

Security ADVISOR

MIDDLE EAST

Empowering WOMEN IN TECH





Smart Monitoring Solutions

Free Lifetime Video Recording

3 Year Warranty

Free Installation

Free after-sales service

Keep an eye on your home even when you are away

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

Starts at AED 20*



For more information, lookup Smart Monitoring at www.etisalat.ae/smartmonitoring

*Terms and conditions apply

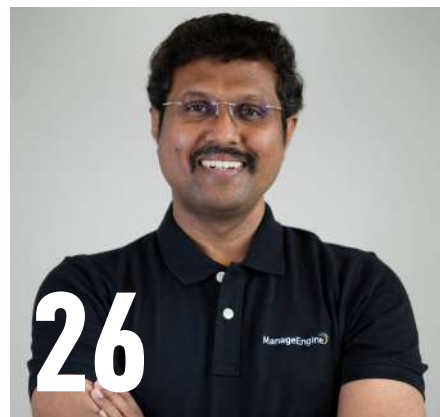


10

EMPOWERING FUTURE: WOMEN IN GENAI AND THEIR GROWING ROLE IN A GLOBAL WORKFORCE



16



26



46

6 CrowdStrike first cloud-native cybersecurity ISV to exceed \$1 billion in annual AWS marketplace sales

26 ManageEngine ushers in a new era of customizable and unified security analytics with its Open API-Based platform

16 The Women in Tech Awards 2025 spotlights the UAE's role in empowering women innovators

46 Goodbye CISO scapegoating - The age of corporate accountability is here



CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD
CLEANROOM™ RECOVERY



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

EDITOR'S NOTE



Talk to us:

E-mail:
sandhya.dmello@cpimediagroup.com

Sandhya DMello
Editor

EMPOWERING INNOVATION AND SECURITY: WOMEN IN GENAI AND CYBERSECURITY TRENDS IN THE MIDDLE EAST

The Middle East continues to assert its position as a hub of technological innovation and resilience, with this issue of Security Advisor Middle East spotlighting two critical narratives shaping the future: the rising influence of women in Generative Artificial Intelligence (GenAI) and the evolving cybersecurity landscape. Our lead feature, "Empowering Future: Women in GenAI and their Growing Role in a Global Workforce," explores how women are breaking barriers in the rapidly expanding GenAI sector, projected to surpass \$88 billion globally this year. The UAE's leadership in this space is particularly notable, as evidenced by the Women in Technology Forum and Awards 2025, which aligns with International Women's Day's call to 'Accelerate Action' for gender equity. Dr. Alexandra Urban of Coursera praises the region's progress, while Dr. Barbara Oakley reminds us to balance equity with respect for individual choice—a nuanced perspective that resonates deeply in this transformative era. Parallel to this, the cybersecurity

domain remains a top priority as threats grow more sophisticated. From Positive Technologies uncovering a new malware campaign targeting the Middle East and North Africa, to Group-IB's High-Tech Crime Trends Report highlighting state-sponsored attacks on GCC countries, the stakes have never been higher. Innovations from industry leaders like Sophos, CrowdStrike, Rubrik, and ManageEngine underscore a collective push toward AI-driven security and resilience, while Visa's Tap to Add Card launch in Saudi Arabia exemplifies how convenience and security can coexist. As Extreme

CHARTING AN INNOVATIVE PATH IN THE REGION

Networks appoints Anisha Vaswani as Chief Information and Customer Officer and IDEMIA Public Security expands its partnership with Tahakom for road safety in the Kingdom, we see a region embracing both human ingenuity and technological advancement.

This issue celebrates the synergy of diversity, innovation, and vigilance—key pillars for a secure and equitable digital future in the Middle East and beyond.

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

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

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

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

DIGITAL SERVICES
Web Developer
Adarsh Snehanjan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

© Copyright 2025 CPI
All rights reserved

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

CROWDSTRIKE FIRST CLOUD-NATIVE CYBERSECURITY ISV TO EXCEED \$1 BILLION IN ANNUAL AWS MARKETPLACE SALES

CrowdStrike's sales deals average 4x larger when transacted in AWS Marketplace.

CrowdStrike has announced it is the first cloud-native cybersecurity independent software vendor (ISV) to exceed \$1 billion in sales through AWS Marketplace within a calendar year. This milestone underscores the ease and simplicity of AWS Marketplace – a curated digital catalog that customers can use to find, subscribe to, deploy and govern third-party software, data and services to build solutions and run their businesses – and the growing demand for cybersecurity consolidation on the CrowdStrike Falcon® platform.

As the threat landscape becomes increasingly complex and sophisticated, organizations are looking to consolidate disparate cybersecurity tools and processes into a single platform to bolster their security posture and improve operational efficiencies. With the CrowdStrike Falcon® cybersecurity platform in AWS Marketplace, customers can more easily procure and deploy solutions to consolidate point products and secure their organizations across the entire attack surface while running on the most flexible and secure cloud computing environment available today.

"The market continues to send a clear message – many of the world's most innovative companies build their cloud businesses on AWS and secure them with CrowdStrike," said Daniel Bernard, Chief Business Officer, CrowdStrike. "CrowdStrike's unprecedented traction in AWS Marketplace is a testament to our strategy and execution, aligning the CrowdStrike partner go-to-market ecosystem to leverage AWS Marketplace in driving Falcon platform adoption at scale. Together with AWS, we look forward to bringing the power of the Falcon platform to even more organizations worldwide, across industries and market segments."



Daniel Bernard, Chief Business Officer, CrowdStrike

In October 2023, CrowdStrike became the first cloud-native cybersecurity ISV to exceed \$1 billion of software sales through AWS Marketplace, less than six years after CrowdStrike first made the Falcon platform available in AWS Marketplace. From January 1, 2024 to December 31, 2024, CrowdStrike exceeded \$1 billion in AWS Marketplace sales. CrowdStrike's network of partners, which includes leading resellers, system integrators, distributors and managed services providers are also able to drive sales in AWS Marketplace, empowering partners to deliver seamless, scalable and industry-leading cybersecurity solutions to customers worldwide on their preferred cloud platform.

Growth points highlighting CrowdStrike's year-over-year (YoY) business traction in AWS Marketplace include:

- 91% YoY global sales growth

- 48% YoY Europe, Middle East and Africa (EMEA) sales growth
- 136% YoY global public sector sales growth
- 3,548% YoY global growth in distributor sales
- CrowdStrike's deals average 4x larger when transacted in AWS Marketplace
- AWS Marketplace customers use an average of 7 CrowdStrike Falcon platform modules

"AWS Marketplace continues to be the go-to-destination for AWS customers to procure, deploy, and govern IT solutions to innovate and scale their business," said Ruba Borno, Vice President, Global Specialists and Partners, AWS. "CrowdStrike's achievement of \$1B in revenue through AWS Marketplace in 2024 underscores the value of the Falcon platform in helping customers innovate faster with greater confidence in their

security. This milestone marks another step in our continued partnership with CrowdStrike to help organizations build, operate, and secure their business.”

This milestone follows a strategic collaboration agreement the two companies announced in 2024 that included Amazon unifying its cybersecurity protection on the CrowdStrike Falcon® platform and CrowdStrike expanding its use of AWS services, including Amazon Bedrock and Amazon SageMaker, to build and deploy custom models, such as Charlotte AI. Charlotte AI is CrowdStrike’s generative AI agentic security analyst that benefits from the scalability, flexibility, and resiliency of AWS while helping customers meet stringent security requirements for generative AI usage.

CrowdStrike was named the AWS 2024 Global Security Partner of the Year, AWS North America Marketplace Partner of the Year, AWS MENA Technology Partner of the Year, and AWS LATAM Public Sector Technology Partner of the Year – recognizing its critical role in helping customers secure innovation built on AWS.

“Our cyber security transformation

journey is focused on people, processes and technology. We have made significant changes in our technology stack and focused on proven market leaders in their respective areas such as CrowdStrike and AWS for secure cloud capabilities,” said Kostas Georgakopoulos, Chief Information Security and Technical Officer, Mondelez International. “Through AWS Marketplace, we selected CrowdStrike and have consolidated our cybersecurity stack on the Falcon platform. This transformation has eliminated immeasurable amounts of operational complexity and sunk costs. Together, AWS and CrowdStrike have transformed not just our cloud and cybersecurity strategies, but the way we do business.”

“As organizations move more critical infrastructure to AWS, security and how customers procure it, cannot be an afterthought; it must evolve alongside them,” said Conor Waddell, SVP of Integrated Technology Solutions at CDW. “From infrastructure to endpoints, CDW is committed to providing global organizations with seamless, intelligent security that adapts to change, without adding

complexity or slowing down operations. By combining CrowdStrike’s industry-leading threat protection with our deep cloud expertise – bolstered by our recent Mission Cloud acquisition – and the power of the AWS Marketplace, CDW ensures customers have frictionless access to the end-to-end security they need to operate with confidence.”

“This milestone cements how AWS and CrowdStrike are transforming the channel ecosystem. CrowdStrike has demonstrated that when a market-leading ISV and channel partners collaborate through AWS Marketplace, they win customers faster and drive larger, high-value deals,” said Jay McBain, Chief Analyst at Canalys. “Surpassing \$1 billion in annual sales highlights the surging demand for unified, cloud-native security platforms that simplify operations, enhance protection, and deliver measurable ROI in the AI era. This is a pivotal moment for both CrowdStrike and AWS as they redefine how cybersecurity vendors and partners go to market – fueling innovation, security, and growth in the cloud.”

POSITIVE TECHNOLOGIES EXPERTS UNCOVER NEW MALWARE CAMPAIGN IN THE MIDDLE EAST

Three-quarters of potential victims are residents of Libya, Saudi Arabia, and Egypt

Threat Intelligence specialists at the Positive Technologies Expert Security Center (PT ESC) have identified and analyzed a new malware campaign targeting individuals in the Middle East and North Africa. Active since September 2024, the campaign uses a modified version of AsyncRAT to target victims. To spread the malware, the attackers posed as news outlets on social media, creating pro-motional posts with links to file-sharing platforms or Telegram channels. The modified malware is designed to steal cryptocurrency wallet data and communicate with a Telegram bot.

The investigation revealed

approximately 900 potential victims, most of whom are everyday users. Among those affected are employees working in industries such as oil and gas, construction, IT, and agriculture.

Analysis showed that most victims are located in Libya (49%), Saudi Arabia (17%), Egypt (10%), Tur-key (9%), the UAE (7%), Qatar (5%), and other countries.

The group behind the campaign was dubbed Desert Dexter, named after one of the suspected au-thors. During the investigation, researchers found that the attackers rely on temporary accounts and fake news channels on Facebook to bypass the platform’s ad filters. A

similar attack was docu-mented by Check Point researchers in 2019, but the campaign described here introduces new techniques to the attack chain.

Denis Kuvshinov, Head of Threat Intelligence, Positive Technologies Expert Security Center, said: “This attack follows a multi-stage process. The victim is lured from a promotional post to a file-sharing service or a Telegram channel operated by the attackers, which imitates a media outlet. From there, the victim receives a RAR archive containing malicious files. These files download and execute AsyncRAT, gather necessary system information, and send it to the attackers’

Telegram bot. The AsyncRAT version used in this campaign includes a modified IdSender module that collects information about cryptocurrency wallet extensions, two-factor authentication extensions in various browsers, and software used to manage cryptocurrency wallets.”

While Desert Dexter’s tools are not particularly sophisticated, their use of social media ads, legitimate services, and the geopolitical context of the region has made the campaign effective. The group posts messages about allegedly leaked confidential information, making the attack chain versatile enough to infect the devices of not only regular users but also high-ranking officials.

Researchers note that ongoing tensions in the Middle East and North Africa have made the region a prime target for cyberattacks aimed at both government institutions and individual users. Political themes remain a common lure in phishing campaigns, with attacks becoming more sophisticated and malware being continuously adapted to meet the needs of different threat actors.



Positive Technologies experts uncover new malware campaign in the Middle East

SOPHOS AND PAX8 ANNOUNCE STRATEGIC PARTNERSHIP TO STREAMLINE SECURITY MANAGEMENT

Sophos’ Portfolio of Cybersecurity Solutions is the Most Comprehensive Security Offering on the Pax8 Marketplace

Sophos, a global leader of innovative security solutions for defeating cyberattacks, today announced a strategic partnership with Pax8, the leading cloud commerce marketplace. The collaboration introduces the most comprehensive portfolio of cybersecurity solutions available to Pax8’s network of more than 40,000 managed service providers (MSPs). MSPs in the Pax8 network now have a complete one-stop shop of best-in-class cybersecurity solutions available from a single vendor – including Sophos Managed Detection and Response (MDR), Sophos Endpoint powered by Intercept X and Sophos Firewall. This revolutionizes opportunities for channel partners to

streamline operations, simplify billing and significantly reduce the complexity of cybersecurity management across customers.

According to the Sophos MSP Perspectives 2024 report, MSPs that consolidate their security stack with a single vendor can cut daily security management time by nearly 50% – a savings that jumps to 69% for those juggling six or more security vendors. By partnering with Pax8, Sophos is removing a key operational barrier for MSPs, enabling them to seamlessly manage cybersecurity through a single vendor platform to streamline solution integration and enhance efficiency while

strengthening their security posture and simplifying cloud procurement cycles.

“Sophos and Pax8 are strongly aligned in our mission to empower MSPs with best-in-class end-to-end security services and products while simplifying lifecycle management of these solutions and reducing operational overhead. MSPs want to align with vendors who are easy to work with and this agreement will make it even easier for MSPs to work with Sophos, something we’ve long been committed to,” said Joe Levy, CEO of Sophos. “With cybersecurity, speed and innovation are essential for defending against attackers. This partnership with Pax8 accelerates MSP access to critical

cybersecurity tools, enabling them to better protect their customers in an increasingly complex and volatile threat landscape.”

Key advantages of the Sophos and Pax8 partnership for MSPs include:

- Driving new revenue opportunities for partners by providing the most comprehensive portfolio of security offerings by a single vendor on the Pax8 Marketplace.
- Reducing overhead costs and freeing up partners’ billable hours by simplifying procurement and billing via a fully integrated Pax8 Marketplace experience.
- Empowering partners with seamless experiences through coordinated MSP enablement, support and sales training initiatives.
- Compatible and comprehensive 24/7 security for MSPs’ Microsoft Defender customers with Sophos’ MDR service for Microsoft environments.

“MSPs today need solutions that align with the way they operate—cloud-first, flexible and easy to manage at scale. Pax8 is revolutionizing the way MSPs access and deploy cloud-based solutions, and cybersecurity is an important piece of the overall stack,” said Scott Chasin, Chief Executive Officer of Pax8. “By bringing Sophos’ innovative security offerings to our marketplace, Pax8 is providing our partners with access to enterprise-grade security solutions for their SMB customers in a way that simplifies management, reduces risk and drives profitability.”

Comprehensive Security, Unparalleled Efficiency

“MSPs say they could cut day to day management time almost in half by consolidating on a single cybersecurity platform – and Sophos enables them to achieve that goal. By managing all their customers’ cybersecurity in the cloud-based Sophos Central platform, MSPs can reduce workload and free up valuable billing hours,” said Raja Patel,



Chief Product Officer, Sophos. “What’s more, with a complete portfolio of Sophos cybersecurity solutions at their fingertips, Pax8 MSPs enjoy extensive opportunities to sell additional revenue-generating products and services that meet their clients’ evolving cybersecurity needs.”

Backed by real-time threat intelligence from Sophos X-Ops, a global team of elite threat hunters and security analysts, Sophos’ solutions provide proactive, AI-driven protection against cyberattacks. As the leading pure-play cybersecurity provider of MDR services, Sophos protects over 28,000 organizations globally. Insights from Sophos MDR further strengthens security by providing MSPs and their customers with unparalleled protection. Automated threat detection, managed response, and deep security insights across Sophos’s portfolios equip MSPs to enhance defenses, minimize risk exposure, deliver enterprise-grade protection and cut through the noise to reduce management complexity.

Better security for Microsoft environments

More than 60% of Sophos MDR’s customers are managed via MSPs, giving Sophos unparalleled insights into attacks on MSP-managed environments. Sophos leverages these learnings to

update customers’ defenses in real-time, optimizing their protection from ever-evolving attacks and providing peace of mind to both clients and partners. Furthermore, with Sophos’s robust MDR service for Microsoft environments, Pax8 MSPs can elevate the security of clients using Microsoft Defender while enabling their customers to see greater return on their Microsoft investments.

The Sophos MDR service through Pax8 supports MSPs in several ways. They can either leverage Sophos’ managed service completely or to augment their customers’ in-house department, including coverage on nights and weekends, which are critical times to defend networks because they are when attackers often strike. For MSPs that provide in-house MDR services, the new AI Assistant in Sophos XDR enables operators of all skill levels to neutralize adversaries faster with existing threat investigation and response intelligence from frontline Sophos MDR analysts.

Availability

The Sophos offering is available on the Pax8 Marketplace starting February 28, 2025. Pax8 partners interested in learning more about Sophos offerings coming to the Pax8 Marketplace can learn more and sign up at www.sophos.com/msp.





EMPOWERING FUTURE: WOMEN IN GENAI AND THEIR GROWING ROLE IN A GLOBAL WORKFORCE

■ BRIDGING THE GENDER GAP IN GENAI TO
DRIVE INNOVATION AND EQUITY

By Sandhya D'Mello

Generative Artificial Intelligence (GenAI) — technology that creates text, images, and other content — is transforming industries and the global workforce, and women are stepping into key roles within this exciting field.

Women are emerging as key contributors in the field of GenAI, a technology reshaping industries and the global workforce. In 2025, with the GenAI market projected to exceed \$88 billion globally, according to industry estimates, their role is increasingly vital to fostering innovation.

Shifting landscape

The adoption of GenAI has surged, with the WEF's Future of Jobs Report 2025 noting that 86% of surveyed employers—representing over 14 million workers across 55 economies—anticipate AI and information-processing technologies will transform their businesses by 2030. This shift is expected to create 170 million new jobs globally while displacing 92 million existing roles, highlighting the magnitude of change underway.

Women are starting to play a significant role in this transformation, using GenAI to boost productivity and innovation in sectors like healthcare, education, and technology. The WEF's Global Gender Gap Report 2024 reports a post-pandemic rise in women's labor force participation, climbing from 63.5% in 2023 to 65.7% in 2024 across 101 tracked countries, a trend that could amplify their impact in AI-driven fields.

Research Insights: Progress and Persistent Gaps

WEF research offers a detailed perspective on women's position in the GenAI landscape. According to the Future of Jobs Report 2025, technology, particularly AI, ranks as the most disruptive force shaping labor markets, surpassing other macro trends. Women's representation in



Dr. Alexandra Urban

tech has advanced—reaching 28.2% of the STEM workforce in 2024, per the Global Gender Gap Report—yet their share in AI-specific roles remains lower, aligning with industry estimates of around 22%. Progress is evident, however, with LinkedIn data cited in the 2024 report showing female participation in AI engineering has more than doubled since 2016, especially in sectors like Technology, Information, and Media.

The Future of Jobs Report 2025 projects that 39% of current skill sets will become obsolete by 2030, with 63% of employers identifying skill shortages as the top obstacle to digital transformation—a barrier that disproportionately impacts women due to limited training access. The Global Gender Gap Report 2024 cautions that achieving global gender parity could take 134 years at current rates, with

women in tech facing a steep climb to senior roles.

Challenges persist despite these gains. The WEF indicates that only 30% of learners in AI and big data courses on platforms like Coursera are women, constraining their ability to address workforce skill gaps in high-demand fields.

Strategies to close the gender gap

Coursera, a leading online learning platform, recently released the 'Closing the Gender Gap in GenAI Skills' playbook, a new resource aimed at addressing the gender gap in GenAI skills. The playbook explores actionable strategies to empower more women to harness GenAI, highlighting the critical need for continued efforts to build a more inclusive and equitable AI landscape.

Women currently represent 32% of

global GenAI enrollments on Coursera. In the UAE, they make up 23.8% of GenAI learners—a figure that, while reflecting ongoing efforts to increase female participation in STEM, also underscores the gender gap that still exists in GenAI. While AI education in the UAE continues to expand rapidly, the need for targeted strategies to ensure equitable access to GenAI opportunities remains.

Amid this disparity, interest in AI skills continues to rise. In 2024, the UAE saw over 900% increase in enrollments for GenAI courses. Women also account for 56% of government university graduates in STEM fields. However, despite these advancements, female representation in leadership remains limited, with nearly 11% of board positions held by women. This highlights the challenge of translating educational progress into greater professional advancement and reinforces the need for further action to drive gender inclusivity in technology

“THE UAE’S COMMITMENT TO BRIDGING THE GENDER GAP IN TECHNOLOGY IS COMMENDABLE. A DIVERSE AND INCLUSIVE TECH WORKFORCE IS ESSENTIAL FOR DRIVING INNOVATION, ESPECIALLY IN TRADITIONALLY MALE-DOMINATED FIELDS LIKE AI. WHILE PROGRESS IS EVIDENT, EXPANDING OPPORTUNITIES FOR WOMEN IN GENAI, EQUIPPING THEM WITH CRITICAL SKILLS, AND EMPOWERING THEM TO LEAD IN THE DIGITAL ECONOMY REMAINS AN URGENT PRIORITY.”
DR. ALEXANDRA URBAN, LEARNING SCIENCE RESEARCH LEAD AT COURSERA

leadership and beyond.

Dr. Alexandra Urban, Learning Science Research Lead at Coursera, said: “The UAE’s commitment to

bridging the gender gap in technology is commendable. A diverse and inclusive tech workforce is essential for driving innovation, especially in



Dr. Barbara Oakley

traditionally male-dominated fields like AI. While progress is evident, expanding opportunities for women in GenAI, equipping them with critical skills, and empowering them to lead in the digital economy remains an urgent priority.”

The playbook recognizes the systemic barriers to women’s participation in GenAI and identifies key challenges that must be addressed, including: Confidence gaps reduce persistence; and perceived lack of relevance.

Coursera’s insights are designed to equip women with strategies to thrive in the rapidly evolving field of GenAI, aligning with the UAE’s National Strategy for AI 2031, which underscores the importance of women taking an active role in shaping the future of AI. The UAE ranks among the top 10 countries in AI companies per capita, increasing female participation in GenAI will be key to advancing the nation’s AI and digital transformation ambitions.

Dr. Barbara Oakley, Professor of Engineering at Oakland University and Coursera’s inaugural “Innovation Instructor,” highlights the unique challenges women face when engaging with GenAI. “Research shows that women often excel in communication and interpersonal skills,” she explains, “which may contribute to hesitancy toward fields perceived as less people-oriented, like GenAI and STEM.”

To counteract this hesitancy, Oakley advocates for the power of relatable female role models and real-world applications in GenAI learning. “Connecting AI concepts to real-world communication can resonate strongly with many learners, including women,” she notes.

Beyond boosting enrollment, Oakley stresses that self-directed curiosity must be nurtured rather than forced. “We have to be careful not to push too hard in the name of equity for women. We also need to respect women’s choices,” she advises, emphasizing the importance of inclusive course design that removes barriers while allowing women to engage at their own pace.

The Business Imperative

Including women in GenAI is a strategic necessity, not merely an equity concern. The WEF’s Future of Jobs Report 2025 stresses that AI-driven job growth, such as roles for AI and machine learning specialists, demands diverse teams to reduce bias and enhance impact. Women contribute essential soft skills—strategic leadership and collaboration—where they outperform men by 28%, per LinkedIn data from 2024 cited by the WEF. These strengths are crucial for crafting human-centric AI solutions that serve diverse populations.

The economic implications are substantial. The WEF’s ChatWTO: An Analysis of Generative Artificial Intelligence and International Trade 2024 report estimates that GenAI could add \$4.4 trillion annually to the global economy. Realizing this potential depends on a skilled workforce. With 85% of employers planning to prioritize upskilling by 2030 (Future of Jobs Report 2025), and 70% aiming to hire for AI-specific roles, addressing the gender gap in training and recruitment is essential. Companies with diverse AI teams are better positioned to innovate, a point reinforced by the WEF’s

emphasis on responsible AI governance in its AI Governance Alliance initiatives.

Charting the Path Forward

To integrate women fully into the GenAI ecosystem, businesses must take decisive action. The WEF’s Future of Jobs Report 2025 advocates for proactive reskilling, with 77% of employers committed to funding workforce development to enhance productivity. Targeted programs for women—especially in AI and big data, where participation lags—can address the 33% of workers who report limited access to GenAI tools, as noted in broader industry surveys. The WEF’s Global Gender Parity Sprint 2030 initiative calls for reshaping labor markets through technology, positioning gender equity as a pillar of sustainable growth.

Collaboration is critical. The WEF’s AI for Impact white paper (2024) underscores AI’s potential as a tool for social innovation when deployed ethically, a mission women in GenAI can advance with diverse perspectives. As 50% of businesses restructure for AI integration (Future of Jobs Report 2025), leadership must ensure women are included. Initiatives like the WEF’s Reskilling Revolution platform, reaching over 350 million people since 2020, provide a model for scaling these efforts.

Women in GenAI stand at a defining moment. The WEF’s 2025 data reveals a workforce in flux, with AI offering vast opportunities alongside significant challenges. By leveraging women’s growing presence—supported by a 65.7% labor participation rate and rising AI talent—businesses can unlock innovation and equity. Closing the gender gap, however, demands sustained investment in skills, access, and leadership opportunities. In an AI-driven world, empowering women is not just a moral duty—it’s the bedrock of a resilient, inclusive, and prosperous global economy. 🌟

WE HAVE TO BE CAREFUL NOT TO PUSH TOO HARD IN THE NAME OF EQUITY FOR WOMEN. WE ALSO NEED TO RESPECT WOMEN’S CHOICES.”
DR. BARBARA OAKLEY, PROFESSOR OF ENGINEERING AT OAKLAND UNIVERSITY

1ST

IN THE REGION

PIONEERING CONVERSATIONAL AI AS A SERVICE

Our Industry Landscape



Retail



Healthcare



Banking



Education



Oil & Gas

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

SCAN QR



LEARN MORE

OMNIX
Conversational **AI**



 tahawultech.com

Women in TECHNOLOGY FORUM AND AWARDS

Beyond Boundaries, Building Tomorrow

The UAE is steadfastly encouraging women's active participation in technology, recognizing that an inclusive digital future depends greatly on gender diversity and equality. Through dedicated initiatives such as women-focused tech incubators, targeted educational programs, and strategic mentorship, the country is ensuring women have every opportunity to excel in STEM fields. By championing women's roles in technology today, the UAE is shaping an inclusive and dynamic future, fostering resilient generations poised to lead the nation toward continued innovation and global competitiveness.

Following is the list of winners of the Women In Tech Awards 2025



Inspirational Woman Leader 2025
Esha D'Souza
 Corporate Group



Inspirational Woman Leader 2025
Dr. Pallavi Ranjan
 Murdoch University Dubai



Inspirational Woman Leader 2025
Vasudha Khandeparkar
 Grant Thornton – UAE



Inspirational Woman Leader 2025
Zina Ashour
 Women in Crypto Arabia (WIC)



Inspirational Woman Leader 2025
Mariana Missakian



Inspirational Woman Leader 2025
Mary O'Leary



Inspirational Woman Leader 2025
Suraya Turk
 Legal Circle



Woman Leader of the Year
Sherifa Hady
 HPE Aruba Networking



Cybersecurity Sales Visionary of the Year
Meriam ElOuazzani
 SentinelOne



Technology Visionary Leader of the Year
Haidi Nossair
 Dell Technologies



Marketing Visionary of the Year
Yasmin Khaliq
 Equinix



Marketing Visionary of the Year
Naghah Halaby
 Infor

Following is the list of winners of the Women In Tech Awards 2025



Marketing Visionary of the Year
Sirin Akrouk
Pure Storage



Technology Leadership Innovator of the Year
Loubna Imenchal
Logitech



Influential Sales Personality of the Year
Nigina Bender
Jabra



Woman Executive of the Year
Sheeba Sultan Hasnain
SENTIENTE



Senior Marketing Leader of the Year
Kristin McDonald
Kaspersky Middle East



Senior Marketing Leader of the Year
Shradha Subramanian
Nutanix



Senior Marketing Leader of the Year
Zeina Haggag
OPSWAT



Senior Marketing Leader of the Year
Gunika Arora
Kyriba



Technology Executive Leader of the Year
Fionnuala Morris
Kyndryl



Marketing Excellence in Operations & Analytics
Litty Reji
TechBridge Distribution



Marketing Executive of the Year
Joumana Karam
Acer



Marketing Pioneer of the Year
Manal Abi Rafeh
Fortinet

Following is the list of winners of the Women In Tech Awards 2025



Technology Frontrunner of the Year
Eliane Geroges
Dynatrace



Innovative Marketing Leader of the Year
Nidhi Aiyanna
Citrix



Innovative Marketing Leader of the Year
Nabila Ayatti
Mindware



Innovative Marketing Leader of the Year
Amrita Ghanty
Cyble



Innovative Marketing Leader of the Year
Shaed Khader
Logicom Distribution



Influential Channel Personality of the Year
Sabine Salloum
Commvault



Marketing Strategist of the Year
Chanchal Hotwani
Ingram Micro Gulf



Marketing Strategist of the Year
Zainab Yusuf
StorIT Distribution FZCO



Marketing Strategist of the Year
Sonali Basu Roy
Bulwark Technologies



Channel Sales Rising Star of the Year
Widad Abdalhadi
Cisco



Technology Businesswoman of the Year
Areej Khan
Innoxhub Global



Influential Marketing Personality of the Year
Mary Mikhail
SentinelOne

Following is the list of winners of the Women In Tech Awards 2025



Strategic Sales Leader of the Year
Anita Quadros
Wesco Anixter



Strategic Sales Leader of the Year
Konika Khandelwal
Inception - A G42 Company



Strategic Sales Leader of the Year
Reena Alex John
Finesse



Brand Awareness Marketeer of the Year
Bindhya Ramadasa
Forescout Technologies Inc.



Brand Awareness Marketeer of the Year
Eleni Papapostolou
Vectra AI



Brand Awareness Marketeer of the Year
Meenakshi Vashisht
VisionTech Systems International LLC



Brand Awareness Marketeer of the Year
Reshma Yasodharan
emt Distribution META



Brand Awareness Marketeer of the Year
Heeba Siddiqua
VAD Technologies



Marketing Rising Star of the Year
Dannah Jane Gargar
Gulf Business Machines (GBM)



Marketing Rising Star of the Year
Nana Xu
Hikvision FZE



Marketing Rising Star of the Year
Safa Qamar
NX Digital Technology



Marketing Rising Star of the Year
Thriпти Rao
Jedox

Following is the list of winners of the Women In Tech Awards 2025



Marketing Rising Star of the Year
Saranya Chandradas
 MITSUMI Distribution



Marketing Rising Star of the Year
Krishnapriya Nikhil
 Digit Solutions LLC

Marketing Visionary of the Year
Nichola Banerjee
 Nextthink

Marketing Visionary of the Year
Raji Joy John
 StarLink

Senior Marketing Leader of the Year
Khushnida Akramova
 Seidor MENA

Technology Trailblazer of the Year
Lena Halbourian
 Commvault

Technology Icon of the Year
Ekta Puthran
 Barco

Influential Marketing Personality of the Year
Tarannum Mohammed Saqib
 TP-Link

Marketing Rising Star of the Year
Tamara Zbibo
 Zero&One

Brand Relationship Executive of the Year
Rasha A. Zaki
 Cisco

Brand Relationship Personality of the Year
Rima Taha
 Huawei Technologies

Technology Champion of the Year
Manju Mathew
 StorIT Distribution FZCO

Transformational Marketing Leader of the Year
Mallika Sharma
 HPE Aruba Networking

Marketing Strategist of the Year
Anusree M.
 Avientek

Influential Marketing Personality of the Year
Chantelle Tavid
 NVIDIA

Strategic Sales Leader of the Year
Nandini Sapru
 emt Distribution META







RUBRIK'S NEW CAPABILITIES SET TO TRANSFORM CYBER RESILIENCE ACROSS CLOUD, HYPERVISOR AND SAAS PLATFORMS

Rubrik has announced significant innovations designed to enhance protection for cloud, SaaS, and on-premises environments. The innovations aim to provide customers with even more ability to anticipate breaches, detect potential threats, and recover with speed and efficiency no matter where their data lives.

“Cyber criminals won’t stop innovating, and neither will we. Our utmost priority is the security, safety, and appropriate accessibility of our customer’s data, regardless of where the data lives,” said Arvind Nithrakashyap, Chief Technology Officer and Co-Founder of Rubrik.

“We are seamlessly integrating new technologies across the world’s major cloud platforms, SaaS offerings, and on-premises so our customers can better detect compromised data, enhance the speed of identifying affected data, and accelerate the discovery of clean entry points.”

Expanding cloud adoption and recent hypervisor industry consolidation are driving broad re-platforming of business-critical operations. Rubrik is meeting customers at their platform of choice, delivering unified management, advanced cyber resilience capabilities, and enhanced visibility across more cloud, SaaS, and enterprise apps.

- **Cloud Posture Risk Management (CPR):** CPR addresses the lack of data visibility by automatically discovering and inventorying cloud data assets and identifying unprotected or sensitive data. CPR



Arvind Nithrakashyap, Chief Technology Officer and Co-Founder of Rubrik

helps organizations make informed backup decisions and strengthen their overall backup posture by protecting only what truly matters, reducing risk and unnecessary costs.

- **Oracle Cloud Protection:** Rubrik Security Cloud (RSC) is planned to support data protection for Oracle Cloud Infrastructure (OCI) — beginning with Oracle Cloud VMWare (OCVS) workloads and self-managed Oracle DB workloads operating OCI VMs. The solution is designed to enable customers to safeguard their cloud-based environments with the same robust, unified backup and

recovery capabilities they rely on for other cloud and on-premises data.

- **Expanding Data Protection to PostgreSQL:** Rubrik recognizes the critical importance of fortifying data defenses across all platforms. According to a recent Rubrik Zero Labs report, attackers are targeting backups in 96% of cyberattacks. By extending coverage to PostgreSQL, Rubrik ensures that one of the world’s most popular open-source databases thrives in the face of evolving digital threats. The comprehensive data security solution provides organizations with the assurance of maintaining data

- backup, availability, and recoverability.
- **Red Hat OpenShift Virtualization Data Protection:** Sixty-percent of enterprises have adopted Kubernetes, emphasizing the critical need for cyber resilience solutions for their critical workloads. Rubrik's new OpenShift support marks a significant step in securing these environments with comprehensive, automated, and immutable backups that deliver fast recovery from cyber incidents. Businesses have the flexibility to choose virtualization platforms for critical business processes without compromising manageability or cyber resilience.
 - **Azure DevOps and GitHub Backup:** For organizations using continuous integration and continuous development to accelerate innovation, Rubrik now protects Azure DevOps and GitHub with cyber resilient automated backups, granular recovery, extended retention, and robust compliance coverage for critical data stores.
 - **Rubrik Cloud Vault (RCV) for Amazon Web Services, Inc. (AWS):** RCV reduces the complexity and cost of managing a highly secure off-site archival location, with flexible policies and/or regions. RCV features immutable, isolated, logically air-gapped off-site backups combined with role-based access controls, advanced encryption, and retention locks to provide unparalleled confidence in data recovery.
 - **Security and Resilience for Microsoft Dynamics 365:** Rubrik's enhanced protection for Microsoft Dynamics 365 aims to ensure businesses can secure their critical operational and customer data within a unified platform.
 - **Sandbox Seeding for Salesforce:** An intuitive user experience designed to allow users to select objects and records depending on specific criteria. This process aims to prevent seeding errors by thoroughly analyzing data

selection size versus destination size availability before moving data to the sandbox environment. The goal of this solution, planned for 2025, is to save queries for future repetitive use, further expediting the sandbox seeding process.

Rubrik Introduces Identity Recovery to Strengthen Cyber Resilience

Identity is one of the most critical vulnerabilities today with the majority of cyberattacks involving compromised credentials and fifty percent of businesses having experienced an Active Directory attack in the last two years. Without resilient identity services, organizations risk operational paralysis following a cyber incident.

With the introduction of Identity Recovery, Rubrik delivers the industry's most comprehensive, automated, and secure solution for protecting hybrid identity environments across Entra ID and Active Directory (AD). Identity Recovery includes orchestrated Active Directory Forest Recovery to rapidly and cleanly restore entire identity environments - eliminating manual complexity and reducing downtime.

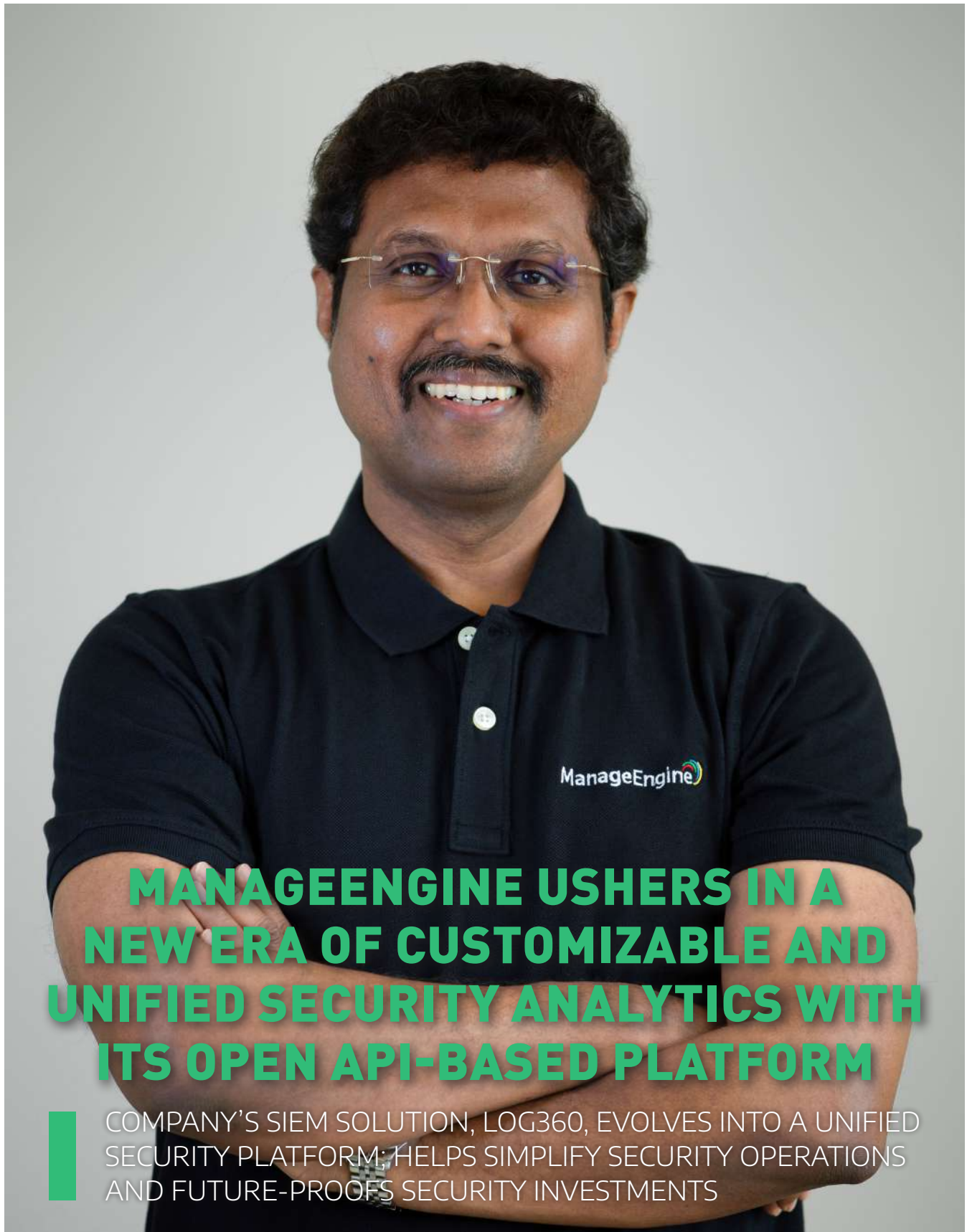
With Rubrik Identity Recovery, organizations can ensure fast, clean recovery of AD and Entra ID without reintroducing malware or misconfigurations, helping maintain business continuity and strengthen cyber resilience in the face of growing identity-based threats.

Rubrik continues to position its customers ahead of the curve for cyber resilience by delivering market-defining capabilities to help customers detect, mitigate and recover from cyber threats faster. The goal is to keep businesses running by minimizing operational disruptions.

- **Advanced Security Features for Azure & Amazon Web Services, Inc. (AWS):** Leveraging advanced machine learning and automation, new capabilities available today include Anomaly Detection, Data

Discovery and Classification, and soon, Threat Hunting and Threat Monitoring. These capabilities are designed to work together to proactively detect and mitigate cyber threats, accelerate recovery, and ensure sensitive data remains protected and compliant.

- **Orchestrated Recovery for Azure VM:** Rubrik is planning to extend its Orchestrated Recovery capabilities to the cloud beginning with Azure VM. By enabling customers to automate recovery sequences, schedule regular test recoveries, and generate comprehensive recovery reports, the solution is designed to reduce complexity and minimize the potential for human error.
- **Turbo Threat Hunting:** Unlike traditional methods that scan one object at a time or require navigating multiple panes of glass, Turbo Threat Hunting scans at scale by leveraging pre-computed hashes stored within Rubrik's metadata. This eliminates the need for file-by-file scanning, allowing organizations to rapidly pinpoint the exact recovery points free from malware or other threats within seconds — even in the most complex data environments. Internal testing found Turbo Threat Hunting scans 75,000 backups in less than 60 seconds.
- **Enterprise Edition for Microsoft 365:** Delivering enterprise-grade security and resilience for Microsoft 365, Rubrik expands its capabilities for organizations to rapidly detect, respond to, and recover from attacks. New capabilities available for Microsoft 365 include Sensitive Data Discovery, which identifies and protects high-risk data before an attack happens, and Prioritized Recovery, which restores critical data first for fast operational recovery. Coming soon, Rubrik's customers using Enterprise Edition for Microsoft 365 will also be able to add Anomaly Detection, Threat Monitoring, Threat Hunting, and Self-Service Recovery capabilities. 🔒



MANAGEENGINE USHERS IN A NEW ERA OF CUSTOMIZABLE AND UNIFIED SECURITY ANALYTICS WITH ITS OPEN API-BASED PLATFORM

COMPANY'S SIEM SOLUTION, LOG360, EVOLVES INTO A UNIFIED SECURITY PLATFORM; HELPS SIMPLIFY SECURITY OPERATIONS AND FUTURE-PROOFS SECURITY INVESTMENTS

M

anageEngine, a division of Zoho Corporation and a leading provider of enterprise IT

management solutions, announced the evolution of Log360—its unified security information and event management (SIEM) and IT compliance management solution—into an security analytics platform. The platformization of Log360, encompassing open APIs and a developer ecosystem, enables ManageEngine to address the critical need for adaptable, future-proof security. ManageEngine’s leadership believes this shift empowers enterprises, system integrators (SIs) and managed security service providers (MSSPs) to combat evolving threats on their own terms, turning SIEM from a cost center into a strategic asset.

Pricing and Availability

Log360 is available as both on-premises and cloud deployments. The cloud version, Log360 Cloud, is available in four editions—Basic, Standard, Professional, and MSSP. The Basic edition starts at \$300 per year with 75GB of default storage and 90-days search retention. The on-premises deployment starts at \$1,540.

Building the Platform on the Core Security Capabilities

Log360’s evolution into a robust security platform began last year

- Log360 transforms security operations from a cost center to a strategic asset
- Open APIs and community-driven innovation ensure rapid response to emerging threats while reducing total ownership costs
- Partnership forged with Sacumen, a specialist cybersecurity firm, to build connectors

with key enhancements, laying the foundation for future innovation. These enhancements included proactive threat intelligence through dark web monitoring powered by Constella Intelligence, investigation triad capabilities for faster alert analysis via enriched security events and an enhanced correlation engine for complex threat detection.

“A platform isn’t defined by just what it does today, but by what it enables tomorrow. With Log360 evolving as a platform, we’re empowering customers and partners to innovate on top of our foundation, whether integrating cutting-edge AI models or niche compliance frameworks. This ecosystem-driven approach turns security from a cost center into a strategic enabler,” says Manikandan Thangaraj, vice president at ManageEngine.

Key Highlights of ManageEngine’s Unified Security Platform


- **Unified visibility, zero complexity:** Make it easier for teams to identify, investigate and respond to threats. Log360 facilitates the consolidation of disparate security data into a single, unified view, eliminating the need to juggle multiple tools and dashboards.
- **Customizations at scale:** Enable customizations at scale through API-driven integrations that empower MSSPs, SIs and enterprises to address unique challenges, optimize their security workflows and go beyond standard roadmaps.
- **Accelerated innovation:** Enable swift integration of AI, machine learning, and other advanced technologies with the platform architecture. This not only keeps Log360 at the forefront of security but also ensures enterprises benefit from the swift adoption of latest advancements in threat detection and response.
- **A perfect sharing ecosystem:**

Facilitate industry-specific threat intelligence sharing, enabling smaller teams to benefit from the collective knowledge of the community. ManageEngine’s Marketplace democratizes access to valuable expertise and improves incident response effectiveness by making extensions and data connectors publicly available.

- **Compliance agility:** Leverage Log360’s developer ecosystem to enable rapid updates, addressing new regulations and revisions to existing mandates as they arise. This eliminates the delays associated with traditional vendor upgrades.

Partnership Forged with Sacumen

Looking ahead, ManageEngine will expand Log360’s platform capabilities by growing its partner and developer ecosystem with industry-specific extensions, integrating advanced AI and ML tools for predictive security and fostering community-driven security innovation. As an initial step towards this direction, ManageEngine has entered into a partnership with Sacumen, a firm specializing in the development of cybersecurity product engineering and services.

“Our partnership with ManageEngine reflects our shared vision: empowering enterprises with comprehensive and integrated security solutions. Sacumen’s contribution lies in building the crucial bridges—the connectors—that allow Log360 to seamlessly interact with the broader security ecosystem, maximizing its value for customers,” says Nitesh Sinha, CEO and founder of Sacumen. “ManageEngine’s platform approach coupled with Sacumen’s expertise in connector development breaks down the data silos, providing unified visibility and streamlined integration, empowering enterprises to move beyond reactive security and embrace a proactive, data-driven defense.” 

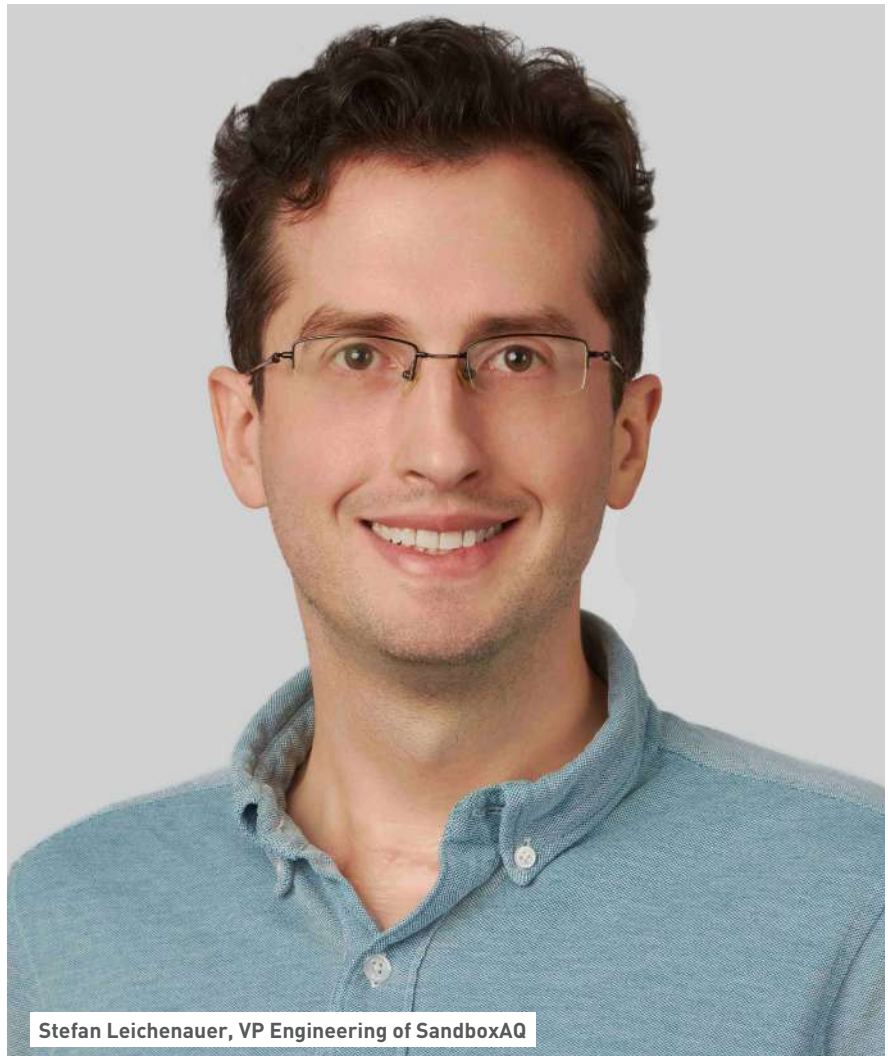
SANDBOXAQ JOINS UNITED NATIONS INTERNATIONAL COMPUTING CENTRE'S AI HUB AS A FOUNDING MEMBER

INITIAL COLLABORATIONS WILL FOCUS ON CRYPTOGRAPHIC DISCOVERY TO STRENGTHEN THE UN'S CYBERSECURITY POSTURE, WITH FUTURE PROJECTS FOCUSED ON DEPLOYING LARGE QUANTITATIVE MODELS TO ADDRESS GLOBAL CHALLENGES FACING UNICC PARTNERS

SandboxAQ has joined the United Nations International Computing Centre (UNICC) as a founding member of its new AI Hub, which has been established to be the primary AI solutions provider and resource center for more than 100 UN entities and other international organizations around the globe.

The UNICC is the largest strategic partner for digital solutions and cybersecurity within the United Nations system. Leveraging SandboxAQ's AQtive Guard unified encryption management platform, the UNICC will begin offering AI-enhanced cryptographic discovery services to identify any vulnerable cryptography (e.g., outdated or expired algorithms, keys and certificates) throughout a member organization's entire IT infrastructure, including applications, networks, and filesystems. These insights will enable constituents and partners to upgrade their cryptography to meet emerging and future threats, including AI- and quantum-based attacks.

"Over the last five decades, UNICC has continually expanded the diverse technology services designed for the UN family, including fostering strategic



Stefan Leichenauer, VP Engineering of SandboxAQ



partnerships with trusted partners like SandboxAQ to develop state-of-the-art solutions,” said Sameer Chauhan, Director, UNICC. “Leveraging SandboxAQ’s innovative quantum, AI and cybersecurity solutions, we’re pleased to welcome them as a founding member of the UNICC AI Hub and share their expertise with our partners.”

The UNICC AI Hub’s Focus and Mission

The new UNICC AI Hub will serve as a center of excellence for AI deployment within the UN system and other international organizations, gathering best-in-class experts, partners,

knowledge, solutions and capabilities to help constituents and partners accelerate positive impact around the world. The AI Hub will provide expertise and training on a broad range of predictive, generative and quantitative AI solutions that are UN-tailored, battle-tested, cost-effective, secure and compliant. The AI Hub and members such as SandboxAQ will assist with setting up and scaling AI projects, ensuring robust data integrity, ethical compliance, optimal model performance, and measurable results.

In addition to cybersecurity services and solutions, SandboxAQ will collaborate with the UNICC to roll-out additional

quantitative AI solutions powered by Large Quantitative Models (LQMs). These solutions will drive breakthroughs in complex system modeling, post-quantum cryptography, predictive analysis, and other areas related to the Sustainable Development Goals, such as clean water, good health and wellbeing, climate action, and affordable clean energy.

“As AI continues to fundamentally transform all aspects of our daily lives and the global digital economy, we applaud the UNICC’s bold step to create a one-stop shop where all UN agencies and affiliates can find the AI expertise, resources and solutions they need to protect themselves from cyber attacks and affect positive change on a global scale,” said Stefan Leichenauer, VP Engineering of SandboxAQ. “SandboxAQ is incredibly proud to be a founding member of the UNICC’s AI Hub, and we look forward to helping its members tackle some of society’s biggest challenges.”

→ **“SANDBOXAQ IS INCREDIBLY PROUD TO BE A FOUNDING MEMBER OF THE UNICC’S AI HUB, AND WE LOOK FORWARD TO HELPING ITS MEMBERS TACKLE SOME OF SOCIETY’S BIGGEST CHALLENGES”**



VISA LAUNCHES TAP TO ADD CARD IN SAUDI ARABIA, ENHANCING THE EASE AND SECURITY OF ADDING CARDS TO DIGITAL WALLETS

Visa announced the launch of Tap to Add Card in Saudi Arabia marking a significant advancement in digital wallet provisioning. This innovative technology addresses the growing need for secure and streamlined digital payment solutions by allowing cardholders to add their Visa contactless cards to digital wallets with a simple tap on their mobile device.

Bringing enhanced security and convenience, Tap to Add Card eliminates the cumbersome process of manual entry, a common source of errors and a vulnerability exploited by fraudsters seeking to compromise sensitive card information. The tap generates a unique, one-time code validated by Visa's Chip Authenticate service, ensuring secure provisioning of card credentials and offering a significantly faster and more secure alternative to traditional methods.

"We are excited to bring the enhanced security and simplicity of Tap to Add Card to Saudi Arabia," said Ali Bailoun,

Regional General Manager for Saudi Arabia, Bahrain and Oman at Visa. "The solution provides cardholders with greater peace of mind when adding a card to a digital wallet, knowing their information is protected by advanced security measures. We believe that Tap to Add Card will be instrumental in driving further adoption of digital wallets in the Kingdom by addressing key security concerns and simplifying the user experience."

Global Momentum and Regional Impact

Tap to Add Card feature has quickly gained traction worldwide since its introduction last September by Visa, as part of its suite of new services aimed at enhancing digital payment experiences. With over 80,000 Tap to Add Card tokens enabled in Saudi Arabia the technology has demonstrated its ability to streamline and secure digital wallet provisioning.

Benefits for the Ecosystem

Tap to Add Card is designed to benefit all

stakeholders in the payments ecosystem. Offering an experience similar to in-store payments, cardholders can enjoy a faster, more convenient, and more secure way to add cards to their digital wallets, encouraging greater adoption of digital payments.

For issuers, Tap to Add Card can help reduce the risk and associated costs of provisioning fraud, simplifies the add-to-wallet process leading to fewer customer service inquiries, and improves transaction approval rates.

Similarly, for digital wallets, Tap to Add Card follows Visa security standards, reducing the risk of card compromise and promising a potentially higher token provisioning rate due to fewer card entry errors, while also presenting the opportunity to introduce new customer experiences.

The technology is supported by digital wallets globally, ensuring seamless integration with existing digital wallet experiences. 📱



معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC

GLOBAL

06 - 08 MAY 2025
DUBAI WORLD TRADE CENTRE

HOSTED BY



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER



OFFICIALLY SUPPORTED BY



شرطة دبي
DUBAI POLICE



MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE



ENQUIRE FOR 2025!

OFFICIAL DISTRIBUTION PARTNER



LEAD STRATEGIC PARTNER



STRATEGIC PARTNERS



PLATINUM SPONSORS



GOLD SPONSORS



CTF PARTNER



BRONZE SPONSORS



CONTACT US

✉ gisec@dwtc.com

☎ +971 4 308 6469

🌐 cyber.gisec.ae

📱 #gisecglobal



IDEMIA PUBLIC SECURITY, TAHAKOM EXPAND PARTNERSHIP TO REINFORCE LOCAL SOURCING, INNOVATION TO ENHANCE ROAD SAFETY IN SAUDI ARABIA

IDEMIA AND TAHAKOM TO COLLABORATE ON LOCAL SOURCING FOR ASSEMBLY OF PRODUCTS AND LEVERAGE THEIR AI AND RESEARCH AND DEVELOPMENT CAPABILITIES.



(L) Mazen Hamadallah, SVP, Road Safety, IDEMIA Public Security.

DEMIA Public Security, the leading provider of secure and trusted biometric-based solutions, and Tahakom, the Saudi Technology and Security Comprehensive Control Company, are expanding their strategic partnership through the signing of an extensive agreement to develop and implement local sourcing and foster continued innovation to ensure safer roads in the Kingdom.

The new agreement marks a turning point in enhancing road safety in the Kingdom and moving a step closer to Saudi Vision 2030, which includes a significant focus on improving road safety, but also on making the country a global investment powerhouse through the development of local activities.

IDEMIA and Tahakom's expanded collaboration aims to develop and implement local initiatives focused on sourcing, assembling, and servicing, in addition to leveraging each other's expertise and capabilities within AI and research and development.

The signed agreement focuses on three core subjects:

- **Assembly:** With Tahakom's commitment to local sourcing, IDEMIA will source components and services for their products from Saudi Arabia. In support of this, IDEMIA will establish a new entity, IDEMIA Road Safety Limited – Saudi Arabia, which will be specialized in assembling Road Safety products in Saudi Arabia and reinforce the use of local content by engaging with local suppliers and partners in the Kingdom whenever possible.
- **Artificial Intelligence and Research & Development (R&D):** IDEMIA's R&D Team and Tahakom's AI team will set up multiple workshops throughout the year to collaborate and share ideas surrounding AI and R&D advancements.
- **Transfer of Knowledge:** IDEMIA and Tahakom will focus on bringing experts around the globe to set up sessions around IDEMIA's products and technologies and openly conduct and offer these sessions to Saudi Arabian citizens.

"We are thrilled to expand our partnership with Tahakom and support their commitment to local sourcing in Saudi Arabia," shared Mazen Hamadallah, SVP, Road Safety, IDEMIA Public Security. "Together we continue to develop and implement initiatives that will drive maximum benefit and impact on our communities, while enhancing operational efficiency and sustainability. This agreement is not only a testament to Tahakom and IDEMIA's dedication to ensure safer roads in the Kingdom, but also to our commitment to leveraging local expertise and resources and aligning to the Saudi Vision 2030 set by the Kingdom."

As IDEMIA and Tahakom work closely together on this new initiative, they aim to set up a program to improve local content while working on product localization, strengthening the local workforce, and sharing knowledge and research on local content. They will also be exploring other potential areas to expand into in the future. 📌

NDF, ENDAVA AND GOOGLE CLOUD HOST LANDMARK DATATHON IN RIYADH

FIRST-OF-ITS-KIND EVENT BRINGS TOGETHER TOP TALENT TO DRIVE DATA-DRIVEN INNOVATION



Andrew Rossiter, Global SVP & Google Cloud Unit Lead at Endava.

Endava, a global leader in digital transformation, hosted a datathon in Riyadh in collaboration with the National Development Fund (NDF) and Google Cloud in Saudi Arabia. The event brought together data scientists, engineers and industry experts to tackle real-world challenges through data-driven innovation.

The datathon served as a collaborative platform for participants to harness the power of data and technology to develop solutions that align with Saudi Arabia's Vision 2030 goals. By leveraging cutting-edge tools and methodologies, teams worked on key challenges across finance, sustainability, and digital infrastructure, showcasing the potential of data analytics and artificial intelligence in shaping the future.

Andrew Rossiter, Global SVP &

Google Cloud Unit Lead at Endava, said: "Data is at the heart of today's AI-driven digital transformation, and this event underscores our commitment to fostering innovation in Saudi Arabia. By bringing together the best minds from Endava, NDF and Google Cloud, we have created a unique environment for ideation and problem-solving, accelerating the Kingdom's journey toward a data-driven economy."

Ahmed Bawareth, Service Excellence Office Sr. Executive Director at NDF, emphasised that organising this datathon reflects the Fund's commitment to fostering digital innovation and empowering local talent. He highlighted that leveraging big data and artificial intelligence to develop practical technological solutions is a fundamental pillar in achieving sustainable development and driving digital transformation in the Kingdom.

This initiative aligns with the Fund's strategy to enhance collaboration among development entities and harness advanced technologies to create solutions that support the digital economy and contribute to the objectives of Saudi Vision 2030.

Throughout the event, participants had access to mentorship from industry leaders, hands-on workshops, and the latest tools from Google Cloud and its AI ecosystem. The winning teams presented innovative solutions with the potential to be further developed and implemented within strategic initiatives across the Kingdom.

The datathon marks the beginning of deeper collaboration between Endava, NDF and Google Cloud in Saudi Arabia, with future initiatives aimed at accelerating digital transformation and fostering a thriving tech ecosystem. 📌

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



UNDER THE AUTHORITY OF



IN PARTNERSHIP WITH

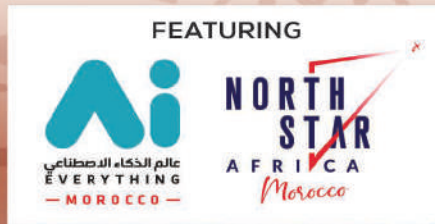


ORGANISED BY



14 - 16 APRIL 2025 MARRAKECH

Defining Africa's Future with AI Impact



**AFRICA'S LARGEST TECH AND
STARTUP EVENT JUST GOT BIGGER**

45,000

ATTENDEES

1,500

EXHIBITING & STARTUP
COMPANIES

650+

GOVERNMENT REPRESENTATIVES

130+

COUNTRIES REPRESENTED

435

MEDIA ATTENDEES

660+

SPEAKERS

**FEATURING THE LATEST
SOLUTIONS & THOUGHT LEADERSHIP:**

- AI EVERYTHING
Cloud x IOT x AI
- Cybersecurity
- Telecom / Network
Infrastructure
- Digital Cities
- Future Banking and
Finance
- GITEX Digi Health
- GITEX Agritech &
Food Security **NEW**
- GITEX EdTech **NEW**
- Sports Tech **NEW**
- Sustainability
- Mobility
- Consumer Tech
- Startups



GET YOUR
TICKETS TO VISIT



LAST CHANCE
TO EXHIBIT

in X f @ /gitexafrica

AI AND RANSOMWARE: CUTTING THROUGH THE HYPE



Rick Vanover, Vice President Product Strategy, Veeam

It might be the great paradox: Artificial Intelligence (AI). Everyone's bored of hearing it, but can't stop talking about it. It's not going away so we had better get used to it. AI is disrupting most digital industries and cybercrime is no exception.

However, cutting through the hype and getting to the facts is worth it. Much has been made of AI's potential impact on the global ransomware threat, but how much does it really change the picture?

AI-Cops and AI-Robbers

While the future potential of AI, on cybercrime and society in general, is immense (and a little scary), it's more helpful to focus on the here and now. Currently, AI is just another tool at threat actors' disposal, but it is quite a significant one because it lowers the barrier to entry for criminals.

Using AI to assist with coding is already common among legitimate programmers. Even if it's just reviewing broken code or answering specific questions faster than Google, AI will support people hacking systems just as much as those developing them. But while this might make ransomware gangs' lives easier, it won't make things any worse for security teams. The result hasn't changed; depending on who you ask, the end product might even be worse.

However, the other current use cases are more consequential. AI algorithms can scan networks or environments to map architecture and endpoints and, crucially, spot vulnerabilities. Threat actors will already do this manually, but AI will make it much easier and more effective. AI can also be used to automate information gathering for more targeted attacks. These tools can scrap the internet (particularly social media) to collect as

much information on a target as possible for phishing and social engineering.

This brings us to the last typical use of AI by cybercriminals. In a conversation where the hype is aplenty, describing AI as 'supporting phishing' is probably underselling it. At its most basic, even the most readily available AI tools can be used to craft better phishing emails - bridging the language barrier that often makes such scams spottable. That's another example of AI improving malicious activity that already exists, but the voice cloning (deepfakes) of specific people is another entirely different thing. When combined with automated information gathering on a target, we're looking at the next generation of social engineering.

What it means for security

While cybercriminals having more tools at their disposal is never going to feel great, there are two things to bear in mind: one, security teams have access to these tools as well, and two, AI is going to make attacks more sophisticated and effective. For now, it isn't introducing any brand-new or entirely novel threats, so there's no need to tear up the playbook.

AI is already used on both sides of the battle line. It's probably fair to say that while ransomware gangs have access to their dark marketplaces of solutions and services, we 'normies' have access to far more. The 'ransomware industry' was valued at (a still massive) \$14 billion as of 2022, but the global security industry makes this look tiny compared to its \$222 billion.

On the security side, AI can be used for behavioural analytics, threat detection and vulnerability scanning to detect malicious activities and risks. AI can be employed to monitor both the system itself (scanning for vulnerabilities and entry points) and activity on the system (behavioural

analytics, data analysis, etc.). AI-enabled security aims to predict and catch threats before they turn into breaches. More advanced tools will automatically respond to these threats, alerting security teams or restricting access. Much like on the criminal side, most of these concepts exist now (such as firewalls and malware detectors), but AI is making them more efficient and effective.

You can't beat basic principles

So, even though AI will be used on both sides, it's not a case of getting AIs to battle each other in the cyber realm (although that does sound cool.) Ransomware isn't changing (for now, at least), and attackers' tactics aren't transforming. Digital hygiene and zero trust all still work. Security will need to keep up, sure. After all, social engineering only needs to work once, but ransomware prevention and resilience need to work every time.

Ultimately, the best practice remains the best practice. As AI-enabled ransomware becomes more common, having copies of your data becomes more critical than ever. When all else fails - you need backup and recovery. All of these scary scenarios, even the most advanced phishing attack known to man (or machine), could all end up with - 'thank god I had trusted backup and recovery'.

As backup is your last line of defence; you must know you can rely on it. Again, the best practice hasn't changed here. You need multiple copies of your data, one offline and one off-site. You also need a well-rehearsed recovery strategy, including scanning backups for infection and setting up a recovery environment that is ready to rock.

It's less daunting than it seems. AI isn't changing the game - it's just a natural progression. Progression is the game's name in cybersecurity - you can't do everything, but you should do something. The basic principles still get you pretty far, so keep following those, keep up to date on best practices, and make sure you can trust your backup when all else fails. 📌

AI CAN BE USED FOR BEHAVIOURAL ANALYTICS, THREAT DETECTION AND VULNERABILITY SCANNING TO DETECT MALICIOUS ACTIVITIES AND RISKS.



Andre Troskie, EMEA Field CISO at Veeam

GOODBYE CISO SCAPEGOATING - THE AGE OF CORPORATE ACCOUNTABILITY IS HERE

Responsibility for cybersecurity and data resilience can no longer be placed on the shoulders of CISOs alone. New EU regulations like NIS2 and DORA bring corporate accountability to the foreground, holding the wider corporate leadership team responsible. Collectively, boards need to be educated on cyber threats as they face being held accountable for any cybersecurity incidents that occur under their watch - and can now be fined individually alongside the wider organization in the case of non-compliance.

Despite this, awareness of corporate accountability is still too low. That's not to say that there's not been buy-in, but C-levels aren't moving fast enough. And it's no use being aware of a concept if you don't take action. 95% of EMEA organizations alone have siphoned budgets from other resource pots to reach compliance. So, the urgency is there, but C-suite action is yet to catch up. What do they need to change to get up to speed?

Shifting priorities

NIS2 and DORA have ushered in a new era of corporate accountability, enshrining it in regulation on a level never seen before in cybersecurity. And for good reason. Over the last couple of decades, practically every business function has become digital, creating an exponentially growing source of data for organizations to manage and, more importantly, protect. Cybersecurity has become a vital business outcome, making it just as important as any commercial aspect, so naturally, it should sit under the purview of the C-suite.

These regulations simply formalize what should have been occurring within organizations. For

many, however, cybersecurity and resilience was still being sidelined. Understandably, the C-suite has historically left cybersecurity in the hands of the security teams. Admittedly its business value can be hard to see at times. Being more resilient and able to recover faster will minimize the damage organizations face, across share prices, revenue, and customer trust. As C-suites are educated further on the topic thanks to these regulations, these long-term benefits should help adjust priorities - alongside the added pressure of non-compliance!

While these pressures have improved the rates of C-suite buy-ins to corporate accountability, hands-on involvement is still not at the necessary levels. The vast majority of EMEA organizations siphoned budgets from other sources to meet NIS2 compliance, so while they understand the need for compliance, C-suites still lack a joined-up strategy to reach it. Sure, part of this can be chalked up to the immense learning curve that many C-suite executives are facing. Cybersecurity is no small task. To understand it properly, they'll need to get stuck in at the deep end.

Taking the leap

Getting first-person experience of your organization's incident response plans is essential for executives seeking to truly understand their responsibilities in this new age of corporate accountability. The same regulations that demand this also call for consistent compliance, not a one-and-done tick box. C-levels will need to be able to demonstrate that their organization's incident response plans work in the real world, with consistent and rigorous scenario testing. It's not something that executives can memorize and recite when the occasion arises, they need to live and breathe it.

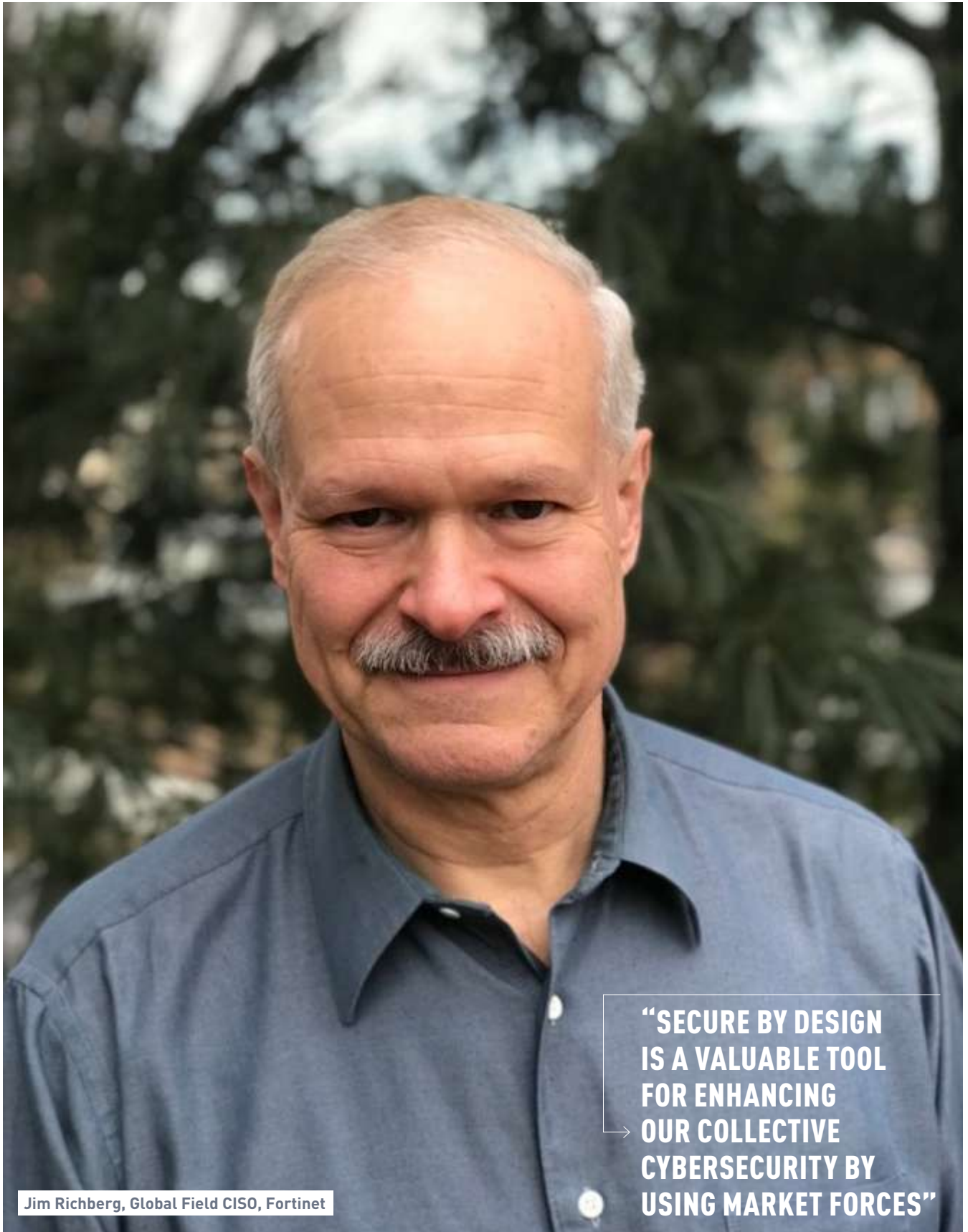
These regulations don't call for executives to become experts on cybersecurity by any means. The core thing that C-suites need to know inside and out, are their incident response plans. Take physical security safety as an example. As a C-suite, you wouldn't need to know the ins and outs of your fire alarm systems, you just need to know they're there, that they function, and who is in charge of maintaining them. It's not their responsibility to be the fire safety expert, simply to know who is, who the backups are, and to ensure that the necessary drills are taking place to adequately prepare.

Cybersecurity incident response plans follow a similar philosophy, and both NIS2 and DORA compliance hinges on their robustness, and that's where C-suites need to focus their efforts. With a practical understanding of these plans, executives can identify and address their weak spots, whether that be with new processes or by bringing in new, external skills into their workforce.

Forward-thinking

Just as these regulations call for consistent compliance and frequent scenario-based stress testing of plans - so does the cybersecurity landscape. Vulnerabilities and attack surfaces change every day, and plans need to be able to keep up. Using the demands of these regulations as an opportunity not just to tick a box, but to develop a truly security-aware and data-resilient culture is an opportunity that executives can't afford to miss.

You can be as compliant as possible but it's impossible to become 100% secure. Without data resilience and safeguards like back-ups in place, C-suites won't be able to recover following a breach - no matter how compliant they are. 📌



**“SECURE BY DESIGN
IS A VALUABLE TOOL
FOR ENHANCING
→ OUR COLLECTIVE
CYBERSECURITY BY
USING MARKET FORCES”**

Jim Richberg, Global Field CISO, Fortinet

SECURE BY DESIGN: A CONTINUED PRIORITY IN 2025 AND BEYOND

Enhancing cyber resilience has long been a shared responsibility. Entities across public and private sector organizations, from government to academia to end-users, all play a critical role in protecting our collective digital infrastructure.

Yet, as the threat landscape grows more complex while organizations of all sizes adopt new technologies at an unprecedented rate, technology vendors are uniquely responsible for delivering secure products and systems.

A Crucial Tool for Advancing Cybersecurity for All

Secure by design is a foundational approach to product development that vendors must embrace, ensuring that security is a foundational component of the design and development process instead of being applied as an afterthought.

The Cybersecurity and Infrastructure Security Agency (CISA) introduced this concept as part of its work to implement the 2023 U.S. National Cybersecurity Strategy. The national strategy recognized the need for a fundamental shift in how the United States should allocate cyberspace roles, responsibilities, and resources. It highlighted the need to “rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, local governments, and infrastructure operators, and onto the organizations that are most capable and best positioned to reduce risks for all of us.” Technology vendors must take ownership of customer security outcomes and embrace radical transparency and accountability.

While some technology providers, including Fortinet, have applied these

principles to their product development processes for decades, secure by design remains an important but underappreciated tool for improving cybersecurity.

Today, secure by design must remain a priority for our industry. Even as political landscapes shift, advancing our collective cyber resilience benefits everyone.

CISA’s Secure by Design Pledge Sparks Momentum Across the Industry

Since the inception of the secure-by-design philosophy, CISA has introduced several initiatives to encourage the adoption of these principles, one of which is the Secure by Design Pledge. This pledge is voluntary for organizations committed to upholding key secure-by-design development practices for enterprise software. I was pleased to be one of the leaders in the extensive collaboration with CISA to develop its secure-by-design principles and pledge. Last month, I was honored to join CISA and receive the Institute for Security and Technology’s 2025 Cyber Policy Award in the U.S. Domestic Policy Impact category for our efforts in creating the Secure by Design Pledge.

The pledge was introduced in May 2024, with 68 companies initially signing. By the end of last year, that number had jumped to more than 250 signatories. This positive reception to the pledge marked an important step forward in the dynamics of the cybersecurity marketplace. The pledge made the abstract concept of secure by design usable by offering software companies a roadmap to enhance product security and a guide for customers to use during the procurement process.

Secure by Design Is an “On Ramp” to Stronger Cyber Resilience

While developing the pledge, CISA and its industry collaborators agreed that this

would be an “all or nothing” undertaking rather than one that allowed vendors to choose which goals to pursue. When desired outcomes are straightforward, the pledge could be designed to offer signatories the freedom to tackle the goals as they saw fit instead of prescribing a specific path. We also knew that the goals should generate measurable outcomes and readily understandable measures of progress that vendors could share with prospects and customers.

As a result, the pledge is envisioned as an “on-ramp” for technology vendors to use to enhance their customers’ security, offering a meaningful and flexible guide for implementing secure-by-design practices. The pledge and its goals also give purchasers a much-needed resource to examine vendor and product cybersecurity during procurement. Technology buyers can use the pledge as a starting point by asking vendors whose products they are considering whether they’ve taken the pledge and, if so, what they can share about implementing its principles.

What’s Next for Secure by Design

Secure by design is a valuable tool for enhancing our collective cybersecurity by using market forces. While it’s encouraging that many vendors have embraced these principles, more work is required. Technology buyers must also demand that their vendors embrace secure by design and that they share their progress in meeting pledge goals.

As a company, we look forward to continuing to work with our partners in both the public and private sectors to advance the secure-by-design philosophy. Together, we will build a safer and more resilient digital future for all. 🔒



Sally Adam, Senior Director, Solution Marketing at Sophos.

MDR USERS CLAIM 97.5% LESS IN CYBER INSURANCE THAN ENDPOINT-ONLY USERS: SOPHOS STUDY

THE AVERAGE CLAIM FOLLOWING A SIGNIFICANT CYBERATTACK IS JUST \$75,000 FOR MDR USERS, COMPARED WITH \$3 MILLION FOR ENDPOINT-ONLY USERS.

Sophos, a leading global provider of innovative security solutions designed to neutralise cyberattacks, has unveiled the results of a new independent study to quantify the financial impact of various cyber security controls on cyber insurance claims. The study reveals the different impact that endpoint solutions, EDR/XDR technologies and MDR services have on claims resulting from an attack, providing valuable insights for insurers and organisations.

Sally Adam, Senior Director, Solution Marketing at Sophos, said: 'Every year, organisations spend huge amounts of money on their cybersecurity. By quantifying the impact of controls on the outcome of cyberattacks, this study enables them to focus their investments on the most cost-effective options. At the same time, insurers have a major influence on cybersecurity spending through the controls they require of organisations wishing to be covered and the discounts they offer when a given scheme is in place. This study enables them to encourage investments that can make a real difference to incident outcomes and the resulting claim amounts.'

The study reveals that the average (median) amount of compensation claimed by organisations using MDR services is 97.5% lower than that of organisations using endpoint solutions. The median claim for MDR services users is just \$75,000, compared with \$3 million for organizations using endpoint security alone. In other words, when they are the victims of an attack, endpoint-only users' generally claim 40 times more than MDR service users. The lower claims of MDR customers are likely due to the ability of MDR services to quickly detect and block malicious activity, and repel attackers before they can cause serious damage.

There is also an advantage to using an EDR or XDR tool alongside an endpoint solution. The average claim for users of



EDR/XDR tools is only one-sixth of that for users of endpoint solutions (\$500,000 versus \$3 million).

MDR users have the most predictable claims

The predictability of claims is a key indicator of the consistency and reliability of cybersecurity controls in reducing the impact of cyberattacks. The study reveals that claims from users of MDR services are the most predictable, while those from users of EDR/XDR tools are the least predictable.

These results reflect the consistency and speed with which MDR providers detect and neutralise threats. By providing 24/7 monitoring, investigation and response by security experts, MDR services enable organisations to act quickly at any time of the day or night.

In contrast, the unpredictability of claims from users of EDR/XDR tools demonstrates that the ability of these technologies to effectively stop cyberattacks before major damage is done depends entirely on the skills and responsiveness of users.

MDR users have the most predictable recovery time after a ransomware incident

Recovery times vary depending on the solution used by organisations: users of endpoint solutions are positioned 'in the middle of the table', with an expected recovery time of 40 days. Users of EDR/XDR tools are the slowest to recover, with an expected recovery time of 55 days.

MDR service users are the fastest to recover from a ransomware incident, with an expected recovery time of just three days. These results demonstrate the ability of an MDR service to significantly reduce the impact of cyberattacks on organisations. They also reveal the highly unpredictable recovery times experienced by users of EDR/XDR tools. Nevertheless, it's important to remember that EDR/XDR solutions are tools and, as such, their effectiveness and impact depend on how they are used.


Adam concludes: 'The research confirms what many people instinctively know: the type of security solution used has a significant impact on

cyber insurance claims. Cyberattacks are inevitable, but defences are not. These results are a useful tool for organisations wishing to optimise their cyber defence and their return on investment in cybersecurity. They will also be useful for insurers looking to reduce their exposure and offer suitable policies to their customers.'

About the survey

The survey was conducted by Vanson Bourne on behalf of Sophos during the second half of 2024. It looked at claims resulting from cyberattacks that had occurred in the previous 12 months.

Specifically, the study was conducted on 282 claims reported by 232 organisations with between 50 and 3,000 employees. Respondents used cybersecurity solutions from a wide range of vendors, including 19 endpoint protection vendors and 14 MDR vendors. All organisations were using Multi-Factor Authentication (MFA) at the time of the cyber-attacks that led to the claims.

All results were subject to rigorous and robust statistical validation using multivariate regression models. 



Ryan Windham, CEO of Forcepoint

FORCEPOINT TO ACQUIRE GETVISIBILITY, EXPANDING AI-DRIVEN DATA SECURITY AND RISK VISIBILITY

Global data security leader Forcepoint has signed a definitive agreement to acquire Getvisibility, an innovator in AI-powered Data Security Posture Management (DSPM) and Data Detection and Response (DDR).

Forcepoint's Data Security Everywhere platform unifies visibility and control over sensitive data, while Getvisibility enhances the user's ability to identify and mitigate data risk. The acquisition tightens the synergy to simplify security management, enhance risk mitigation and speed compliance for enterprise and government customers.

The agreement builds on a successful multi-year partnership, further integrating Getvisibility's AI-driven risk visibility and remediation within Forcepoint's full-lifecycle data security solutions. By strengthening interoperability between Getvisibility's DSPM and DDR capabilities and the Data Security Everywhere architecture, Forcepoint enables seamless discovery, classification, prioritization, remediation and protection of sensitive data—including PII, intellectual property and other critical assets—across modern hybrid and AI environments.

For more than two years, Getvisibility's DSPM and AI-mesh technology—a coordinated network of specialized AI models designed to improve accuracy and speed in data classification and risk detection—has been a core component in Forcepoint's data security approach. Using Getvisibility technology, customers and partners gain superior visibility and insights into data risks such as redundant and obsolete data, improper access, misplaced files and regulatory exposure.

Getvisibility's DDR capabilities, with integrated AI, automate classification and enable dynamic remediation to mitigate threats before they escalate. This acquisition expands that integration, delivering comprehensive security that continuously adapts to how users'

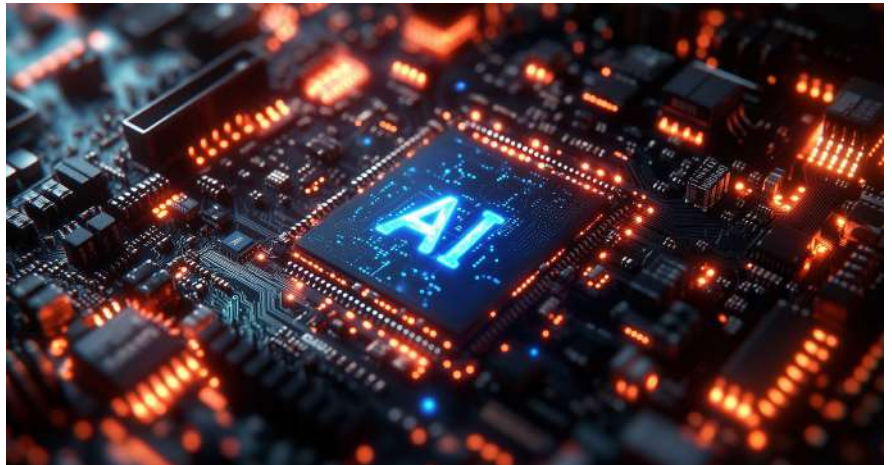
access, share and interact with data across devices, cloud applications and GenAI platforms.

“Data is the new currency of business, and every organization is racing to unlock its value while minimizing risk,” said Ryan Windham, CEO of Forcepoint. “By further integrating Getvisibility’s AI-driven DSPM and DDR into our portfolio, Forcepoint is equipping enterprises and governments with the visibility, automation and adaptive controls needed to transform data security from a compliance obligation into a strategic advantage. This acquisition reinforces our commitment to helping organizations protect sensitive data at scale, while turning security into a driver of growth and innovation.”

Managing data risk is critical for every organization’s success. All businesses are dependent on data which is crucial for accurate insights, decision-making, driving innovation and gaining a competitive edge. Loss of proprietary and sensitive data results in more than regulatory fines and remediation costs, today averaging \$5 million per data breach. With the fast-rising tide of class action suits, industry insiders predict that breach-related class action costs will exceed regulatory fines by 50 percent in 2025. The stakes for mitigating data vulnerability and risk have never been higher.

“With data surging throughout the cloud, and GenAI systems increasing the

- Acquisition will strengthen Forcepoint’s leadership in data security, transforming data risk into proactive protection with AI-powered visibility and continuous controls
- Getvisibility’s DSPM, DDR and AI-Mesh technology will integrate seamlessly into Forcepoint’s Data Security Everywhere architecture, advancing real-time risk detection, automated response and compliance enforcement



risk that sensitive information will get exposed, organizations are struggling to know where their data actually is, how it’s being used, what the sensitivity of the data is, and how to protect it,” said Frank Dickson, Group Vice President for Cybersecurity Products at IDC. “They are tired of cobbling together siloed products and now are looking for new, integrated approaches that unify visibility and control so that they can reduce the complexity, cost, and risk of innovating.”

Enhancing Data Security with AI for AI and Emerging Technologies

Forcepoint’s Data Security Everywhere approach unifies security policies across AI websites, endpoints, email, SaaS applications and custom environments. With Getvisibility’s DSPM and DDR capabilities even more deeply integrated, organizations will gain:

- **Proactive risk visibility:** Continuous discovery and classification of sensitive data across SaaS, cloud, and on-premises environments
- **Real-time threat mitigation:** Automated enforcement of security policies across CASB, Web Security and Enterprise DLP
- **Adaptive security controls:** Policy enforcement that uses the intelligence of AI to dynamically protect sensitive data across AI platforms (e.g., ChatGPT Enterprise, Copilot, Gemini) and enterprise applications

Ronan Murphy, Co-founder of Getvisibility, added: “From day one, our mission has been to help organizations understand their data risks—because you can’t secure what you don’t see. Real-time risk mitigation is key to preventing breaches before they happen. By joining forces with data security’s original architects, Forcepoint, we’re amplifying our AI-powered insights to help customers and partners pinpoint risk, protecting critical data assets with accuracy and speed that redefine industry standards.”

With this acquisition, Forcepoint is redefining data security in the AI era—enabling organizations to secure their most critical assets, ensure compliance and stay ahead of modern cyber threats. Further details on the integration of Getvisibility within Forcepoint’s Data Security Everywhere portfolio will be announced later this year following completion of the acquisition.

“We couldn’t be more excited to formally unite with Forcepoint and bring our teams into such a successful company to form a formidable force in data security,” said Mark Brosnan, Co-founder of Getvisibility. “By joining Forcepoint, we’re amplifying our AI-driven risk mitigation capabilities and accelerating innovation, ensuring customers have the most advanced solutions to protect their most critical data assets.” 



Zayan Sadek, Managing Director for Service Providers MEA at Cisco

CISCO UNVEILS SIGNIFICANT UPGRADES TO MOBILITY SERVICES PLATFORM

Cisco has introduced new functionalities of the Mobility Services Platform. Built and deployed globally, delivered as-a-service, and with an extensive API ecosystem, it's open to developers, Communication Service Providers, and enterprises to create new, differentiated value from the network, from traditional IoT and voice services to emerging AI-based services for people, spaces, and intelligent machines.

This platform has been applied across high-value use cases for people, places,

things, and fast-evolving intelligent machines. The value of the platform has been recognized by both Frost & Sullivan and Counterpoint as the industry-leading Connectivity Management Platform (CMP).

Introducing Cisco Programmable Core: Innovation Through Mobile Core-as-a-Service

Now generally available, the Cisco Programmable Core transforms a mobile core network into a source of differentiation, innovation, and growth. Fully orchestrated by Cisco and delivered as-a-Service, the Programmable

Core frees up operational assets so Communication Service Providers can quickly target high-growth opportunities, including Network-as-a-Service deployments, Mobile Virtual Network Enablement platforms, Fixed Wireless Access, IoT solutions, complex enterprise use-cases, and multi-country deployments.

The Programmable Core is a fully scoped end-to-end offering that handles voice, messaging and data services for IoT, private networks and public network use-cases which also unleash the innovation of 5G advanced services. It can

be deployed as an adjacent growth core alongside existing deployments or as a primary core for Communication Service Providers that want full as-a-service offerings.

Zayan Sadek, Managing Director for Service Providers MEA at Cisco, said: "The introduction of new functionalities in the Cisco Mobility Services Platform and the availability of Cisco Programmable Core mark a significant step forward in how Communication Service Providers and enterprises can create, and scale differentiated services. By delivering these solutions as-a-service, we are enabling greater agility, faster innovation, and expanded monetization opportunities—whether through IoT, Fixed Wireless Access, or 5G advanced services. With an open API ecosystem and industry-leading connectivity management, these advancements empower our partners to drive new value from their networks."

Mobility Services Platform: Driving Differentiated Value with New Functionality

The Mobility Services Platform introduces new services for partners and their enterprise customers.

New monetization opportunities for our Communication Service Provider partners

- **Smart grid, simplified:** Mass Scale IoT Solution enables service providers to offer comprehensive smart meter solutions with

automated device management, real-time monitoring, analytics, and security capabilities, with a licensing model that reduces upfront costs for utilities and municipalities.

- **Borderless business connectivity:** Fixed Wireless Access aaS enables Communication Service Providers to deliver high-speed wireless connectivity to both businesses and branch offices, through virtualized network functions, centralized management, and streamlined eSIM provisioning.
- **Adapt networks to use-case:** Communication Service Providers and car OEMs can leverage radio networks more efficiently and effectively by dynamically prioritizing traffic and quality of service.
- **Retail subscriptions in cars:** Connected Car OEMs can launch retail subscription services for car owners making use of Dynamic Policy and Charging as well as on-demand 5G standalone network slicing orchestration.
- **Monitor and monetize API usage:** Communication Service Providers can monetize actual usage and enable enterprises to track and understand their API usage, and buy capacity as needed
- **Seamless security with enterprise integration:** Integrated with existing enterprise security, leveraging shared identity and policy to deliver

cross-network security


- **eSIM Flex:** Aligns business needs with device management, ensuring the optimal profile for each device. eSIM Flex supports the M2M profiles today for IoT and is being extended to support the SGP .32 GSMA standard to support even more devices and outcomes for customers

Improved flexibility and operations

- **In-country or cloud deployment:** Can be deployed in-country on dedicated hardware, and on AWS infrastructure globally – increasing flexibility and speed to market
- **TMForum-based API exposure:** With catalog-driven service creation using standard API exposure (TMForum) it delivers more rapid service creation and seamless orchestration of services
- **Improved analytics:** Identifies anomalies in usage and traffic patterns, account churn, provisioning and business analytics as well as dynamic dashboarding and reports
- **AI assistant:** The new Mobility Services Platform AI assistant helps users and customers to realize more value from the platform more quickly

New packet core capabilities

At the heart of our platform, the Converged Core technology is also delivering new capabilities for customers:

- **5G Advanced:** Powering services like mass scale IoT, RedCap support and low latency, and Agentic AI workload integrations
- **Flexible optimization:** Flexibility to support 5G Advanced capabilities while maintaining support for traditional voice and data services – with a single software base and deployment automation
- **Multi-access, multi-network support:** Seamless policy and service authorization for end customers across multiple access networks, including fiber access, via converged policy solutions. 

“THE INTRODUCTION OF NEW FUNCTIONALITIES IN THE CISCO MOBILITY SERVICES PLATFORM AND THE AVAILABILITY OF CISCO PROGRAMMABLE CORE MARK A SIGNIFICANT STEP FORWARD IN HOW COMMUNICATION SERVICE PROVIDERS AND ENTERPRISES CAN CREATE, AND SCALE DIFFERENTIATED SERVICES”
ZAYAN SADEK, MANAGING DIRECTOR FOR SERVICE PROVIDERS MEA AT CISCO



Jeff Denworth, Co-Founder at VAST Data

VAST DATA PLATFORM ADDS NEW CAPABILITIES TO BECOME THE FIRST AND ONLY ENTERPRISE AI DATA PLATFORM FOR REAL-TIME AGENTIC APPLICATIONS

VAST INSIGHTENGINE POWERS AI-DRIVEN DECISION-MAKING WITH REAL-TIME DATA INGESTION, PROCESSING, AND RETRIEVAL – UNIFYING VECTOR SEARCH, EVENT-DRIVEN AUTOMATION, AND FINE-GRAINED SECURITY WITHIN A SINGLE HIGH-PERFORMANCE DATA PLATFORM

VAST Data, the AI data platform company, today announced new enhancements to the industry-leading VAST Data Platform, making it the first and only system in the market to unify structured and unstructured data, into a single DataSpace that scales linearly to hyperscale – with unified enterprise-grade security. These new capabilities are redefining enterprise AI and analytics by combining real-time vector search, fine-grained security, and event-driven processing into a seamless, high-performance data ecosystem that powers the VAST InsightEngine, which transforms raw data into AI-ready insights through intelligent automation, enabling enterprises to build advanced AI applications, agentic workflows, and high-speed inferencing pipelines.

Organizations today face significant challenges in scaling enterprise AI deployments. AI models call for ultra-fast vectorized search and retrieval for fast access to the most up-to-date information, with AI-driven workloads requiring massive computational power and well integrated data pipelines. Enterprise AI applications involve sensitive data and mission-critical workflows, yet many AI pipelines lack enterprise-grade security, encryption, and governance controls that span all data sources.

To address these challenges, the VAST Data Platform now includes include:

- **Vector Search & Retrieval:** The VAST DataBase is the first and only vector database that supports trillion-vector scale with the ability to search large vector spaces in constant time, making it both possible and practical to index all data and make it available to agentic workflows at any scale. With AI-powered Similarity search for real-time analytics and discovery, organizations can turn real-time data into AI-driven decisions by automatically embedding vectors for search and retrieval.
- **Serverless Triggers & Functions:** The VAST DataEngine is the first and only solution to create real-time workflows that don't require background ETL tools or scanning to provide generative-AI access from source data. With event-driven automation for AI workflows and real-time data enrichment, this system can embed and serve context to agentic applications instantaneously, breaking down the barriers to real-time RAG in the enterprise to allow organizations to accelerate AI and analytics with high-speed queries, serverless processing, and automated pipelines that securely ingest, process, and retrieve all enterprise data (files, objects, tables, and streams) in real-time.
- **Fine-Grained Access Control & AI-Ready Security:** VAST's built-in enterprise-grade security context now offers advanced row- and column-level permissions, ensuring

compliance and governance for analytics and AI workloads, while unifying permissions for raw data and vector representations.

As organizations embrace AI retrieval, and as embedding models continue to make exponential improvements in their understanding of enterprise data, only the VAST Data Platform can provide a unified, AI-ready solution that can meet the needs of extreme-scale agentic enterprises. The parallel transactional nature of VAST's unique DASE architecture makes it possible to update vector spaces in real-time for the first time, and this shared-everything approach allows for all servers to search the entire vector space in milliseconds – enabling VAST InsightEngine to transform raw data into AI-ready insights instantly, empowering organizations to make decisions with maximum accuracy.

"Only two kinds of companies exist today: those becoming AI-driven organizations, and those approaching irrelevance," said Jeff Denworth, Co-Founder at VAST Data. "In order to thrive in the AI era, enterprises need instant AI insights, enterprise-grade security, and limitless scalability – without worrying about managing fragmented tools or data infrastructure. The VAST InsightEngine is the only market's first and only solution able to securely ingest, process, and retrieve all enterprise data – files, objects, tables, and streams – in real-time to make enterprise data instantly usable for accurate AI-driven decision making." 🔒



Anisha Vaswani

EXTREME NETWORKS ANNOUNCES APPOINTMENT OF ANISHA VASWANI AS CHIEF INFORMATION AND CUSTOMER OFFICER

I COMPANY CREATES NEW EXECUTIVE ROLE TO DRIVE THE INTERLOCK BETWEEN INNOVATION AND CUSTOMER EXPERIENCE

Extrême Networks, Inc. (Nasdaq: EXTR), a leader in AI-powered automation for networking, has appointed Anisha Vaswani as Chief Information and Customer Officer (CICO). Vaswani will report directly

to Extreme President and CEO Ed Meyercord.

As CICO, Vaswani will develop and implement the company’s overall IT strategy, ensuring that technology investments support the company’s business objectives and growth.

Additionally, she’ll focus on driving internal innovation and customer success for the company by acting as “Extreme’s Customer ONE,” testing and validating Extreme’s products and solutions before rolling them out to customers to ensure they create a new industry standard for excellence. Vaswani will also oversee the company’s customer success initiatives, proactively engaging with customers to complete successful technology migrations and deliver significant value add – prioritizing long-term customer relationships, loyalty and retention.

“At Extreme, we believe technology and customer experience must be seamlessly integrated, which is why we created the CICO role. Anisha is the perfect candidate to ensure that every innovation enhances the customer journey. Her expertise in cloud adoption, cybersecurity and AI, combined with her track record of driving product adoption, maximizing value and increasing customer lifetime value, will help Extreme continue its journey to becoming a leading SaaS company in our space,” said Ed Meyercord, President and CEO of Extreme.

Prior to Extreme, Vaswani served in several CIO roles at prominent companies such as IDG, Box, Toast, Inc., and Shockwave Medical. As Shockwave Medical, she helped the company scale operations and grow annual revenue to \$1B. As CIO of Toast, she helped guide the company through the IPO process and played a role in growing the company from \$1B in revenue to over \$3B in annual revenue. She holds a B.S. in Management Information Systems from San Jose State University.

Anisha Vaswani, CICO at Extreme, said, “Extreme is at a pivotal moment, with innovations like Extreme Platform ONE set to redefine the future of networking. I’m excited to join a team of visionary thinkers and believe that through relentless innovation and an unwavering focus on our customers, we’ll turn bold ideas into transformative success. Creating customer value is at the heart of everything we do.”



Fortify Your Cybersecurity

Fortinet
Global Cybersecurity Leader

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

Learn more at fortinet.com

Delinea

Securing identities at every interaction

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



Secure Credentials



Privileged Remote Access



Privilege & Entitlement Elevation



Identity Threat Protection



Identity Governance



Follow us on



delinea.com