher resolution images also support analytics, for instance in large crowds, busy traffic intersections, or fast-moving production lines.

The human is still very much "in the loop", as the saying goes. Operators will be automatically alerted to scenes they need to pay attention to, increasing efficiency and effectiveness of a response. Image quality as a focus will also place keen attention on the maintenance of surveillance cameras – still often a manual task – as small obstructions can have a significant impact on analysis.

The long-term value in products comes through software support

At the higher end of the security sector, the quality of hardware has been improving year-on-year. Today, hardware devices can be of such high-quality – particularly in terms of performance and capabilities – that expectations about their lifetime are greater than ever.

But while quality hardware can last for many years - as illustrated by the length of warranties - the defining factor in a camera's functionality, including cybersecurity, and therefore its lifetime value, comes through ongoing software support.

Vendor commitments to support software throughout the expected lifetime of the hardware are essential; software that continues to enhance and build on the capabilities of the camera and keep it as secure as possible.

This also underpins the total cost of ownership of hardware. An investment in better quality camera, with comprehensive software support throughout its lifecycle, will ultimately be a more effective and efficient solution.

Technology autonomy to the customer's benefit

Our role, and that of our partner ecosystem, is ultimately to focus on meeting the needs of customers. Technology for technology's sake serves nobody's purpose - innovations must be aligned to the priorities of the end user.

This clearly means supporting customers' goals in safety and security, operational efficiency, and business intelligence. But it also means supporting their cybersecurity posture, commitment to sustainability through energy efficient solutions, and flexibility and freedom of choice via open standards-based technologies and platforms.

Technology vendors with more autonomy over their core technologies are clearly best placed to support these customer requirements. Greater control over foundational technology, from the silicon "upwards", will allow a vendor to design specific capabilities and functionality aligned to customer needs into its products. Such an approach to core technology ownership will also allow a vendor to stand by commitments of being "secure by design".

Furthermore, greater control of technology - at a component or even material level - is an important prerequisite to more effectively mitigate the risks of broader disruption to global supply chains. This enhances the ability to meet the requirements of customers, when they are needed.

We're already seeing companies that would have traditionally been seen as software vendors designing their own semiconductors to gain more control over their service delivery – particularly in the area of AI – and we foresee this trend continuing in all sectors. Core technology independence is a trend we're proud to say we're some way ahead of, having developed our own system-on-chip, ARTPEC, for the last 25 years.

So, there you have it, our take on some of the trends that will shape the security sector in 2025. We're sure you'll have views on these and maybe some other trends of your own. We'd be delighted to continue the discussion on this with you.