

INSIDE Channel Insights

Enterprise

AUTOMATION • ARTIFICIAL INTELLIGENCE • CLOUD

CHANNEL PARTNERS

MEA

PAGES 44
VOLUME 12 | ISSUE 5
DECEMBER 2024
WWW.EC-MEA.COM

ENTERPRISE SOLUTIONS CHANNEL PARTNERS

Piers Morgan
SVP & General Manager-
EMEA

SIMPLIFIED
CYBERSECURITY
BY CORO





GLOBAL CIO EXPERTISE,
DRIVING INNOVATION
FOR PEOPLE AND PLANET

CONSULTING | RESEARCH | ON DEMAND

www.iamcaas.com



- RESEARCH
- INSIGHT & BENCHMARKING
- EMERGING TECHNOLOGIES
- GOVERNANCE
- RISK & COMPLIANCE
- CYBER SECURITY
- DIGITAL TRANSFORMATION
- DEOPS & DIGITAL INFRASTRUCTURE
- ERP & CRM



The trends that defined tech in 2024

As we wind down 2024, it's important to look back through the rearview mirror and reflect on the defining trends and milestones that shaped this year. 2024 was undoubtedly the year that AI came of age. While 2023 laid the foundation for generative AI's rise, this year witnessed AI moving beyond experimentation into the inferencing stage—where real-world applications began delivering value at scale. Businesses across industries accelerated their AI initiatives, from automation and personalization to data-driven decision-making. For organizations the question is no longer “Should we adopt AI?” but rather “How quickly can we scale it across operations?”

It was also a strong year for channel partners, who continued to thrive by presenting differentiated value propositions. In a competitive technology landscape, channel players who delivered measurable outcomes aligned with their client's goals, whether in AI deployment, cybersecurity, or cloud integration, continued to reap rich rewards.

Another trend that dominated this year was the accelerated adoption of public cloud, with organizations of all sizes embracing cloud solutions to modernize their IT infrastructure and drive scalability. Cloud providers like AWS, Microsoft Azure, and Google Cloud saw accelerated regional growth as enterprises prioritized flexibility, agility, and innovation. As digital transformation gains momentum, cloud adoption is all set to become a cornerstone of business resilience and agility.

At the same time, the cybersecurity market surged to new heights in 2024, responding to an increasingly complex and threatening security landscape. Cyberattacks grew more sophisticated, targeting businesses, and governments alike. Ransomware, data breaches, and phishing attacks dominated headlines, underscoring the urgent need for robust security measures.

The market's “red hot” status also reflected the growing demand for skilled cybersecurity professionals and advanced tools to protect critical data and systems.

According to Canalsys, 2025 is expected to be a year of significant growth for the tech industry, with global IT spending projected to expand by 8%. The firm also predicts that partner-delivered IT will grow by 7.1%, accounting for 70% of the total addressable IT market.

Seize these opportunities, and I wish all our readers a very happy holiday season.

JEEVAN THANKAPPAN

jeevan@gecmmediagroup.com

PUBLISHER

TUSHAR SAHOO

tushar@gecmmediagroup.com

CO-FOUNDER & CEO

RONAK SAMANTARAY

ronak@gecmmediagroup.com

MANAGING EDITOR

Jeevan Thankappan

jeevan@gecmmediagroup.com

ASSISTANT EDITOR

SEHRISH TARIQ

sehrish@gecmmediagroup.com

**GLOBAL HEAD, CONTENT
AND STRATEGIC ALLIANCES**

ANUSHREE DIXIT

anushree@gecmmediagroup.com

GROUP SALES HEAD

RICHA S

richa@gecmmediagroup.com

PROJECT LEAD

JENNEFER LORRAINE MENDOZA

jennifer@gecmmediagroup.com

SALES AND ADVERTISING

RONAK SAMANTARAY

ronak@gecmmediagroup.com

Phone: + 971 555 120 490

Content Writer

KUMARI AMBIKA

IT MANAGER

VIJAY BAKSHI

DESIGN TEAM

CREATIVE LEAD

AJAY ARYA

SENIOR DESIGNER

SHADAB KHAN

GRAPHIC DESIGNERS

JITESH KUMAR

SEJAL SHUKLA

PRODUCTION, CIRCULATION, SUBSCRIPTIONS

info@gecmmediagroup.com

DESIGNED BY



SUBSCRIPTIONS

info@gecmmediagroup.com

PRINTED BY

AI Ghurair Printing & Publishing LLC.

Masafi Compound, Satwa, P.O.Box: 5613, Dubai, UAE



(UAE) Office No #115

First Floor, G2 Building

Dubai Production City

Dubai, United Arab Emirates

Phone : +971 4 564 8684

(USA) 31 FOXTAIL LAN,

MONMOUTH JUNCTION,

NJ - 08852

UNITED STATES OF AMERICA

Phone : +1 732 794 5918

A PUBLICATION LICENSED BY

International Media Production Zone, Dubai, UAE

@copyright 2013 Accent Infomedia. 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.

JOIN

FUN & THRILL WEEKENDS

BADMINTON
CRICKET
CYCLING
FOOTBALL
SWIMMING
TENNIS
TABLE TENNIS
GOLF
TEAM BUILDING TASK
TUG OF WAR
ATHLETIC
FITNESS CHALLENGE
BOWLING
VOLLEY BALL
BASKET BALL



GEC
TECH+
CORPORATE CHAMPIONSHIP

PARTICIPANTS
3000+

SPORTS
15

MATCHES
150+

CONTENTS



03
EDITORIAL

06-10
EVENTS

12-17
VIEWPOINT



18-26
NEWS

28-33
FEATURE

38-40
INTERVIEW



41
EXECUTIVE APPOINTMENTS

42
LAST WORDS





Empowering the future of Governance: insights and innovation at the GEC Government Technology Summit 2024

The GEC Media Group's recent summit brought together government leaders, industry experts, and technology pioneers to discuss the transformative power of digital strategies, artificial intelligence, and cybersecurity in public services. The event featured a rich lineup of speakers and panelists, offering valuable insights into critical areas of governance, innovation, and security.

The evening commenced with Jeevan Thankappan, Managing Editor of GEC Media Group, addressing the audience with a welcome note. His opening set the tone for a thought-provoking dialogue on leveraging technology to enhance citizen experiences.

A key highlight was the panel discussion on the role of AI in public services, moderated by Zaheer Kazi, Information Security Senior Specialist at the Ministry of Interior. Panelists included Dr. Hamad Khalifa Alnuaimi from Abu Dhabi Police GHQ, Noman Ejaz representing a government entity, Satheshwaran Manoharan of ADQ

Aviation and Aerospace, and Imran Khan from DEWA. They explored how AI-driven solutions are revolutionizing operational efficiency, citizen engagement, and policy-making.


In another engaging panel discussion, cybersecurity challenges specific to the BFSI sector were tackled under the moderation of Flavio Carvalho, CISO Iberia at Group Credit Agricole. The panelists, Dennis Pokupec of Creditplus Bank AG, Neha Yadav from Abu Dhabi Securities Exchange, and Saqar Al Ali from Sharjah Finance Department, shared strategies for safeguarding data, transactions, and compliance with global standards.

Vendor keynotes further enriched the dialogue, with Amit Mathur of Ensurity Technologies discussing effective cybersecurity measures for air-gapped government infrastructures and Mohamed Djenane from Seclore presenting on the transformations anticipated by 2030. Nasir Manzoor, Business Unit Head at AV Tech First Gulf FZ LLC, also shared

groundbreaking insights during his keynote.

The final panel focused on digital governance and shared services, moderated by Jeevan Thankappan. Panelists included Kelly Machado, Hessa Almatroosi of Free Zones Authority Ajman, Suzan Alghanem from the Environment Agency – Abu Dhabi, and Annu Chouraria, an expert in IT Governance and Risk Management. The discussion centered on collaborative models for efficient service delivery and the challenges of implementing shared services.

The summit concluded with a celebration of the Top 20 Government Champions, recognizing exemplary contributions to advancing public services. A networking dinner provided attendees an opportunity to exchange ideas and build connections, wrapping up a successful and inspiring event.

This summit reaffirmed the critical role of collaboration, innovation, and security in shaping the future of governance, leaving participants with actionable strategies to navigate an ever-evolving digital landscape. 

GEC media group hosts a transformative Vertical Days Event, highlighting innovation and sustainability in BFSI, education, and hospitality



GEC Media Group concluded its highly successful Vertical Day Event, a comprehensive gathering designed to showcase the role of technological advancements and sustainability across three key sectors: Banking, Financial Services, and Insurance (BFSI), Education, and Hospitality. The event provided a dynamic platform for industry leaders, technology innovators, and sustainability advocates to discuss critical trends, opportunities, and challenges shaping the future of these industries.

The event opened with an engaging

registration and networking coffee session, setting the tone for a day of learning, collaboration, and celebration. Each vertical hosted specialized sessions tailored to address the unique demands and innovations of its respective industry.

The Education Day began with opening remarks delivered by Anushree Dixit, Global Head - Strategy and Alliances at GEC Media Group, emphasizing the importance of technology innovation in reshaping education. The first panel discussion, moderated by May El Barachi, Director of Computer Science and IT at the University of Wollongong in Dubai,

explored how EdTech is redefining education. The panel featured distinguished voices such as Dr. Munir Majdalawieh, Head of the Information Systems and Technology Management Department at Zayed University, and Ahmed Mansour, IT Infrastructure Team Leader at Emirates College for Advanced Education. Together, they discussed the transformative role of digital tools and platforms in enhancing accessibility and engagement in education.

The day's second panel discussion focused on sustainable education practices and technological innovations in green education, moderated by Abdulrahman

BANKING & FINANCIAL SERVICES INNOVATION DAY

NAME	ORGANIZATION	CATEGORY
KHALDUN AL KHALDI	DUBAI ISLAMIC BANK	TOP BFSI CHAMPION
HALA ELGHAWI	STANDARD CHARTERED BANK	TOP BFSI CHAMPION
MADAN MOHAN	BDO	TOP BFSI CHAMPION
TUSHAR VARTAK	RAKBANK	TOP BFSI CHAMPION
ALI ABEDI	YAS TAKAFUL PJSC	TOP BFSI CHAMPION
MAMOUN ALHOMESSY	AJMAN BANK	TOP BFSI CHAMPION
MUHAMMAD TARIQ SIDDIQUI	ABU DHABI NATIONAL TAKAFUL	TOP BFSI CHAMPION
ASHOK PRASANNA THARMIA GNANSEKARAN	AL ANSARI FINANCIAL SERVICES	TOP BFSI CHAMPION
MOHAMMED AL DOSERI	TASHEEL FINANCE	TOP BFSI CHAMPION
ALI CHEHADE	CFI FINANCIAL GROUP	TOP BFSI CHAMPION
RAHUL CHHABRA	FIRST ABU DHABI BANK (FAB)	TOP BFSI CHAMPION
KASHIF KHAN	ABU DHABI NATIONAL INSURANCE COMPANY (ADNIC)	TOP BFSI CHAMPION
MOHAMMED TARIK KOUBAA	EMIRATES NBD	TOP BFSI CHAMPION
FAWAZ KHALIL	COMMERCIAL BANK INTERNATIONAL	TOP BFSI CHAMPION
KALYAN KRISHNA	STANDARD CHARTERED BANK	TOP BFSI CHAMPION
HUSSAIN ALKHALSAN	ZAND BANK	TOP BFSI CHAMPION
MUHAMMAD AZAM	ABU DHABI NATIONAL TAKAFUL CO. PSC	TOP BFSI CHAMPION
SHUJAT ALI MOHAMMED	ABU DHABI ISLAMIC BANK	TOP BFSI CHAMPION
ANAND KRISHNAN	EMIRATES INVESTMENT BANK	TOP BFSI CHAMPION
SYED MOHAMMAD ALI NAQVI	RAQAMI ISLAMIC DIGITAL BANK	TOP BFSI CHAMPION

Khaiwi, Head of IT Department at Emirates National Schools. Experts, including Sutharsan CP, Head of AI and Product Architecture at GEMS Education, and George Akhras, Chief Information Officer at AMSI, shared insights on achieving sustainability goals within academic institutions. The event culminated in the Top 20 Champions Awards for Education, recognizing groundbreaking contributions to innovation and sustainability in the education sector, followed by an evening of networking and dinner.

The Hospitality Day was inaugurated by Richa Samantaray, COO of GEC Media

Group, who delivered the opening remarks and underlined the pivotal role of technology in driving advancements in hospitality. The first panel discussion, moderated by Ahmed Hafez, Corporate Director IT at Jannah Hotels & Resorts, addressed the future of artificial intelligence in hospitality. Panelists, including Muhamed Noufel, IT Manager at Royal Continental Hotel Dubai, and Amila Karunaratne, Director of IT Operations at The First Group, discussed how AI is revolutionizing guest experiences and operational efficiency.

The second panel explored the theme of sustainability and net-zero initiatives in

hospitality, moderated by Shanaka Perera, Head of IT at Ras Al Khaimah Tourism Development Authority. Panelists such as Mohamed Slama, Project Director for Global Guest Technology & Innovation at Accor, and Lijesh Rajan, Corporate Director of IT Strategy & Services at Rotana, shared strategies for reducing carbon emissions and integrating sustainable technologies within the hospitality sector. The day concluded with the Top 20 Champions Awards for Hospitality, honoring exceptional achievements in leveraging technology for sustainability, followed by an evening of networking and a formal dinner.

EDUCATION DAY

NAME	ORGANIZATION	CATEGORY
ABDULRAHMAN KHAIWI	EMIRATES NATIONAL SCHOOLS	TOP EDUCATION CHAMPION
GEORGE AKHRAS	AMSI	TOP EDUCATION CHAMPION
SREEJIT CHAKRABARTY	GEMS EDUCATION	TOP EDUCATION CHAMPION
JOSEPH ANINIAS	ABU DHABI UNIVERSITY	TOP EDUCATION CHAMPION
AHMED MANSOUR	EMIRATES COLLEGE FOR ADVANCED EDUCATION	TOP EDUCATION CHAMPION
SANIL ABDULLA MANOLY	UNIVERSITY OF WOLLONGONG IN DUBAI	TOP EDUCATION CHAMPION
ALVEENA ABRAR	PARAMOUNT EDUCATION	TOP EDUCATION CHAMPION
AHMAD KHANFER	SAMA AMERICAN PRIVATE SCHOOL	TOP EDUCATION CHAMPION
MAY EL BARACHI	UNIVERSITY OF WOLLONGONG IN DUBAI	TOP EDUCATION CHAMPION
SARAVANAKUMAR DHINAKARAN	BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI DUBAI	TOP EDUCATION CHAMPION
NAZIK ZAIDAN	MOHAMMED BIN ZAYED UNIVERSITY FOR HUMANITIES	TOP EDUCATION CHAMPION
DR. MUNIR MAJDALAWIEH	ZAYED UNIVERSITY	TOP EDUCATION CHAMPION
OMAR WAEEL	TAALEEM	TOP EDUCATION CHAMPION
RIJESH KUMAR	GEMS DUBAI AMERICAN ACADEMY	TOP EDUCATION CHAMPION
PRAGNESH MENON	MIDDLESEX UNIVERSITY DUBAI	TOP EDUCATION CHAMPION
HUSSAIN ALKHALSAN	ZAND BANK	TOP BFSI CHAMPION
MUHAMMAD AZAM	ABU DHABI NATIONAL TAKAFUL CO. PSC	TOP BFSI CHAMPION
SHUJAT ALI MOHAMMED	ABU DHABI ISLAMIC BANK	TOP BFSI CHAMPION
ANAND KRISHNAN	EMIRATES INVESTMENT BANK	TOP BFSI CHAMPION
SYED MOHAMMAD ALI NAQVI	RAQAMI ISLAMIC DIGITAL BANK	TOP BFSI CHAMPION

The BFSI Innovation Day featured a series of impactful discussions on the role of technology in banking and financial services. The opening remarks, delivered by Anushree Dixit, highlighted the importance of technological advancements in driving innovation and efficiency within the BFSI sector. The first panel, moderated by Jordan Savvides, Global CISO at Global CISO Advisory, focused on cybersecurity and risk management. Panelists such as Sunil Nair, CISO at McCoin Virtual Assets, and Uneiza Alvi, Infosec and Threat Assessment Manager at Emirates NBD, explored strategies for safeguarding financial

transactions and ensuring compliance with global data protection regulations.

The second panel discussion delved into sustainable finance and ESG initiatives, moderated by Jayakumar Mohanachandran, Group CIO at Buzeki Group. Key speakers, including Anand Krishnan, Head of Technology at Emirates Investment Bank, and Syed Mohammed Naqvi, Chief Technology Officer at Raqami Islamic Digital Bank, discussed innovative approaches to achieving ESG goals and fostering sustainable financial ecosystems. The BFSI segment concluded with the Top 20 Champions Awards,

celebrating organizations and individuals who have made significant contributions to innovation and sustainability in the financial sector, followed by dinner and networking opportunities.

The Vertical Day Event underscored GEC Media Group's commitment to fostering innovation and sustainability across industries. By bringing together experts and leaders, the event provided a unique opportunity for collaboration and exchange of ideas, setting a strong foundation for continued growth and transformation in BFSI, education, and hospitality. 🏡

HOSPITALITY TECHNOLOGY DAY

NAME	ORGANIZATION	CATEGORY
MUHAMED NOUFEL	ROYAL CONTINENTAL HOTEL, DUBAI	TOP HOSPITALITY CHAMPION
HUSAM MAHMOUD	ABU DHABI NATIONAL HOTELS	TOP HOSPITALITY CHAMPION
HARIS BASHEER	CONRAD ABU DHABI ETIHAD TOWERS	TOP HOSPITALITY CHAMPION
ATUL KUMAR GUPTA	WYNDHAM HOTELS & RESORTS	TOP HOSPITALITY CHAMPION
AMILA UDANA	THE FIRST GROUP	TOP HOSPITALITY CHAMPION
ROGER TABBAL	ACCOR	TOP HOSPITALITY CHAMPION
AHMED SHAWKY	MILLENNIUM HOTELS AND RESORTS	TOP HOSPITALITY CHAMPION
LIJEESH RAJAN	ROTANA HOTELS	TOP HOSPITALITY CHAMPION
ASHRAF SALAH	HILTON WORLDWIDE	TOP HOSPITALITY CHAMPION
SHANAKA PERERA	RAS AL KHAIMAH TOURISM DEVELOPMENET AUTHORITY	TOP HOSPITALITY CHAMPION
PRASHANT DUTTA	JUMEIRAH HOTELS & RESORTS	TOP HOSPITALITY CHAMPION
FEROZ PATEL	IMG WORLD OF ADEVENTURE	TOP HOSPITALITY CHAMPION
SAJITH PILLAI	MILLENNIUM PLACE MARINA	TOP HOSPITALITY CHAMPION
AMAR PRAKASH	AL TAYER	TOP HOSPITALITY CHAMPION
RAMKUMAR VALLIAPPAN	MARRIOTT INTERNATIONAL	TOP HOSPITALITY CHAMPION
ASLAM KHERAWALA	ILYAS & MUSTAFA GALADARI GROUP	TOP HOSPITALITY CHAMPION





THE NEW OPTIPLEX FAMILY

INTELLIGENCE MEETS SIMPLICITY

Dell's new desktops are redesigned and simplified to make finding your perfect match easier than ever. The new OptiPlex family features Windows 11 Pro, AI-personalization from the latest Optimizer, one BIOS for all-in-ones and one BIOS for towers. Find the OptiPlex that fits your workstyle now.



Dell Technologies recommends
Windows 11 Pro for business



New study finds 80% of organizations experienced an email-related security breach in the last year

Yiyi Miao

Chief Product Officer at OPSWAT



OPSWAT, a global leader in critical infrastructure protection (CIP) cybersecurity solutions, has released the 2024 Report: Email Security Threats Against Critical Infrastructure

Organizations. This research was conducted with Osterman Research, known for its in-depth analysis and insights into emerging trends and technologies in IT security and data management. The study surveyed IT and security leaders working within critical infrastructure industries and revealed that 80% of organizations experienced an email-related security breach over the past year and 63.3% of respondents acknowledge that their email security approach needs to be improved.

Email is a necessary tool for communication and productivity across all sectors, but it is also

the primary attack vector for cyber threats with attackers exploiting vulnerabilities through phishing attempts, malicious links, and harmful attachments. Once infiltrated, these threats can cascade through networks, jeopardizing both IT and operational technology (OT) environments. Alarming, more than half of respondents believed email messages and attachments to be benign by

default, failing to realize inherent email risks

Key takeaways from the research include:

Up to 80% of organizations in critical infrastructure sectors have been the victim of an email security breach in the past 12 months

Per 1,000 employees, the organizations in this research experienced 5.7 successful phishing incidents per year, 5.6 account compromises, and 4.4 incidents of data leakage, among other types of email security breaches. Organizations in critical infrastructure sectors are highly attractive to cyberthreat actors and are under constant attack.

Email is the primary cybersecurity attack vector in critical infrastructure sectors. A median of 75% of cybersecurity threats against organizations in critical infrastructure sectors arrive via email. For two out of three organizations, the share of cybersecurity threats arriving by email ranges from 61% to 100%.

Success metrics for email security are low

48% of the critical infrastructure organizations in this research are not confident that their current email security protections are sufficient against email-borne attacks. Only 34.4% are fully compliant with the email-related regulations that apply to them, e.g., GDPR and other privacy

regulations. And 63.6% are not confident that their approach to email security is best in class.

Threat levels for all types of cybersecurity attacks are expected to increase, with phishing, data exfiltration, and zero-day malware attacks leading the way


Over 80% of organizations expect threat levels of all email attack types to increase or stay the same over the next 12 months.

Organizations aspire to be dramatically better—and rapidly, too. While current email security efficacy metrics are low, aspirations run high for a dramatic and rapid shift. While only 52.0% of organizations are confident in their current email security protections, it is the aspiration of 74.8% to reach this level within 12 months. In a similar vein, 84.8% of the organizations aspire to be at a place where their approach to email security protects them from emerging and as-yet-unknown email threats over the next 12 months.

“This survey findings emphasize the need to adopt a zero-trust mindset. The prevalence of

email-related breaches poses a significant threat to critical infrastructure organizations,

necessitating a shift to a stronger, prevention-based perimeter defense strategy against

established communication and data exchange channels,” commented Yiyi Miao, Chief Product Officer at OPSWAT. 

Businesses anticipate increase in cyber threats, yet remain: Cloudflare research

Christian Reilly,
Field CTO EMEA, Cloudflare



It's no secret that cyber-attacks are becoming increasingly sophisticated, while simultaneously growing in number and volume. And this worrying trend is only expected to rise. In fact, Cloudflare's own research shows that a staggering 78% of business leaders in the Middle East and Türkiye (MET) region expect their organizations to be hit by a cyberattack within the next year.

But, despite these concerns for the near future, the same study shows that only 46% of those leaders believe they are adequately prepared to handle such an incident. Clearly, there is a significant disconnect between the perceived risk of cyber threats and the level of preparedness among the nation's businesses.

So, as the digital threat landscape continues to evolve, regional businesses find themselves in an increasingly delicate position when it comes to cybersecurity. The growing number of incidents facing modern companies is well documented in today's headlines, leaving organizations in no doubt that this is a serious issue that every business should have near the top of their agendas.

In this landscape, how can companies become more confident in their ability to defend themselves against modern cyber threats?

This discrepancy isn't a question of ignorance

but of confidence – or the lack thereof. With 82% of organizations in the MET region reporting a cybersecurity incident in the past year according to our data, the threat is very real. And still, less than half of the business leaders surveyed feel they have the necessary defenses in place. This points to a critical issue: while awareness is growing, true preparedness remains worryingly low. That's despite the real-life ramifications that can be expected when a business suffers a breach.

Cost of a breach is more than just financial

Not only could an incident have serious consequences for the business itself, but it could also have a negative impact on your employees and customers. Whether it's financial losses, regulatory penalties or reputational damage, the stakes are high when it comes to having a lack of robust defense mechanisms. The financial losses arising from incidents can rack up quickly. Among the 53% of respondents whose organizations experienced a cybersecurity incident in the past year, 77% estimated the financial impacts to be at least US\$1 million, while one third (38%) estimated the loss to be US\$2 million or more. Financial loss is not the only impact organizations have suffered. 38%

organizations have had to put growth plans on hold in the aftermath of an incident, and 37% have had to lay off staff as a result of the financial impact.

Learning from experience

What stands out from the Cloudflare data is that sectors in the region with higher attack frequencies, such as Financial Services and IT, report feeling more prepared for future incidents. This is logical – experience breeds resilience. This confidence also likely stems from the sectors' early adoption of advanced cybersecurity tools and practices, equipping them to handle the evolving threat landscape.

SolarWinds is a great example of a business that took significant steps to overhaul its security practices after a breach – and come out stronger. The company enhanced its software development process with its Secure by Design principle, adopted a Zero Trust architecture, and increased transparency by openly communicating with customers and regulators.

SolarWinds also collaborated with cybersecurity experts to continuously improve their defences, while contributing to industry-wide efforts to bolster software supply chain security. 🔴

The exploitation of gaming engines: A new dimension in cybercrime

Eli Smadja,
Group Manager
Checkpoint



In the ever-evolving landscape of cyber threats, cybercriminals continually enhance their tactics to achieve higher infection rates and remain under the radar of cyber security systems. A recent discovery by Check Point Research has unveiled a chilling new trend that takes advantage of gaming engines, specifically their scripts. A popular open-source game engine, Godot Engine, has been exploited by threat actors to run malicious scripts called GodLoader and drop payloads, resulting in the infection of over 17,000 machines. This innovative technique enables attackers to carry out credential theft and deploy ransomware, posing significant risks to the 1.2 million users of Godot-developed games.

Here, we will describe how threat actors leverage Godot Engine, how the malware is distributed, and its potential to infect more players of Godot-developed games.

Understanding the Godot Gaming Engine Godot Engine is an open-source game development platform revered for its flexibility and comprehensive toolset. Designed for creating both 2D and 3D games, it supports various export formats, facilitating the reach of developers to platforms such as Windows, macOS, Linux, Android, iOS, and HTML5. With a user-friendly interface and a Python-like scripting language called GDScript, Godot empowers developers of all levels. Additionally, its active community of over 2,700 contributors and 80,000 followers on

social media highlights its popularity and dedicated support. However, this very appeal is now being exploited by cybercriminals.

The GodLoader Technique

Threat actors have utilized Godot's scripting capabilities to create custom loaders, called GodLoader, that remain undetected by many conventional security solutions. Since Godot's architecture allows platform-agnostic payload delivery, attackers can easily deploy malicious code across Windows, Linux, and macOS, sometimes even exploring Android options. Additionally, the simplicity of GDScript, combined with Godot's ability to integrate into various operating systems, enables attackers to bypass traditional detection methods.

Since June 29, 2024, a new technique utilizing the malicious GodLoader has evaded detection by most antivirus tools, reportedly infecting more than 17,000 machines within three to four months.

Mechanism of Attack

The Godot Engine is vulnerable due to its use of .pck files, which bundle game assets like scripts and scenes. These files can trigger malicious GDScript execution via a built-in callback function, allowing attackers to download malware or execute remote payloads undetected. GDScript's functionality enables anti-sandbox, anti-VM, and remote execution capabilities, helping the malware stay hidden. Though initial attacks target Windows,

Godot's cross-platform nature puts other operating systems at risk as well.

Spreading GodLoader

The loader leverages the Stargazers Ghost Network, a sophisticated Distribution as a Service (DaaS) framework that masquerades malware delivery through seemingly legitimate GitHub repositories. From September to October 2024, GodLoader was distributed via 200 repositories, supported by over 225 Stargazer Ghost accounts that have artificially boosted the visibility of these malicious repositories by starring them. This approach creates an illusion of legitimacy, enticing unsuspecting developers and gamers to become victims.

The repositories were distributed and released into four separate waves, primarily targeting developers and gamers.

The Implications for Developers and Gamers

This new threat poses significant risks. Developers using open-source platforms like Godot Engine may unknowingly integrate malicious code into their projects, while gamers face heightened risks from downloading games created with compromised tools. The attacker behind this threat used the sophisticated Stargazers Ghost Network to distribute GodLoader, exploiting trust in open-source software to spread malware discreetly. By disguising malware as legitimate applications, the network quickly spreads to thousands of users. 🔴

DNS security: A must-have under NIS2

Craig Sanderson

Principal Cyber Security Strategist
at Infoblox



On 14 December 2022, the European Commission published “Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union,” otherwise known as the NIS2 Directive. This directive is the EU’s update to the Network and Information Systems Directive (NIS), aimed at strengthening cybersecurity across the EU by setting higher standards for security in essential and important sectors. The NIS2 Directive focuses on enhancing the resilience of critical infrastructure and improving the ability of EU member states to respond to cybersecurity incidents. It has a broad reach and significant impact on both EU and non-EU entities, applying to a wider range of sectors, including digital infrastructure, healthcare, energy, transportation, and critical public services. Additionally, it expands coverage to include not just essential services but also medium and large entities in critical sectors, including digital services and suppliers of key technologies.

October 17, 2024, was the deadline for EU Member States to implement NIS2 into national law. The European Commission has adopted the NIS2 Implementing Regulation, outlining key technological requirements for compliance. These requirements set the baseline across the EU, with more technical

details and guidance expected in the coming months.

Of particular relevance to legal, compliance and cybersecurity practitioners working for entities subject to NIS2, are the requirements of the Implementing Regulation on DNS security. Article 6(7) of the Implementing Regulation requires that “the relevant entities shall . . . apply best practices for the security of the DNS”.

The European Union Agency for Cybersecurity (ENISA) will help define what constitutes “best practice for the security of the DNS” and we look forward to collaborating with them in that endeavor.

Infoblox has been providing DNS and DNS security solutions for over 25 years and has performed countless numbers of DNS health and security assessments in organizations across the globe. Based on our experience we expect the best practices to focus on three key areas:

- Securing the DNS Platform
- Securing the DNS Protocol and
- Implementing DNS as a Cyber Security Control

Securing the DNS Platform

Cybersecurity regulations are focusing more on operational risk and digital resiliency, especially the availability of critical

infrastructure like DNS. Disruptions due to attacks or misconfigurations can be severe, and NIS2 will likely ensure that regulated entities have resilient DNS systems in their business continuity plans.

Infoblox found that many organizations have not assessed the strength of their DNS deployments, exposing them to operational and cybersecurity risks. Regulated entities will likely need to conduct DNS architecture assessments to address issues like poor patch management and resilience before implementing processes to maintain their DNS infrastructure. WW

Securing the DNS protocol

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) highlights that DNS is often exploited by cybercriminals for various attacks, including ransomware and phishing. Without proper security protections, DNS can be used to exfiltrate data, as it is typically allowed in cybersecurity systems for web browsing. Threat actors also use “lookalike” domains to increase phishing success rates, targeting both employees and consumers. Infoblox research shows 25,000 new lookalike domains are detected weekly, affecting organizations of all sizes. As DNS abuse grows, regulations like NIS 2 will likely push organizations to secure their external domains. 🔴

Why addressing the sustainability-profitability trade-off is a job for cloud ERP

Vibhu Kapoor

Regional Vice President - Middle East,
Africa & India, Epicor



Many supply chains end with the consumer. Even B2B enterprises are commonly part of a chain that terminates at a B2C link. The modern consumer, therefore, has great influence on the way a significant chunk of the economy operates. And that same modern consumer expects businesses to behave ethically and to respect the environment.

In the Middle East, where the last two COP summits were held, sustainability has become a regional focus. Qatar announced its National Environment and Climate Change Strategy (QNE) in 2021 as a means to fulfil the environment pillar of the country's National Vision 2030. Saudi Arabia started the National Energy Efficiency Program (NEEP) in 2008 and followed up in 2010 with the launch of the Saudi Energy Efficiency Centre (SEEC) and the King Abdullah City for Atomic and Renewable Energy (KACARE). The UAE government established the Ministry of Climate Change and Environment, which has authored a range of regulations and conventions on sustainability and green practices. And at the Egypt-hosted COP27, the UAE government unveiled its Net Zero 2050 Charter.

While these moves are admirable and necessary, we would be remiss if we did not

acknowledge the challenges manufacturers face in complying. Heavier industries play a huge part in economic diversification, but they face growing material and shipping costs. Fortunately, the Internet of Things is on hand to help. IoT solutions have allowed the emergence of smart factories, where data insights from shop floors and supply chains feed shrewd decision-making at every link in the manufacturing process — sourcing, production, and distribution.

Circular economy

The goals are reductions in materials waste and carbon output, and digital technologies can deliver at scale. But to be clear, these are new technologies. Legacy systems come with inefficiencies, including wasteful use of energy, because of the extensive physical infrastructure involved. Servers use electricity, heat up, and require even more electricity to power cooling solutions. These setups represent a relatively large carbon footprint. The answer is a migration to circular economy models.

The Qatar Foundation already has a plan for the circular economy, Saudi Arabia established the National Center for Waste Management (MWAN), and the UAE set up a Circular Economy Council. Subsequently, we have seen shifts in strategy across these economies

as enterprises explore ways to comply. All this motion has opened doors for technology providers that can support sustainability efforts.

It all begins with the supply chain. Cloud-based ERP solutions, integrated with MES, enable net-zero compliance while maintaining profitability. A 2023 Epicor report found that 96% of enterprises use cloud ERP, which offers benefits like minimal business downtime, reduced onsite energy use, and the ability to remotely monitor warehouses and factory floors.

Carbon accounting

Advances in AI and wireless connectivity have improved decarbonization, but now we must focus on analyzing complex supply chains. Integrated ERP systems can calculate compliance costs and provide visibility into product quality, traceability, and reparability, helping businesses balance profitability with environmental regulations. ERP also enables resilience against external challenges like logistics issues and inflation. Carbon accounting becomes second nature, driving emission reductions. ERP automates improvements and helps businesses offer verifiable sustainability claims, which will be key differentiators in the future. 🔥

Threat predictions for 2025: Get ready for bigger, bolder attacks



While threat actors continue to rely on many “classic” tactics that have existed for decades, our threat predictions for the coming year largely focus on cybercriminals embracing bigger, bolder, and—from their perspectives—better attacks. From Cybercrime-as-a-Service (CaaS) groups becoming more specialized to adversaries using sophisticated playbooks that combine both digital and physical threats, cybercriminals are upping the ante to execute more targeted and harmful attacks.

In our 2025 threat predictions report, our FortiGuard Labs team looks at tried-and-true attacks cybercriminals continue to rely on and how these have evolved, shares fresh threat trends to watch for this year and beyond, and offers advice on how organizations worldwide can enhance their resilience in the face of a changing threat landscape.

Emerging Threat Trends to Watch for in 2025 and Beyond

As cybercrime evolves, we anticipate seeing several unique trends emerge in 2025 and beyond. Here’s a glimpse of what we expect.

- **More Attack Chain Expertise Emerges:** In recent years, cybercriminals have been spending more time “left of boom” on the reconnaissance and weaponization phases of the cyber kill chain. As a result, threat actors can carry out targeted attacks quickly and more precisely. In the past, we’ve observed many CaaS providers

serving as jacks of all trades—offering buyers everything needed to execute an attack, from phishing kits to payloads. However, we expect that CaaS groups will increasingly embrace specialization, with many groups focusing on providing offerings that home in on just one segment of the attack chain.

- **It’s Cloud(y) With a Chance of Cyberattacks:** While targets like edge devices will continue to capture the attention of threat actors, there’s another part of the attack surface that defenders must pay close attention to over the next few years: their cloud environments. Although cloud isn’t new, it’s increasingly piquing the interest of cybercriminals. Given that most organizations rely on multiple cloud providers, it’s not surprising that we’re observing more cloud-specific vulnerabilities being leveraged by attackers, anticipating that this trend will grow in the future.
- **Automated Hacking Tools Make Their Way to the Dark Web Marketplace:** A seemingly endless number of attack vectors and associated code are now available through the CaaS market, such as phishing kits, Ransomware-as-a-Service, DDoS-as-a-Service, and more. While we’re already seeing some cybercrime groups rely on AI to power CaaS offerings, we expect this trend to flourish. We anticipate that attackers will use the automated output from LLMs to power CaaS offerings and grow the market,

such as taking social media reconnaissance and automating that intelligence into neatly packaged phishing kits.

- **Playbooks Grow to Include Real-Life Threats:** Cybercriminals continually advance their playbooks, with attacks becoming more aggressive and destructive. We predict that adversaries will expand their playbooks to combine cyberattacks with physical, real-life threats. We’re already seeing some cybercrime groups physically threaten an organization’s executives and employees in some instances and anticipate that this will become a regular part of many playbooks. We also anticipate that transnational crime—such as drug trafficking, smuggling people or goods, and more—will become a regular component of more sophisticated playbooks, with cybercrime groups and transnational crime organizations working together.

Enhancing Collective Resilience Against an Evolving Threat Landscape

Cybercriminals will always find new ways to infiltrate organizations. Yet there are numerous opportunities for the cybersecurity community to collaborate to better anticipate adversaries’ next moves and interrupt their activities in a meaningful way.

The value of industry-wide efforts and public-private partnerships cannot be overstated, and we anticipate that the number of organizations participating in these collaborations will grow in the coming years. 🔴

Milestone Systems enhances cloud connectivity and the care plus experience with the latest Xprotect release

Milestone Systems has announced the release of the R2 2024 update to its XProtect platform today. This release introduces XProtect Remote Manager, a cloud-connected service that enhances the value of Care Plus subscriptions. The update also includes improvements to user experience and expanded language support.

Enhancing the Value of Care Plus

As organisations increasingly seek flexible, efficient ways to manage their video security systems, Milestone is expanding the value of its Care Plus subscription. The company is introducing XProtect Remote Manager, a cloud-connected service that allows XProtect administrators to monitor the health and status of distributed XProtect installations in one view from anywhere through a browser.

XProtect Remote Manager enables administrators to:

- View real-time health status of devices and servers across multiple sites



- Manage basic camera settings remotely
- Grant or revoke reseller access to customer sites

While XProtect Remote Manager is still in its early stages, it represents a significant step in Milestone's cloud strategy, laying the groundwork for future enhancements and capabilities. The latest XProtect release also includes updates aimed at improving user experience and expanding global accessibility:

- A new layout for video grids in Mobile Clients for Tablets, optimising space usage and enhancing visibility
- Vietnamese language support added to operator clients, furthering Milestone's commitment to serving diverse markets
- Additionally, Milestone has overhauled its XProtect 360 Split View plugin, improving video loading speed, reducing memory consumption, and enhancing overall stability for users working with 360-degree cameras.
- These updates reflect Milestone's ongoing dedication to innovation and responsiveness to customer needs. By continually refining its offerings and exploring new technologies, Milestone aims to provide video management solutions that meet current demands and are adaptable to future challenges in the security industry.

Gartner forecasts MENA IT spending to grow 7.4% in 2025



Eyad Tachwali, Sr. Director Advisory at Gartner

IT spending in the Middle East and North Africa (MENA) region is projected to total \$230.7 billion in 2025, an increase of 7.4% from 2024, according to the latest forecast by Gartner, Inc.

"Governments and private sector enterprises in MENA are investing heavily to position the region as a world-leading AI innovation hub, supported by strong cybersecurity and

cloud platforms to enable a highly scalable infrastructure," said Mim Burt, Managing VP Analyst at Gartner. "Local organizations are ramping up investments in research and development to create new business models, enhance customer experiences, and build a skilled workforce for global competitiveness, thereby boosting IT spending in the region."

AI and Cloud to Drive MENA Data Center Systems Spending in 2025

"In 2025, chief information officers (CIOs) in MENA are expected to increase their spending on data center technologies to cope with the growing adoption of AI and cloud services, as well as the rise in consumption of data storage and processing capacity," said Burt. "In addition, several major hyper-scalers in the region are investing in data center systems to provide sustainable, scalable AI-embedded cloud infrastructure, further bolstering the growth of this segment."

Strategic Shift in GenAI Investments for MENA CIOs in 2025

Software spending in MENA is projected to grow 13.7% in 2025, fueled by increased CIO investments in generative AI (GenAI)-enabled applications. "To enhance the digital workplace, customer experience, and product and service quality, MENA CIOs are spending more on the combined power of GenAI applications, cloud services, and cybersecurity software ensuring the safe acceleration of innovation for competitive differentiation," said Burt.

Pure Storage introduces new GenAI pod to accelerate AI innovation

Pure Storage has announced the expansion of its AI solutions with the new Pure Storage GenAI Pod, a full-stack solution providing turnkey designs built on the Pure Storage platform. Organizations can use the Pure Storage GenAI Pod to accelerate AI-powered innovation and reduce the time, cost, and specialty technical skills required to deploy generative AI (GenAI) projects. Pure Storage also announced the certification of FlashBlade//S500 with NVIDIA® DGX™ SuperPOD™, accelerating enterprise AI deployments with Ethernet compatibility.

Companies today face significant challenges deploying GenAI and retrieval-augmented generation (RAG) in private clouds. This includes navigating the complexity of deploying hardware, software, foundational models, and development tools that power GenAI workloads in a timely and cost-effective manner. At the same time, they need a single, unified storage platform to address all of their storage needs, including the most critical challenges and opportunities posed by AI.



Dan Kogan, VP, Enterprise Growth and Solutions, Pure Storage

The Pure Storage GenAI Pod, built on the Pure Storage platform, includes new validated designs that enable turnkey solutions for GenAI use cases that help organizations solve many of these challenges. Unlike most other full-stack solutions, the Pure Storage GenAI Pod enables organizations to accelerate AI initiatives with one-click deployments and streamlined Day 2 operations for vector databases and foundation models. With the integration of Portworx™, these services provide automated deployments of NVIDIA NeMo and NIM microservices through the NVIDIA AI Enterprise software platform, as well as the Milvus vector database, while further simplifying Day 2 operations.

“The pace of innovation is compelling enterprise customers to leverage AI across their business, but customers are held back by the fundamental challenge of siloed data platforms and complex-to-deploy Gen AI pipelines.” — Dan Kogan, VP, Enterprise Growth and Solutions, Pure Storage.

Axis Communications introduces ACS Edge and cloud storage for AXIS Camera Station



David Needham, EMEA Business Development Program Manager at Axis Communications

Axis Communications has launched two brand-new solutions within the AXIS Camera Station ecosystem. AXIS Camera Station Edge (ACS Edge) and AXIS Camera Station Cloud Storage (ACS Cloud Storage) transform network video management through edge

cloud capabilities and enhance companies' physical security and surveillance systems. The two solutions are now available as part of the AXIS Camera Station product suite.

As cloud adoption becomes essential for businesses in the Middle East to navigate

the global digital economy, the cloud also emerges as an essential component of modernising businesses' physical security and surveillance capabilities, combined with its potential for enhanced data analysis and cybersecurity.

A seamless camera-to-cloud experience

Providing a cloud-to-camera experience that's easy to set up and use, ACS Edge introduces a method of managing video data by processing images directly on the camera. This eliminates the need for external servers or cloud-based processing, resulting in reduced infrastructure needs, total cost of ownership (TCO), and operational costs.

“With ACS Edge, we are offering a true cam-to-cloud solution, while the rest of our new ACS offering extends our customers the opportunity of on-premise, cloud, and hybrid solutions,” said David Needham, EMEA Business Development Program Manager at Axis Communications.

COP29: Digital tech and AI can boost climate action

According to the UN International Telecommunications Union (ITU), which organized digital-focused events at COP29, digital technologies can be key tools to accelerate the achievement of the 2030 Agenda for Sustainable Development, as they play a key role in climate monitoring, early warning systems, and overall climate adaptation and mitigation.

The COP29 Declaration on Green Digital Action recognises the importance of digital technologies to mitigate and adapt to climate change. The objectives in the declaration underscore how digital innovations can reduce greenhouse gas emissions and provide life-saving tools to inform and warn communities.



“This milestone moment for Green Digital Action at COP29 should propel us forward with the shared belief that we can and must reduce the environmental footprint of digital technologies while leveraging their undeniable potential to tackle the climate

crisis,” said ITU Secretary-General Doreen Bogdan-Martin.

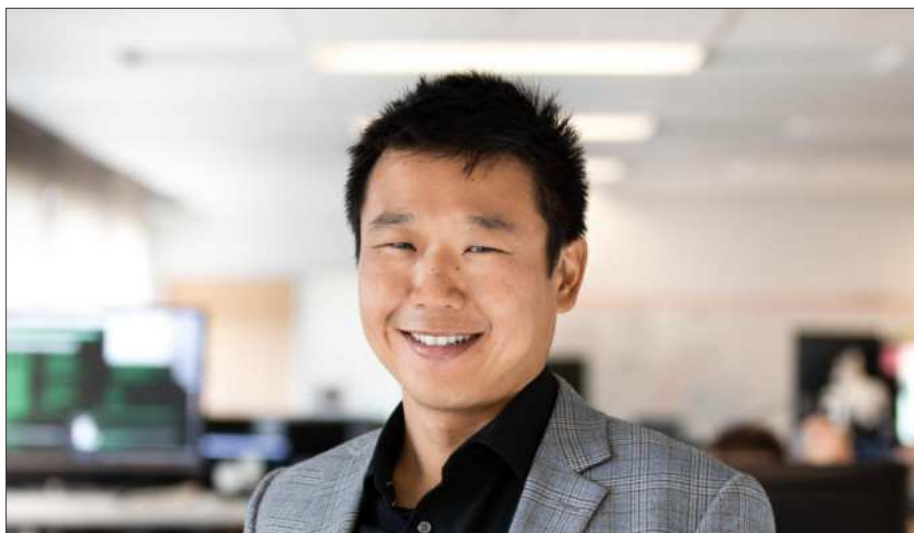
“Let’s keep building our green digital momentum all the way to COP30, and with it, a more sustainable digital future for generations to come,” she said.

Pure Storage announces strategic investment and technology partnership with CoreWeave

Pure Storage have announced Pure Storage’s strategic investment in CoreWeave to accelerate AI cloud services innovation. Alongside the investment, the companies unveiled a strategic partnership, enabling customers to leverage the Pure Storage platform within CoreWeave Cloud.

Building on their shared success with some of the world’s most advanced AI companies, this collaboration helps to fuel the next generation of AI innovators, driving breakthroughs with CoreWeave’s cloud services and the Pure Storage platform. By adding Pure Storage as a partner, CoreWeave recognises Pure Storage’s 15 years of innovation in flash technologies and its proven track record with some of the world’s top AI companies.

“Our strategic collaboration with CoreWeave reflects a shared commitment to delivering AI innovation at scale and marks a major milestone in delivering the flexibility and scalability that AI-driven organisations need to thrive. Integrating the Pure Storage platform into CoreWeave’s specialised cloud service environments enables customers that require massive scale and flexibility in their infrastructure the ability to tailor their infrastructure and maximise performance



Rob Lee, Chief Technology Officer, Pure Storage

on their own terms,” said Rob Lee, Chief Technology Officer, Pure Storage.

Empowering AI Supercomputers with Cutting-Edge Scale, Performance, and Flexibility

The Pure Storage platform is now available as an option within CoreWeave’s dedicated environments, which customers access through the CoreWeave Platform, a no compromise engineering solution purpose-

built for some of the world’s most compute intensive workloads. The CoreWeave Platform uses automation to simplify complexity, maximising infrastructure performance and efficiency, while Pure Storage offers a highly scalable, efficient storage solution, with joint solutions already deployed in production at supercomputing scale across thousands of GPUs. Together, they empower customers to accelerate their time to market.

'Playtime is over' for GenAI: NTT DATA research shows organizations shifting from experiments to investments that drive performance

NTT DATA has released the first results of its extensive original research that reveals "playtime is over" for GenAI. The results overwhelmingly found that leaders are turning their focus from experimentation to long-term use cases that transform business performance, workplace culture, compliance, safety and sustainability.

The study, "Global GenAI Report: How organizations are mastering their GenAI destiny in 2025," found that almost all leaders surveyed already have invested in GenAI, and 83% have established "expert" or "robust" GenAI teams. Top use cases for GenAI include:

- Personalized service recommendations and knowledge management
- Quality control
- Research and Development (R&D)

"The future is clear. Generative AI is more than just another tool – it's a transformative force," said Yutaka Sasaki, President and Chief Executive Officer, NTT DATA Group. "As



Prasanna Rajendran,
Vice President - EMEA, Kissflow

we move beyond experimentation, a tension emerges: move too fast, and we risk unintended circumstances; move too slow and we fall behind. Getting GenAI right isn't optional. That's why we're providing a blueprint to help our clients harness its potential for lasting success."

Two-thirds of C-suite respondents said GenAI will be a "game changer" over the next two years and will improve:

- Productivity and efficiency
- Sustainability
- Compliance
- Business processes
- Security
- Employee experience

Strategy and Transformation

A cycle of consolidation and integration of GenAI technologies is beginning that combines experimental, phased and specific approaches. Focused spending plans will replace scattered experimentation in a relatively short time:

- 97% of CEOs anticipate a material impact from this technology.
- 70% of CEOs expect significant transformation in 2025.
- 83% of respondents said they have a well-defined GenAI strategy in place, but 51% have not yet aligned that strategy with their business plans. This gap limits return on investment and satisfaction with current outcomes.

ServiceNow partners with NVIDIA to accelerate enterprise adoption of Agentic AI

ServiceNow has announced a major expansion to its strategic partnership with NVIDIA to accelerate enterprise adoption of Agentic AI. The companies will use NVIDIA NIM Agent Blueprints to co develop native AI Agents within the ServiceNow platform, creating use cases fueled by business knowledge that customers simply choose to turn on.

NVIDIA will collaborate with ServiceNow to map out multiple AI agent use cases. With six years of joint innovation on AI models, along with several previously announced strategic collaborations, ServiceNow and NVIDIA are reshaping how businesses integrate AI into their operations.

The Now Platform is rapidly becoming a foundation for enterprise transformation in the evolving landscape of generative AI. By harnessing NVIDIA's advanced AI infrastructure — such as the NVIDIA AI



Bill McDermott, CEO, ServiceNow

Enterprise software platform, including the NVIDIA NeMo framework and NVIDIA NIM microservices running on NVIDIA DGX Cloud, and ServiceNow's leading AI platform for business transformation, this partnership is supercharging productivity and streamlining complex workflows across

industries.

"GenAI is a massive tailwind for our industry, and ServiceNow and NVIDIA are bringing the next wave of agentic AI to enterprises everywhere," said ServiceNow Chairman and CEO Bill McDermott.

Enriching ServiceNow AI Agents with NVIDIA NIM Agent Blueprints for Cybersecurity

With unified, real time access to enterprise wide knowledge, tools, workflows, and data on the Now Platform, ServiceNow AI Agents — originally announced in September — can comprehend and interpret context, break down complex outcomes into smaller tasks, prioritize them, plan actions, and execute strategies to achieve desired results. Co development between ServiceNow and NVIDIA will expand out of the box AI agent use cases into additional solution areas, beginning with security vulnerability.

SIBEC 2024 elevates UAE as a global hub for fire and life safety innovation

Powered by SIBCA and ICT Solutions provider has successfully concluded. Held in Abu Dhabi, UAE, from 13-15 November 2024, this year's event welcomed a record number of partners under the theme 'Innovation That Keeps You Safe,' spotlighting the vital role of the Internet of Things (IoT) in ensuring a safer and more secure future.

The two-day event brought together leading experts and professionals from regional and global markets to explore the latest trends and innovations in various sectors, including building management system (BMS), extra-low voltage (ELV), audiovisual (AV), heating, ventilation, and air conditioning (HVAC), lighting, and information and communication technologies (ICT).

A significant highlight of the event was SIBCA's announcement of the Trainovation Fire and Safety Training Academy, a new facility in



Abu Dhabi that is an approved training center under the NFPA Network. This academy aims to equip fire and safety professionals with the essential knowledge needed to protect lives and property. It will offer courses delivered by approved instructors on critical topics such as fire protection, building safety, electrical hazards, and industrial safety, ensuring practitioners in the region are up to date with the latest NFPA codes and standards.

"We would like to thank everyone involved in making the third edition of SIBEC a resounding success. More than just a conference, SIBEC provides attendees with an unparalleled chance to forge connections, pave the way for meaningful partnerships, and directly experience the latest high-quality products and services on the market, all in the interest of improving fire and life safety," said Mr. Ibrahim Lari, Chairman & CEO of SIBCA.

Trend Micro recognized as a leader in 2024 Gartner Peer insights report for network detection and response

Trend Micro Incorporated has earned a customers' choice badge for the Midsize Enterprise in the 2024 Gartner Peer Insights Voice of the Customer for Network Detection and Response (NDR). This recognition underscores Trend Micro's exceptional product performance and unwavering commitment to customer satisfaction.

Trend Micro has been recognized as one of only 9 vendors out of 53 considered and is among just 2 of 53 vendors to receive the "Midsize Enterprise Voice of the Customer" distinction for the \$50M to \$1 billion market segment. This honor reflects a substantial volume of positive reviews, a remarkable "Willingness to Recommend" score of 95%, and high satisfaction with Trend Micro's product capabilities and support experience.

The 2024 Gartner Peer Insights Voice of the Customer for NDR report provides a comprehensive analysis of customer feedback on NDR solutions. It features user reviews and evaluates vendors on product capabilities, support experience, and overall



Dr. Moataz BinAli, Regional Vice President & Managing Director, MMEA, Trend Micro

satisfaction. The report highlights vendors with outstanding ratings and positive customer sentiment, helping organizations make informed decisions in selecting NDR solutions.

"Our recognition with the customer choice

badge from Gartner Peer Insights is more than just an accolade; it is a heartfelt affirmation of the dedication and expertise our team has invested in Trend Vision One," said Dr. Moataz BinAli, Regional Vice President & Managing Director, MMEA, Trend Micro."

Qlik's accelerating growth attracts significant investment from Thoma Bravo and ADIA

Thoma Bravo has signed an agreement to sell a significant minority stake in Qlik, a global leader in data integration, data quality, analytics, and AI, to a wholly-owned subsidiary of the Abu Dhabi Investment Authority (ADIA). As part of the terms of the transaction, Thoma Bravo would remain the majority shareholder and would also make a new equity investment in the company. A consortium of other investors is expected to invest alongside ADIA and Thoma Bravo. This transaction reinforces Qlik's leadership in delivering real-world AI solutions through a flexible, agnostic platform.

Since taking the company private, Thoma Bravo has partnered with the Qlik leadership team to accelerate growth through 14 strategic acquisitions and substantial R&D investments. Qlik serves customers



across a wide range of industries, including healthcare, financial services, retail, and the public sector. Its solutions empower organizations to bring data together, make sense of it, trust it, analyze it, and take action.

The recently launched Qlik Talend® Cloud enables businesses to build a trusted foundation for AI, while Qlik Answers™ brings value to proprietary unstructured data sources by generating relevant answers to questions with full explainability. Qlik's platform supports comprehensive data needs across cloud, multi-cloud, and on-premises environments.

Mike Capone, CEO of Qlik, said, "We look forward to accelerating Qlik's impact in the era of AI and welcome ADIA into our next phase of growth. Our team has seized the AI opportunity, grounded in a commitment to strong partnerships, customer success, and solutions that drive real competitive advantage. These principles have fueled our growth and enabled us to deliver meaningful, tangible value from data and analytics."

Bulwark announces strategic partnership with DNSFilter to enhance cybersecurity solutions

Bulwark Technologies, the leading Cybersecurity specialized VAD, is thrilled to announce a strategic partnership with DNSFilter, a global leader in DNS security and content filtering, to provide enhanced cybersecurity solutions to customers. This partnership will empower organizations to safeguard their networks against evolving online threats through a cutting-edge, cloud-based platform known for its real-time threat detection and intuitive management.

DNSFilter's unique approach leverages artificial intelligence and machine learning to identify malicious domains, block harmful content, and reduce cybersecurity risks. By adding DNSFilter's robust solution to Bulwark cybersecurity offerings, customers will benefit from a reliable, proactive protection against threats such as phishing, malware, and ransomware.

"We're excited to partner with DNSFilter," said Jose Menacherry, Managing Director at Bulwark Technologies. "This collaboration allows us to strengthen our security portfolio and better serve our customers' needs for faster, more



Dan McClean, Director of International Sales, EMEA & APAC and Jose Menacherry, Managing Director at Bulwark Technologies

accurate threat protection."

The partnership aims to provide organizations of all sizes with advanced DNS layer security, enhancing their ability to prevent and respond to potential attacks effectively. Through DNSFilter's innovative technology, which boasts effective threat blocking & world's fastest DNS Solutions, customers can expect a seamless experience that doesn't compromise speed or performance.

"We are thrilled here at DNSFilter on the

announcement of our strategic partnership with Bulwark Technologies. Together, our mutual and unique capabilities will deliver compelling DNS Protective services to their partners and customers throughout the Middle East and beyond," said Dan McClean, Director of International Sales, EMEA & APAC. "Bulwark's established brand and presence in the region, allows us to expand our reach and customer base delivering dependable and necessary security services."

Nutanix unveils new office in Riyadh, symbolizing growth and commitment to Saudi Arabia's digital transformation

Nutanix announces the opening of its new, state-of-the-art office in Riyadh. Situated on the iconic King Fahd Road at Tuwaiq Gate, this expansion highlights Nutanix's continued growth and unwavering commitment to Saudi Arabia's dynamic digital transformation journey.

"Our new office not only reflects our growth but also symbolizes our deep-rooted commitment to supporting Saudi Arabia's digital ambitions," said Talal Al-Saif, Regional Sales Director for Central Gulf at Nutanix. "We are excited to continue our journey in this vibrant market, working closely with our partners and customers to drive innovation and deliver exceptional value across various



sectors."

Spanning three floors and tripling the size of Nutanix's previous workspace, the new office is designed to accommodate the company's robust expansion and provide an enhanced environment for collaboration and innovation.

The office's prime location, named after

the formidable Tuwaiq Mountain—a symbol of resilience and determination as famously compared to the strength of the Saudi people by Crown Prince Mohammad bin Salman—reflects Nutanix's own growth and enduring dedication to the region.

The cutting-edge facility is equipped with the latest technology to support seamless connectivity and collaboration. Nutanix employees will enjoy instant internet access upon entry, and the office is designed for effortless integration with employee cards. Meeting rooms are outfitted with Zoom Rooms, enabling smooth wireless screen sharing and high-definition video collaboration for hybrid teams.

Google Cloud marks first anniversary of Dammam region with summit highlighting growth and AI innovation

Google Cloud marked the first anniversary of the Dammam Cloud Region launch in Saudi Arabia with the inaugural Google Cloud Saudi Arabia Summit. Held at the Four Seasons Hotel Kingdom Tower in Riyadh, the event brought together over 1,500 attendees, including Google Cloud partners, customers, government officials, and industry leaders, to celebrate the achievements of the past year and explore the future of cloud computing and AI in the Kingdom.

The Google Cloud Summit Saudi Arabia underscored Google Cloud's commitment to Saudi Arabia's digital transformation journey and highlighted the significant growth and potential witnessed in the Kingdom's technology landscape.

In his keynote speech, Bader Almadi, Country Manager for Google Cloud in Saudi Arabia, said, "This summit marks a significant milestone in Google Cloud's journey in Saudi Arabia. We are deeply committed to supporting the Kingdom's Vision 2030 objectives by empowering businesses, government entities, and individuals with the transformative power of cloud technology and AI."

Abdul Rahman Al-Thehaiban, Managing



Director, Turkey, Middle East & Africa, Google Cloud, said, "Building on the momentum of our recent announcement with the Public Investment Fund to establish a global AI hub in Saudi Arabia, Google Cloud is dedicated to advancing the Kingdom's position as a leader in technological innovation."

The summit featured an engaging agenda with keynote presentations, breakout sessions, and interactive demos showcasing Google Cloud's latest innovations in AI and data analytics. Prominent businesses like Saudi Airlines, ROSHN, and Almarai shared how they are innovating with cloud technologies and AI.

WSO2 expands executive team to advance customer adoption worldwide

WSO2 has announced the addition of two executives: Jeff Paul and Isabelle Mauny. Together, they will play strategic roles in expanding global adoption of WSO2's offerings via initiatives aimed at customer advocacy, education and counsel.

- Jeff Paul joins WSO2 as senior vice president and global head of sales. He brings more than two decades of technology sales experience, including vice president roles at Red Hat, Intel and IBM.
- Isabelle Mauny rejoins WSO2 as vice president – chief developer advocate. She has 25-plus years of integration and API industry experience, including roles as a 42Crunch co-founder and WSO2 vice president of product management.

Already, thousands of organizations, including



**Jeff Paul, Head of Global Sales,
WSO2**

hundreds of the world's largest corporations, top universities, and governments, rely on WSO2's open source, cloud native solutions to drive their digital transformation efforts—

executing more than 60 trillion transactions and managing over 1 billion identities annually. Using WSO2 for API management, integration, and customer identity and access management (CIAM), these organizations are harnessing the full power of their APIs to securely deliver their digital services and applications.

"We are on a mission to empower enterprises to thrive in the digital economy—supported by our transformative, next-generation technologies and seasoned team of experts," said Dr. Sanjiva Weerawarana, WSO2 founder and CEO. "I'm excited to have Jeff and Isabelle join us in delivering on this commitment. Their deep knowledge of the digital opportunities and challenges facing organizations today will be invaluable in helping customers navigate their transformation journeys."

Epicor accelerates its cognitive ERP leadership with executive appointments

Epicor has announced executive appointments supporting the company's focus in delivering AI-powered cognitive ERP solutions for the make, move, and sell industries worldwide.

Vaibhav Vohra has been named President, building on his current duties as Chief Product & Technology Officer. In his elevated role, Vohra will continue to accelerate industry-focused innovation and digital transformation for Epicor customers, responsible for overall product strategy, development, and design. Since joining Epicor in 2021, Vohra has spearheaded strategic product advancements including introducing the company's AI-infused ERP portfolio tuned to the unique needs of supply chain businesses.

In addition, Arturo Buzzalino has been promoted to Chief Innovation Officer and Group Vice President. In his role, Buzzalino will be focused specifically on driving the company's AI-focused product development initiatives across Epicor AI centers-of-excellence, as well as strategic integration and use of AI technologies across the company.

Scott Morgan has also been hired as Chief Revenue Officer, responsible for leading



Steve Murphy, - CEO, Epicor

Americas sales, global services, and global recurring revenue teams. Morgan brings more than 25 years of software and technology industry experience to Epicor including senior sales and management roles with Infor, Zebra

Technologies, LevaData, and others.

As part of this transition, long-time ERP industry leader Lisa Pope, who has served as President and Chief Revenue Officer since 2017, will be retiring February 2025.

Darwinbox is the first Asia-origin challenger in Gartner's Magic Quadrant for cloud HCM

The Southeast Asia region is witnessing an unprecedented transformation in its workforce landscape, driven by rapid economic growth, a youthful and tech-savvy labor pool, and the increasing adoption of digital solutions. Projected to reach a GDP of \$4.7 trillion by 2025 and home to over 350 million workers, SEA is a thriving hub for growing businesses. Yet, this diversity also brings challenges like navigating complex labor laws, managing geographically dispersed teams, and addressing cultural nuances in the workplace.

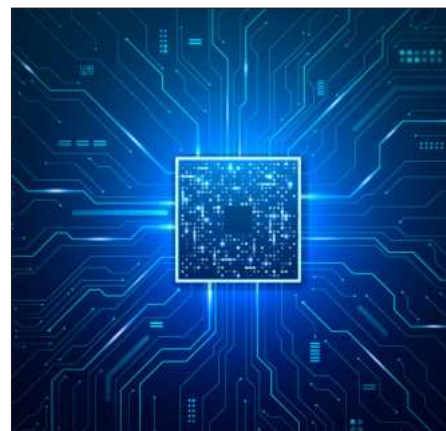
Gartner, a global leader in research and advisory, has long been recognized in evaluating technology solutions. Its Magic Quadrant, a flagship report, is the gold standard for assessing industry players based on their completeness of vision and ability to execute. In the 2024 edition for Cloud HCM Suites for enterprises

with 1,000+ employees, Darwinbox became the first Asia-origin player to be recognized as a Challenger. This milestone underscores Darwinbox's innovation and ability to meet SEA's unique HR needs.

"Our rise to Challenger status is driven by our commitment to building a modern, global HCM platform, supported by AI-driven innovation and user-centric design," said Chaitanya Peddi, Co-founder of Darwinbox. "Our vision has always been to create an agile and adaptable solution that not only meets today's needs but is ready for tomorrow's challenges."

The Dynamics of HR in SEA and the Need for Future Ready HCM Solutions

Southeast Asia's rapid economic growth, fueled by a tech-savvy workforce and a booming digital economy projected to reach \$330 billion by 2025, is reshaping the workforce landscape. While



HR professionals face challenges like complex regulations, a digital divide, and diverse cultural needs, tailored HR tech solutions are unlocking opportunities, with the potential to create 676,000 jobs by 2030.

Omnix International ties-up with Matterport to drive Digital Twin Solutions in the Gulf region

Omnix International has announced a strategic partnership with Matterport, a leading spatial data company driving the digital transformation of the built world. This new collaboration aims to accelerate the adoption of digital twins, creating immersive, high-quality virtual experiences of physical spaces across various sectors, including real estate, construction, hospitality, and insurance, allowing for virtual exploration and remote collaboration.

By combining Matterport's cutting-edge 3D technology with Omnix International's expertise in technology integration, customers are now empowered to make real spaces accessible from anywhere, which can drive sales, enhance customer satisfaction, and streamline operations.

Walid Gomaa, CEO of Omnix International, said, "Our commitment to leading the way in digital transformation is further solidified with our partnership with Matterport. We are excited to offer our customers innovative spatial data solutions that improve accessibility, documentation, and decision-making, while also reducing costs."



Walid Gomaa, CEO of Omnix International, Head of Global Sales, WSO2 and **Nick Halls**, Senior Director for Channel Sales EMEA at Matterport.



"This partnership will combine Matterport's cutting-edge spatial data technology with Omnix's deep industry insights, delivering enhanced solutions for customers focused on Industry 4.0, environmental sustainability, and cross-functional collaboration. As a trusted value-added reseller in the region, Omnix will enable us to make digital transformation more accessible, impactful, and user-friendly," said Nick Halls Senior Director for Channel Sales EMEA at Matterport.

The Middle East is experiencing a growing

demand for digital solutions across various industries. Different sectors are set to benefit from Matterport's technology, with digital replicas for physical spaces aiding in precise visualization and efficient management, which is invaluable for project planning and management.

This partnership aims to target large-scale projects in areas such as real estate development, infrastructure, and smart cities, showcasing the combined strengths of Omnix International and Matterport in delivering high-value digital solutions.

BlueVerve

THE HEARTBEAT OF HEALTHY LIVING



The heartbeat of
healthy living

EMPOWERING CHANNEL PARTNERS FOR SUCCESS

How do you align your channel strategy with your overall business objectives?

Aligning our channel strategy with our overall business objectives requires a clear understanding of both our goals and how our partners can help us achieve them. By segmenting partners effectively, providing the right incentives, offering ongoing support and training, and regularly measuring performance, we can create a channel strategy that is not only aligned with but also actively driving our business objectives forward. This strategic alignment fosters stronger partnerships, increases accountability, and ultimately leads to greater mutual success.

Some of the key drivers would be

Revenue Growth: Expanding sales across existing or new markets

Market Penetration: Gaining a larger market share or entering new geographies or verticals.

Product Launch/Expansion: Introducing new products or services.

Brand Awareness and Loyalty: Increasing recognition and trust in the product offerings. **Customer Success:** Ensuring high customer satisfaction, retention, and advocacy.

What training and enablement programs do you provide to ensure channel partners are up-to-date with your product portfolio?

To keep channel partners up-to-date with our product portfolio, it's essential to offer a multifaceted training and enablement program that provides comprehensive, role-specific learning opportunities, continuous product updates, and easy access to the tools and resources they need to succeed. By combining structured onboarding, specialized training tracks, hands-on experiences, and ongoing support, you can ensure that your partners have the knowledge and skills to effectively sell, support, and grow with your products. Foster a sense of collaboration among your partner ecosystem and build a knowledge-sharing environment. Creating online communities where partners can share insights, ask questions, and discuss product-related topics. Peer-to-peer support can often help partners stay current with product knowledge and best practices, something that has really worked well for Nutanix is detailed sales playbooks that guide partners through the sales process, from prospecting to closing deals. Include common objections, product positioning, competitive differentiation, and pricing information.



Shaista Ahmed
Director Channel
Nutanix

What makes your channel program stand out from competitors?

Nutanix provides partners with a unified program designed to deliver a sustainable and profitable business model. With the Elevate Partner Program, we drive a partner-centric approach, ongoing training, stackable incentives, advanced enablement tools, and collaborative marketing opportunities paired with a focus on customer success and data-driven insights. This helps us create an environment where partners feel supported, valued, and empowered to drive significant business results. We also enable our partners to provide customers a single platform to run all their apps and data across multiple cloud environments efficiently and cost effectively.

By building their business with Nutanix, partners can tap into a leading hybrid multicloud platform that delights customers, brings ample front and back-end profitability, and makes it easy for partner organization to learn, market, and sell Nutanix through seamless partner tools and resource

What emerging technologies or trends should channel partners adopt to remain competitive?

The channel industry especially in the context of technology distribution and partnerships is facing a dynamic set of trends and challenges. Being able to anticipate and navigate these shifts will be crucial to staying competitive and fostering long-term growth. Trends that will shape the future of our business are Digital Transformation and Cloud Migration, AI and Automation Integration, Increasing Focus on Cybersecurity, Navigating Global Market Instability and Geopolitical Risks. The future of the channel sector is shaped by rapidly evolving technologies and changing market dynamics, the key to success will lie in adapting quickly to these trends, investing in innovation, and building resilience against challenges like talent shortages, market instability, and evolving customer expectations. By embracing a mindset of continuous learning, data-driven decision-making, and collaboration, Channel partners can adopt some of these best practices & thrive in an increasingly competitive and complex environment.

How can vendors and partners collaboratively integrate AI, cloud, or IoT solutions into the ecosystem?

There are many emerging technologies that are gaining huge momentum, Like AI, Machine learning, Edge computing, Microservices architecture, Hybrid multicloud, Cloud Native deployment etc. These emerging technologies play a significant role in shaping the future of cloud and software development, driving innovation, efficiency, and scalability in the industry. The technology landscape is dynamic, and at Nutanix we continue to evolve our offerings to address emerging trends and technologies. Supporting per customer to build solutions around Hybrid and Multi-Cloud, Kubernetes and containers, automation & Hybrid and Multi-Cloud, Kubernetes and containers, automation & Orchestration, security & Compliance, Data management & Edge computing, but we are so obsessed with customer success we want to help our partners provide the best available solution so we have partners with over 700 alliances Worldwide that can help customers get the best solution

What new frameworks or best practices can ensure the long-term success of channel partners?

Ensuring the long-term success of channel partners requires a comprehensive approach that focuses on strengthening the relationship, improving collaboration, and providing the necessary tools, resources,

“We drive a partner-centric approach, ongoing training, stackable incentives, advanced enablement tools, and collaborative marketing opportunities paired with a focus on customer success and data-driven insights.”

and incentives. The traditional “vendor-seller” model is evolving, successful long-term partnerships are often based on co-creating value, a developed tiered training approach, provide a unified dashboard that aggregates key metrics and performance data, allowing partners to see how they are performing and identify areas for improvement.

Enabling Incentive programs that align with both short-term and long-term goals including rebates, loyalty programs, or access to exclusive resources and marketing events

Focus on establishing a channel management process that is agile and can quickly adapt to new challenges, whether they be market disruptions, competitive threats, or new opportunities. Ultimately developing long-term strategic partnerships not just transactional relationships- partnership focused on more than just revenue generation will help create mutual long-term value through shared goals, visions, and investments.

How can vendors facilitate better onboarding and development journeys for new partners?

A well-executed onboarding process helps partners quickly understand our business, products, and expectations. A structured development journey ensures they are continuously supported as they grow. We need to be clear about the level of commitment, performance, and goals that is expected from new & existing partners. This could include sales targets, training completion, certification requirements, & marketing participation. Building an ecosystem of knowledge-sharing, trust, and alignment with our partners will not only improve short-term performance but also foster long-term, mutually beneficial relationships. The goal is to equip your partners with the resources, training, and support they need to grow, so they can help drive our business forward and be a true representation of Nutanix in the market. 🔥



Dell targets strategies for collaboration, growth, and innovation

How do you align your channel strategy with your overall business objectives?

Investing in partners remains a core priority for Dell Technologies. With our business roughly 50/50 split between Direct and Channel sales, partners are integral to extending our sales force, expanding our reach, and growing our customer base. Over the past year, we've deepened our commitment to the value partners bring to our go-to-market engine. We've focused on driving greater alignment between our sales teams and partners to enhance collaboration and maximize impact. To support this, Dell established partner ecosystem leaders in every region, creating more visibility, engagement, and enablement at the regional and country levels across all partner types. This has resulted in stronger collaboration and a unified approach to serving customers.

In alignment with customer priorities, we're also investing in key growth areas, further incentivizing new business acquisition, and setting clear expectations to achieve mutual success. As we move into the new year, our strategy will continue to prioritize close collaboration and joint execution, ensuring that we deliver exceptional value for our customers. Together, we're reimagining what's possible. The opportunities before us are vast, and by working hand in hand, we can achieve remarkable outcomes. When our customers and partners win, we all win.

What training and enablement programs do you provide to ensure channel partners are up-to-date with your product portfolio?

At Dell, we prioritize strengthening collaboration and streamlining the partner experience. Over the years, we've enhanced our training and enablement initiatives, and as part of the 2024 Dell Technologies Partner Program this was reflected through our continued investment in partner collaboration through a Partner First Strategy for Storage and expanded Server PoR (Proof of Resale) eligibility.

We've also made significant IT investments to enhance the digital partner experience. This year, these efforts come to life with online quoting and ordering tools, offering streamlined, self-serve capabilities that modernize workflows, improve transparency, and empower partners with future-ready tools to help unlock profit potential.

As customer priorities evolve, competencies and partner certifications will play a vital role in our program. We'll continue to align our enablement resources with future customer needs, and equip partners with the skills, tools, and support needed to stay current with our product portfolio and maximize their growth potential.

What makes your channel program stand out from competitors?

Dell has one of the largest, most diverse partner ecosystems in the industry and we're committed



Walid Yehia

Managing Director
Dell Technologies

“

With the industry's broadest AI solutions portfolio—spanning desktop to data center to cloud—Dell is empowering partners to capitalize on a once-in-a-generation transformation, backed by the right AI tools, services, and optimized sales strategies.

”

to the power of partnership.

This is especially significant in the AI era, with this ecosystem becoming more critical than ever, presenting unparalleled opportunities for partners to grow across all areas of their business. With the industry's broadest AI solutions portfolio—spanning desktop to data center to cloud—Dell is empowering partners to capitalize on a once-in-a-generation transformation, backed by the right AI tools, services, and optimized sales strategies.

Central to this is the Dell AI Factory, which is our comprehensive approach to accelerating AI innovation for organizations of all sizes. It offers a portfolio of products, solutions, and services optimized for AI workloads, acting as a vehicle for opportunity by helping customers realize value, eliminate complexities, and standardize on strategic architectures tailored to their needs. Beyond technical capabilities, the AI Factory supports efficient IT operations and sustainable AI initiatives, enabling customers to achieve their goals with circularity in mind.

For partners, the opportunities are vast—similar to running a physical factory, an effective AI factory requires expertise in strategy, implementation, management, and scaling. These areas allow partners to integrate their services seamlessly with the AI Factory to drive customer success. Through the AI Focus Partner Network, Dell connects partners with established AI practices to our sales teams, offering access to roadmaps, validated designs, training, labs, and other resources. We've seen partners leverage our resources in the AI Network to build out their own solutions powered by the Dell AI Factory. This game-changing, end-to-end framework makes AI deployment scalable, repeatable, and ready for the future.

What emerging technologies or trends should channel partners adopt to remain competitive?

In addition to AI, emerging technologies such as multicloud, security, storage, and edge computing are reshaping the IT and business landscape, presenting both challenges and opportunities. To remain competitive, it is essential for partners to align their strategies with these transformative trends. The increasing adoption of AI, for example, is driving a significant need for robust and scalable storage solutions, highlighting the importance of investing in advanced infrastructure to support data-intensive workloads. Dell's Partner First Strategy for Storage, launched over a year ago, exemplifies how embracing these shifts can yield significant advantages. The strategy, which emphasizes the critical role of partners in driving storage solutions, has demonstrated substantial success in the market.

By focusing on these key growth areas, channel partners can position themselves as valuable enablers of business transformation. Building expertise in these domains allows partners to deliver outcomes that address the evolving needs of customers while also unlocking new revenue streams.

How can vendors and partners collaboratively integrate AI, cloud, or IoT solutions into the ecosystem?

Vendors and partners can collaboratively integrate AI, cloud, and IoT solutions into the ecosystem by focusing on flexible, scalable, and cost-effective strategies tailored to evolving customer needs. As the majority of data and AI initiatives continue to be hosted on-premises, there's a clear trend towards localized AI workloads. While many organizations begin their AI journey in the public cloud due to ease of access, scalability challenges arise as the number of POCs grows, prompting the need for hybrid or on-premises solutions. Flexible, open environments are critical for customers to test, refine, and scale their models securely while

optimizing costs. On-premises solutions, for example, have shown the potential to offer a cost-effective alternative to public cloud models.

Cloud integration also requires addressing customers' virtualization modernization strategies. Many organizations are exploring alternative hypervisor options and seeking optionality in their infrastructure. Collaborative efforts between vendors and partners can support these transformations by offering common infrastructure layers that manage varied hypervisor environments efficiently. These layers enable customers to consolidate infrastructure while simultaneously addressing multiple use cases, such as AI, IoT, and cloud-native applications.

Strategic partnerships play a crucial role in this ecosystem. Whether through public, private, or multicloud approaches, the focus remains on equipping partners to bring maximum value and flexibility to customers, ensuring long-term innovation and success.

What new frameworks or best practices can ensure the long-term success of channel partners?

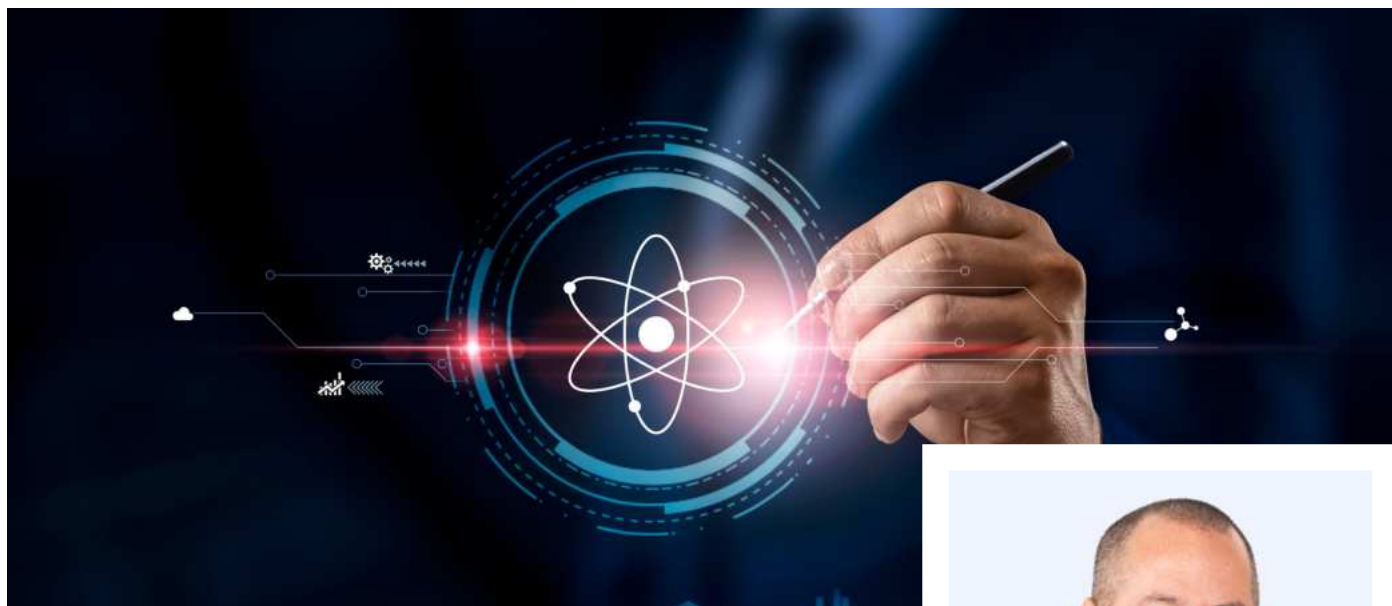
Investing in partners is essential for securing long-term success, with a strong emphasis on modernizing the partner experience as a key driver. Channel partners play a critical role in delivering innovative solutions aligned with evolving market demands, and adopting partner-centric strategies is vital to success. Simplified and transparent engagement frameworks, coupled with clear incentive structures, reduce complexity and allow partners to focus on delivering exceptional customer experiences.

Continuous investment in enablement and training also ensures partners are equipped with the expertise to remain competitive and effectively deliver emerging technologies like AI, multicloud, and edge solutions. Collaborative solution development and ecosystem building further amplify success, enabling partners to co-create integrated offerings that address diverse customer needs. By fostering long-term relationships and shared growth, this approach ensures partners can thrive while meeting the dynamic demands of the market.

How can vendors facilitate better onboarding and development journeys for new partners?

The IT industry can significantly enhance partner onboarding and development by adopting a structured and supportive approach. Comprehensive onboarding programs that provide step-by-step guidance and centralized resource hubs can help new partners quickly access the tools and knowledge they need to succeed. Tailored training programs, offered in diverse formats such as online modules, in-person workshops, and webinars, can help ensure that partners receive role-specific education and certifications to meet evolving market demands. Dedicated support through account managers and regular check-ins helps foster a sense of partnership, offering personalized assistance to address challenges and opportunities.

Strong communication channels are also equally vital, enabling seamless collaboration and the exchange of best practices. With vibrant partner communities, platforms can be used for networking and knowledge sharing, while active feedback loops can help programs remain responsive to partner needs. By continuously assessing partner-focused strategies, the IT industry can create a dynamic, collaborative ecosystem that drives mutual growth, innovation, and success. 



AI, Quantum, Digital Cloning- some of the biggest cybersecurity trends we can expect in 2025

As 2025 approaches, we indulge in the traditional New Year habit of future-gazing. In cybersecurity, we know planning is everything. We know to be forewarned is to be forearmed. At Dubai's GITEX Global 2024 in October, we heard familiar warnings of escalating threats. Several ransomware groups, including Lockbit 3.0 and Rhysida, had been found aggressively targeting the region.

Meanwhile, AI is, in many respects, a boon to businesses but in the wrong hands has been feared to also be a bane. As we shall see, however, much of this fear has been unfounded. As the years progress, industry experts also continue to fret over the implications of quantum computing. So, as in previous festive celebrations, Middle East CISOs and their teams enter the new year on a knife edge, looking to protect environments that are more vulnerable from an attack landscape that is more sophisticated. Let's delve into nine developments that are sure to shape the security industry in 2025.

CISOs enjoy a tentative "phew" moment over the AI threat

Some industries have undoubtedly benefitted from AI. But outside of these specific use cases, even the benefits of the GenAI technologies that made such headlines in the previous two years are now being seen in some quarters as overblown. In 2025, expect to see businesses return to more proven narrow-AI use cases to restore predictability to the ROI of AI projects. Automation and the upskilling of business functions are likely to be among the most common implementations. In parallel, we can expect threat actors, in an attempt to minimize their costs, return to using narrow AI to soften entry barriers. The fear of generative AI catalyzing a volume explosion in targeted, bespoke attacks is therefore unfounded.

Quantum creep

Previous estimates suggest that where a digital machine would take 300 trillion years to crack 2-megabit RSA encryption, a 4,099-qubit quantum computer would only need 10 seconds. This post-quantum reality could be with us by the early 2030s, so we will



Morey Haber
Chief Security Advisor
BeyondTrust

probably continue to see individuals and organizations urge action on this critical future problem because of the implications it has for societies. We could see critical-infrastructure organizations, such as regional banks, telcos and government agencies, form exploratory committees to examine NIST's post-quantum encryption standards. These will be important first steps on the long road to adoption — a road that is likely to be signposted with many new regulatory standards built around post-quantum cryptography.

Farewell Windows 10

October 2025 will see end-of-life (EoL) announcements for Microsoft Windows 10. Only the most recent machines — those that have both Secure Boot and TPM (trusted platform module) will be eligible for Windows 11 upgrades, meaning everyone else will lose access to updates, including security patches. If this sounds like a recipe for vulnerability that is because it is. Expect to see a fire sale of obsolete PCs in the second half of 2025. The forced obsolescence will be good news for the hardware market, however, especially ARM, which will likely see a volume shift to its mobile-friendly processors. Alternative OSes like Linux and Ubuntu will also benefit from organizations trying to minimize replacement costs.

Digital cloning

Breach data repurposed to create fake online personas. It is a new approach to identity theft called “reverse identity theft”, in which an identity is linked to another without the knowledge of the legitimate party. Campaigns are already underway to merge fictitious data with legitimate data, especially where names are common. We can expect this to escalate in 2025.

Nation vs nation: the critical infrastructure problem

As regions like the GCC build their national infrastructures in line with economic-diversification “Vision” programs, critical infrastructure sectors like healthcare and finance will be shiny objects for threat actors, especially those backed by nation states. In cyberwarfare, critical infrastructure is the first target and legacy systems are the most tempting. In 2025, government funding for cybersecurity will concentrate on boosting the cyber-maturity of critical-infrastructure organizations as they continue to merge their OT and IT environments.

Chancing in the moonlight

With its large expat populations, the GCC may come to experience overemployment, with residents taking on multiple remote jobs. While many regional employment contracts explicitly prohibit it, the workers that choose to operate this way will be tempted to outsource some of their workload to AI. This is likely to occur under the employer's radar and may include the creation of fake employees. Such moonlighting will give rise to more shadow IT and all the security implications it implies, as well as legal issues surrounding content creation that failed to observe risks such as plagiarism.

Guarding the Paths to Privilege

As identity compromises increase in frequency, 2025 will be the year CISOs begin to consider the Paths to Privilege™ that allow lateral movement — the insidious practice of gaining increasingly greater access rights. Privilege escalation is an issue that must be addressed through rigorous examination of trust relationships, configurations, and the processes by which entitlements are granted. Attackers are

adept at manipulating cloud permissions, roles, and entitlements. Their attacks are preventable through a thorough re-evaluation of hygiene.

Too many tools

Cybersecurity investments will continue to favor multiple point solutions that do not play well together. This will lead to detrimental effects on reporting and visibility, and security teams will bear the brunt — more gaps, more vectors, more paths to privilege.

Cyber-insurance — some changes

The way cyber-insurance providers calculate risk will see some changes in 2025 to factor in AI and quantum computing. Expect to see more “acceptable use” clauses regarding these technologies and get ready for a long hunt for policies without such restrictions or without exclusions for incidents where either AI or quantum computing are involved in a breach.

Prepare for a bumpy ride

Threat actors are not waiting. They are not trend-watching. They are creating the trends. Defenders must create some trends of their own or invite disaster. They should make cyber hygiene their New Year's resolution. 🏹

“In 2025, government funding for cybersecurity will concentrate on boosting the cyber-maturity of critical-infrastructure organizations as they continue to merge their OT and IT environments.”

SIMPLIFIED CYBERSECURITY BY CORO

Piers Morgan, SVP & General Manager for EMEA, shares insights on Coro's cybersecurity vision and its strategic investments in digital transformation



Piers Morgan

SVP & General Manager-
EMEA

How is Coro tailoring its solutions to address the specific needs of businesses in the region?

The beauty of Coro lies in its modular design, enabling our platform to be custom-tailored to meet the unique needs of any business, regardless of location. In the Middle East, this means providing scalable, AI-driven cybersecurity solutions that ensure compliance with regional regulations while adapting to the specific demands of businesses as they grow and navigate an ever-changing threat landscape.

Are there any sectors in the Middle East where you see particularly strong potential for growth?

The Middle East's finance, healthcare, and government sectors are experiencing rapid digital transformation, making them prime targets for cyberattacks. Notably, the average



cost of a cyber incident in the region has escalated to \$8.75 million, nearly double the global average.

Particularly in Saudi Arabia, with the Saudi Vision 2030 initiative and increased investment in digital transformation, tech-driven SMBs are rapidly adopting new technologies, creating a growing demand for cybersecurity solutions to safeguard their operations.

Coro's AI-driven cybersecurity platform offers robust, scalable protection that aligns with these regulatory standards, ensuring compliance and security for organizations in these sectors. By providing comprehensive solutions that adapt to evolving threats, Coro empowers Middle Eastern organizations to confidently pursue digital transformation while safeguarding their operations and data.

What are the top cybersecurity challenges SMEs in the Middle

East currently face?

Similar to SMEs globally, businesses in the Middle East face challenges like:

- A lack of dedicated IT security resources.
- Managing increasingly sophisticated threats like ransomware and phishing.
- Ensuring compliance with local and international regulations.
- Limited cybersecurity budget

Coro's solutions directly address these issues with automation, affordability, and simplicity.

How does Coro's solution simplify cybersecurity for resource-constrained SMEs?

Answer: Coro automates 95% of cybersecurity tasks, reducing the need for constant manual intervention. Our platform is designed to provide comprehensive protection across devices, email, and cloud apps, enabling SMEs to focus on their

business without needing a dedicated security team.

What sets Coro's channel partner program apart from others in the cybersecurity industry?

What sets Coro's channel partner program apart is its unwavering focus on partner success. It's not just about offering a program—it's about fostering true partnerships. With dedicated support, simplified processes, and real investment in partner growth, Coro ensures its partners have everything they need to thrive. Here's how the program stands out:

- **Scalable Revenue Opportunities:** Coro's straightforward pricing models and flexible solutions help partners maximize profitability while addressing a wide range of customer needs.
- **Ease of Implementation:** The platform is designed for quick deployment and effortless management, making it simple

for partners to deliver value to their customers without added complexity.

- **Unmatched Support:** Coro prioritizes our partners success by providing a robust suite of resources, including training programs, enablement tools, and co-marketing initiatives, all supported by exceptional service. Partners also gain access to a dedicated partner portal and marketing development funds to create impactful campaigns and drive business growth.
- **Partner Brand Investment:** Coro

invests in our partners' brands through co-marketing initiatives, tailored campaigns, and resources to boost market presence and drive demand.

How does Coro empower its channel partners to drive growth and offer value to end customers?

Coro provides a highly intuitive platform that's simple to sell and deploy, minimizing the learning curve for partners. This allows them to focus on delivering exceptional

value to their customers. Additionally, Coro's partner portal offers extensive resources, training, and support to drive partner success.

What role does the partner ecosystem play in Coro's strategy for the Middle East market?

The partner ecosystem is central to Coro's strategy in the Middle East. Partners play a key role by combining their market expertise with Coro's automated, comprehensive cybersecurity platform. Through co-marketing, enablement, and generous incentives, Coro empowers partners to drive growth while providing scalable, affordable cybersecurity to end customers.

How does Coro anticipate the cybersecurity threat landscape evolving in 2025?

As AI-driven threats become more prevalent, Coro anticipates a significant rise in hard-to-detect attacks targeting small and medium-sized businesses. To counter these evolving tactics, leveraging AI-powered solutions will be essential for proactively identifying and neutralizing threats before they cause harm.

What emerging threats should SMEs in the Middle East be prepared for?

SMEs in the region should prepare for:

- AI-powered phishing and ransomware attacks.
- Supply chain attacks targeting smaller vendors to infiltrate larger organizations.
- Increased insider threats as remote work continues to evolve.

Coro's proactive, automated solutions are designed to address these challenges before they impact businesses.

How is Coro helping SMEs build resilience against increasingly sophisticated cyberattacks?

Answer: Coro empowers SMEs by automating threat detection and response, ensuring 24/7 protection without requiring extensive IT resources. Our platform also provides actionable insights and compliance support to help businesses secure users, devices, networks, email, cloud, and data - all through a single pane of glass and a single endpoint agent. 🔴

“

Coro's AI-driven cybersecurity platform offers robust, scalable protection that aligns with these regulatory standards, ensuring compliance and security for organizations in these sectors.

”



The AI Times

INSIGHTS FOR A SMARTER WORLD



Deepfakes and identities in financial institutions

With the financial sector in the Middle East experiencing unprecedented digital transformation, the potential misuse of deepfakes for fraud and cybercrime poses serious concerns. At the forefront of this conversation, Dr. Joye Purser, CISSP, PhD, Global Field CISO, and Johnny Karam, Managing Director & Vice President of International Emerging Region at Veritas Technologies, provide expert insights on the impact of deepfakes in the region.

How do you see the growth of deepfake technology in the GCC/Middle East financial sector? Can you provide specific cases, even if anonymized, where deepfakes have been used to perpetrate fraud in this region

Joye Purser: Yes, globally there have been notable cases where deepfake technology was used to perpetrate fraud. For example, instances where audio deepfakes were used to mimic the voices of CEOs to authorize fraudulent transactions. Globally, the 'wake up call' occurred when the Hong Kong bank employee was duped following a deepfake video conference call with company executives. While specific cases in the GCC/Middle East region may not be publicly documented, the potential for such occurrences is real and growing. While the technology itself is advancing rapidly and could be used for innovative applications, the financial sector is particularly concerned about its misuse for fraudulent activities.

Globally, the number of deepfake incidents surged tenfold from 2022 to 2023. Specifically, the MEA region saw a 450% increase in such cases, highlighting the rising threat. According to a recent report from McKinsey, GCC financial institutions are poised to continue their growth trajectory by further digitizing their offerings and focusing on the customer experience. In turn, the region's financial institutions are investing in advanced cybersecurity measures and collaborating with technology providers to stay ahead of potential threats. Another important measure to counteract this threat technique is better training, tailored for specific employee groups. Executives, human resources and contracting staff, as well as help desks, have been the targets of specific attacks in recent years. They should be informed about these attack techniques and have annual training that incorporates recent lessons learned. Building awareness of 'warning signs' or 'red flags' of bad actors is extremely important. Veritas Technologies is committed to helping these institutions manage and protect their data, ensuring that they have the tools necessary to detect and mitigate the risks posed by deepfake technology.

How significant is the market for deepfake technologies in the Middle East? What level of investment or expansion are companies in this



Johnny Karam
Managing Director & Vice
President of International
Emerging
Veritas Technologies,



Dr. Joye Purser
CISSP, PhD
Global Field CISO

sector experiencing? Are there specific figures or trends you can share to demonstrate the growth of this industry?

Johnny Karam: The market for deepfake technologies in the Middle East is experiencing significant growth, reflecting global trends. The deepfake AI market, which is globally projected to grow from approximately USD 564 million in 2024 to over USD 5.13 billion by 2030, is expanding at a compound annual growth rate (CAGR) of 44.5%. In the Middle East and Africa (MEA) region specifically, the market is expected to see substantial expansion, driven by increasing digitalization and the adoption

of advanced AI technology, especially in the Banking sector.

A key indicator of this trend in the region is the substantial increase in digital banking services in the UAE, where usage of digital channels has increased by 100% since May 2023. This surge underscores the rapid adoption of digital technologies, including AI and deepfake detection systems, as part of a broader push toward digital transformation.

Companies in the MEA region is significantly investing in detection and prevention systems to address the risks associated with deepfake technologies. This investment is particularly critical in

the BFSI sector, where the need to protect against sophisticated cyber threats, such as identity fraud, is paramount. For example, in the UAE, the 2023 LexisNexis® True Cost of Fraud™ Study found that for every dirham lost to fraud, companies incur an additional cost of AED 4.19. Furthermore, 42% of UAE companies reported an increase in fraud over the past year, with digital channels now accounting for the majority of fraud losses in the region.

Significantly, the study also revealed that digital channels now account for 52% of overall fraud losses in the region, surpassing physical fraud for the first time. This shift underscores the growing threat posed by cybercriminals who exploit the anonymity of digital, cross-border transactions to carry out sophisticated fraud schemes.

As digital communication and social media platforms proliferate, the potential for misuse of deepfake technology increases, necessitating robust measures to manage these risks. This dual focus on innovation and security is driving the growth of the technology to tackle deep fake attacks in the region.

How can financial institutions in the region collaborate with regulators to develop effective safeguards against deepfake-based financial crime?

Johnny Karam: Financial institutions typically have some of the most mature security programs relative to other industries, as they hold such huge sensitive data sets, with considerable regulatory and compliance requirements locally and globally. Collaboration between financial institutions and UAE regulators is crucial for developing robust safeguards against, both deepfake-based attacks and the next generation of attack methodologies. This can be achieved through regular dialogue, joint workshops, and the establishment of industry standards for the detection and prevention of deepfake and other forms of fraud. Financial institutions can also share best practices and threat intelligence with regulators to enhance the overall security posture of the sector.

Moreover, aligning these collaborative efforts with the existing legal frameworks in the UAE, such as the UAE Penal Code and Cybercrimes Law, can enhance



the effectiveness of these safeguards. These laws already penalize actions like defamation and fraud conducted through digital means, including deepfakes, providing a foundational legal recourse that institutions can leverage.

Additionally, with the use of DIFC Data Protection Regulations and amendments, financial institutions can ensure their practice aligns with legal requirements while addressing the risks posed by emerging technologies like deepfakes. For example, recent amendments to Article 10 of the DIFC Data Protection Regulations have been made to capture AI-related developments.

Veritas Technologies supports this collaborative approach by providing advanced data security and management solutions that help institutions comply with these regulatory requirements and mitigate risks effectively.

Are you aware of any current or proposed regulations in the Middle East that address the use of deepfakes in the financial sector?

Johnny Karam: While specific regulations targeting deepfake technology in the financial sector may still be in the developmental stages, there is a growing awareness among regulators in the Middle East about the need to address this emerging threat. Countries in the region are actively working on enhancing their cybersecurity frameworks and may soon introduce regulations that explicitly cover the use and misuse of deepfakes.

For instance, while the ADGM and

DIFC have not issued laws explicitly regulating AI, amendments have been made to existing data protection legislation, such as the DIFC Data Protection Regulations, to capture AI-related developments. Additionally, in 2023, the ADGM and Mohamed bin Zayed University of Artificial Intelligence (MBZUAI) signed a Memorandum of Understanding to advance the role of AI in achieving regulatory outcomes within the financial services sector.

In Mainland UAE, there is no single law or regulation directly regulating AI; rather, there is a patchwork of decrees and guidelines issued over time. The AI Office, for example, has published a series of non-binding national guidelines, including the Deepfake Guide (2021), which provides advice on protecting against deepfakes and guidance on reporting them to the appropriate authorities. Organizations must continue to closely monitor regulatory developments and implement solutions that help financial institutions stay compliant and secure. Veritas Technologies remains committed to supporting financial institutions in navigating these evolving regulatory landscapes.

What are the unique challenges and opportunities that deepfakes present for financial institutions in the region?

Joye Purser: Deepfakes present several unique challenges for financial institutions, including the risk of sophisticated fraud, reputational damage, and the erosion of

trust among customers. However, they also offer opportunities for improving customer engagement and personalization through advanced technologies, provided they are used ethically and responsibly. Financial institutions can leverage deepfake detection technologies and partner with experts like Veritas Technologies to turn these challenges into opportunities, enhancing their security measures while exploring innovative uses of the technology.

Could deepfakes be used to create synthetic identities for Know Your Customer (KYC) compliance purposes, raising ethical concerns?

Johnny Karam: Yes, deepfakes could potentially be used to create synthetic identities, posing significant ethical and security concerns for KYC compliance. This could lead to financial fraud, money laundering, and other illicit activities. Financial institutions must implement robust identity verification processes and leverage advanced technologies to detect and prevent the use of synthetic identities. Leveraging the customer-employee relationship can act as a necessary tool in protecting against deepfakes, by inducing the human element into the verification processes.

and machine learning become increasingly integral to IT strategies, Riverbed continues to enhance its machine learning algorithms to provide more accurate predictions and forecasts, helping organizations better prepare for future changes in their IT landscape. 🔴

Alteryx appoints Andy MacMillan as chief executive officer



Andy MacMillan, Chief Executive Officer
Alteryx

Alteryx has appointed Andy MacMillan as Chief Executive Officer (“CEO”). In his new role, MacMillan will drive Alteryx forward in its mission to empower organizations to turn their data into insights and deliver better business outcomes.

“Andy’s capabilities and past leadership success in leveraging AI to drive product innovation and developing high-performing teams at scaled enterprise software companies aligns well with our investment thesis, and we believe his leadership will help propel the Company to new heights,” said Prashant Mehrotra, Partner at Clearlake. “We look forward to partnering with Andy and the rest of the team to support Alteryx in delivering new products and increased value to customers as it continues to enhance its AI-driven analytics cloud platform.”

Deven Parekh, Managing Director at Insight Partners, said, “The Alteryx team is incredibly excited to welcome Andy as CEO. His wealth of experience, paired with his empathetic approach to leadership and deep enterprise software industry knowledge, will forge a new path to success. We can’t wait to see what Andy

will achieve at Alteryx.”

With more than 20 years of leadership experience in the tech industry, MacMillan joins Alteryx from UserTesting, where he served as CEO. He also spent time as the Chairman and CEO of Act-On Software, helping to transform the company’s product portfolio. Previously, he held several positions at Salesforce, including leading its Data.com division, and also served in product leadership roles at Oracle and Stellent.

Among MacMillan’s top priorities in his new role will be accelerating Alteryx’s innovation in its core platform and supporting the development of additional AI capabilities. He is also committed to building on the Company and customer culture that has created a community of more than 600,000 members.

“Great companies are built on the foundational pillars of company culture and customer-centricity, and I’m delighted to join a company that follows this same philosophy,” said MacMillan. “Together with the team, we’ll lead Alteryx into its next phase of growth and product innovation to help our customers succeed in their analytics journey.”

Fugro appoints Annabelle Vos as group director Middle East & India



Annabelle Vos
Group Director,
MEI Fugro

Nutanix has named Chris De Vere as its new EMEA Managed Service Provider (MSP) Leader, effective August 1. Chris will oversee the MSP Sales and Business Development team, including existing members and new hires as part of FY25’s headcount expansion.

The appointment is part of Nutanix’ consolidation of its MSP sales efforts and resources in EMEA following its EMEA Channel organisation. The changes will support accelerated development of Service Provider opportunities with Account Executives as well as better handling of ecosystem requirements for the MSP Channel, such as developing Nutanix’ Service Provider Aggregator ecosystem.

“I feel in good company and I am very happy to be here,” commented Chris. “I look forward to building an MSP team and practice that will not only deliver incremental success to Nutanix, but also inspire innovative thinking and partnerships.”

Chris joined Nutanix recently from a 13-years spell at VMware. In his final role there, he was responsible for VMware’s MSP SaaS business across EMEA. Prior to VMware, he spent 11 years at IBM. Chris lives in the South of England, is married with a grown-up daughter. His main interests outside of work are motor boating across the South Coast of England.

What 2025 holds for channel partners



Sehrish Tariq
Assistant Editor
GEC Media Group

As artificial intelligence continues to dominate conversations in the technology, 2024 marked a significant turning point in the adoption and proliferation of Generative AI tools. This shift, while dominant, has left many enterprises cautiously assessing their readiness to adapt this transformative technology fully in the coming year.

The global IT landscape is poised for notable growth despite new economic and political uncertainties following the 2024 global elections super-cycle. Canalys' recent IT Opportunity update projects an 8.3% rise in worldwide IT spending for 2025, setting the stage for a market worth an impressive US\$5.44 trillion. This growth marks the beginning of a new AI-driven era that is expected to unlock long-term opportunities for technology channel partners.

While the overall IT market is set for expansion, partner-delivered IT services are anticipated to grow at a slightly slower rate. However, this doesn't diminish the critical role of partners in shaping IT spending decisions worldwide. After a period of stagnation and declines, spending in essential hardware categories, such as PCs, networking, storage, and servers, is predicted to rise once again. This resurgence will largely be


driven by the need for refreshes and upgrades within the installed base.

Despite the cyclical nature of hardware investments, the consistent growth areas for the channel lie in cybersecurity, software, and managed IT services. These domains are expected to act as robust growth engines over the long term. Channel partners that have prioritized and heavily invested in these segments are well-positioned to sustain their upward trajectory and capitalize on emerging opportunities.

The road to 2025 presents challenges and opportunities in equal measure. Enterprises and their channel partners must remain agile while technology plays its game. 🔥

www.futureitsummit.com

Unveiling the future at
#futureitsummit

A stylized white graphic element consisting of several nested, angular shapes that form a larger, abstract 'F' or a series of steps, positioned to the left of the main title.

FUTURE IT SUMMIT 2025

UAE - 18 FEB • KSA - 24 FEB • SINGAPORE - 24 OCT
INDONESIA - 27 OCT • MALAYSIA - 29 OCT • INDIA [MUMBAI] - 12 NOV
INDIA [BENGALURU] - 14 NOV • KENYA - 19 NOV



THE
WORLD
CIO 200
SUMMIT

2025 ROADSHOW

APRIL-SEPTEMBER 2025

BOLD. UNSTOPPABLE.