ISSUE 94 | APRIL 2025

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

THE CYBER SHIELD OF THE GULF

tahawultech.com

cnme computer news middle east
SUPPLEMENT

Delinea

Securing identities at every interaction

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

- Secure Credentials
- Privileged Remote Access
- Privilege & Entitlement Elevation
- Identity Threat Protection
- Identity Governance

Follow us on

delinea.com

EDITOR'S NOTE

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

Sandhya DMello
Editor

CYBER RESILIENCE TAKES CENTER STAGE IN A RAPIDLY EVOLVING DIGITAL WORLD

In an increasingly complex and interconnected digital world, April's issue of *Security Advisor Middle East* underscores a pivotal truth—cyber resilience is no longer a luxury, but a necessity.

Our cover story, *The Cyber Shield of the Gulf,* dives deep into the UAE's cybersecurity evolution. Yahya Kassab from Commvault offers timely insights on the region's shift from disaster recovery to cyber resilience—timely advice as AI, hybrid cloud, and critical infrastructure converge.

As we spotlight World Backup Day, we're reminded that resilience starts with awareness. With 87% of users actively backing up data, according to Western Digital's survey, the momentum is clear—but the challenges remain. This issue celebrates both the commitment and the caution that mark today's digital strategies.

This month's news highlights critical developments across the cybersecurity landscape. A vulnerability found in multiple D-Link router models prompts a vendor advisory to upgrade to safer alternatives.

DIGITAL DEFENSE RISING STRONG

Google Cloud deepens its cybersecurity partnership with Atlético de Madrid, enhancing data protection for both men's and women's teams. Cloudflare launches the industry's first cloud-native quantum-safe Zero Trust solution, while WALLIX unveils its UAE-hosted WALLIX One SaaS platform, supporting local data sovereignty. These updates reflect the growing emphasis on secure, future-proof, and localized digital infrastructure.

Product innovation and leadership changes—from Cohesity's Gregg Petersen to Tenable's foresight on AI-driven data risks—signal a dynamic year ahead. Meanwhile, emerging threats like AI-powered deepfakes, as highlighted by Trend Micro, remind us that vigilance must evolve as fast as the threats we face.

At *Security Advisor ME*, we remain committed to bringing you regional intelligence, global foresight, and actionable insights. Whether you're a policymaker, CISO, or tech enthusiast, we hope this edition serves as a valuable resource in your journey toward cyber resilience.

Stay secure, stay ahead.

EVENTS

tahawultech.com FUTURE SECURITY AWARDS

tahawultech.com CISO50 AWARDS & FORUM

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Sandhya DMello
sandhya.dmello@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

PRODUCTION AND DESIGN
Designer
Ulysses Galgo
ulysses.galgo@cpimediagroup.com

DIGITAL SERVICES
Web Developer
Adarsh Snehajan
webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

معرض و مؤتمر الخليج العالمي لأمن المعلومات

GISEC GLOBAL

06 - 08 MAY 2025
DUBAI WORLD TRADE CENTRE

HOSTED BY
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

OFFICIAL GOVERNMENT CYBERSECURITY PARTNER
مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

OFFICIALLY SUPPORTED BY
وزارة الداخلية
MINISTRY OF INTERIOR
شرطة دبي
DUBAI POLICE

MIDDLE EAST AND AFRICA'S LARGEST CYBERSECURITY EVENT

SCAN HERE

GET INVOLVED

OFFICIAL DISTRIBUTION PARTNER
SPIRE INFORMATION. SECURED.

LEAD STRATEGIC PARTNER
HUAWEI

STRATEGIC PARTNER
Microsoft aws

DIAMOND SPONSOR
OPSWAT.

PLATINUM SPONSOR
cisco DREAM

GOLD SPONSOR
1Password cpx CLOUDFLARE CROWDSTRIKE Google Cloud Security

GOLD SPONSOR
PENTERA kaspersky SECTIGO MENLO SECURITY

BRONZE SPONSOR
Honeywell DomainTools

BRONZE SPONSOR
miniOrange Recorded Future Silverfort txOne networks

CTF PARTNER
CTF.ae

CONTACT US

gisec@dwtc.com +971 4 308 6469 cyber.gisec.ae #gisecglobal

CONTENTS

Security ADVISOR MIDDLE EAST

D-LINK RECOMMENDS REPLACING VULNERABLE ROUTERS

Vulnerable devices are no longer supported by the vendor and may pose a risk

Vladimir Razov, an expert from the PT SWARM team, has discovered a vulnerability in several models of D-Link routers. According to Mordor Intelligence, D-Link is one of the top three Wi-Fi router manufacturers in the world. The vendor has been notified of the threat in line with the responsible disclosure policy and recommends that users switch to more recent devices.

The vulnerability, which is registered as BDU:2024-06211 with a CVSS 3.0 score of 8.4, affects the following D-Link models: DIR-878, DIR-882, DIR-2640-US, DIR-1960-US, DIR-2660-US, DIR-3040-US, DIR-3060-US, DIR-867-US, DIR-882-US, DIR-882/RE, DIR-882-CA, and DIR-882-US/RE. At the time of the research, vulnerable routers could be discovered using search engines in the United States, Canada, Sweden, China, Indonesia, and Taiwan.

According to the manufacturer, these models are no longer supported. D-Link recommends retiring the outdated devices and replacing them with supported devices that receive firmware updates.

"If this vulnerability is successfully exploited, a malicious user authorized in the router's web interface can compromise the entire device and gain access to all traffic passing through it," said Vladimir Razov, Web Application Security Analyst at PT SWARM, the offensive security department at Positive Technologies.

As a temporary measure to mitigate the threat, Vladimir Razov recommends using OpenWrt (an open-source embedded operating system based on the Linux kernel and designed specifically for routers) or changing the login credentials for accessing the router's web interface.

Previously, Positive Technologies helped address vulnerabilities in Zyxel routers and other Zyxel devices. Positive Technologies also enhanced its PT Industrial Security Incident Manager (PT ISIM) with an additional expertise pack, enabling cybersecurity teams to detect attempts to exploit vulnerabilities in MikroTik routers and Cisco switches.

> **"IF THIS VULNERABILITY IS SUCCESSFULLY EXPLOITED, A MALICIOUS USER AUTHORIZED IN THE ROUTER'S WEB INTERFACE CAN COMPROMISE THE ENTIRE DEVICE AND GAIN ACCESS TO ALL TRAFFIC PASSING THROUGH IT."**
>
> **– VLADIMIR RAZOV, WEB APPLICATION SECURITY ANALYST AT PT SWARM, THE OFFENSIVE SECURITY DEPARTMENT AT POSITIVE TECHNOLOGIES**

GOOGLE CLOUD AND ATLÉTICO DE MADRID EXPAND CYBERSECURITY PARTNERSHIP

Google Cloud has announced the extension of its partnership with Atlético de Madrid, making it the official cybersecurity partner across both the women's and men's teams. This collaboration reinforces a shared commitment to innovation and resilience in sports technology.

In an era where digital security is more important than ever, Atlético de Madrid is strengthening its defenses beyond the pitch. The club has invested in improving protection of both operational and fan data by moving to Google Cloud's Backup and Disaster Recovery Service. This service, which automatically encrypts data at rest, ensures critical data and systems remain protected and operations can swiftly recover from any potential disruption.

Since the beginning of their collaboration, Google Cloud and Atlético de Madrid have worked together to explore innovative ways to enhance the club's cybersecurity posture. A key focus has

Google Cloud

OFFICIAL CYBERSECURITY PARTNER OF ATLÉTICO DE MADRID

been on the importance of protecting sensitive data and maintaining the integrity of digital operations, including the security of its vast fanbase. Over the past months, Google Cloud and Atlético de Madrid have collaborated to gain a better understanding of the threat landscape that Atlético de Madrid faces and have begun implementing best practices in cybersecurity awareness and resilience.

"Sports clubs today operate in an increasingly digital world, making cybersecurity more important than ever," said **Cristina Pitarch, Managing Director EMEA, Google Cloud Security.** "Atlético de Madrid's proactive approach sets a strong example for the industry. We're excited to support their journey by sharing our expertise, exploring new challenges, and helping them build a secure foundation for the future."

Understanding the threat landscape

Atlético de Madrid, along with other global sports clubs, faces a range of cybersecurity threats that could impact operations, reputation, and fan trust. These challenges include:

- **Data breaches and fan data protection:** With a significant amount of personal data, including payment information and preferences, clubs must ensure stringent protection to comply with GDPR and prevent identity theft or fraud.
- **Ransomware attacks:** A cyberattack could disrupt critical operations such as ticketing, merchandising, and performance analysis, particularly during crucial game weeks.
- **Website and mobile app security:** As digital platforms play a crucial role in fan engagement, securing these touchpoints against defacement and DDoS attacks is essential.
- **Phishing and social engineering:** Players, staff, and even fans are potential targets for phishing attempts aimed at stealing credentials and financial information.

> **"SPORTS CLUBS TODAY OPERATE IN AN INCREASINGLY DIGITAL WORLD, MAKING CYBERSECURITY MORE IMPORTANT THAN EVER."**
>
> **– CRISTINA PITARCH, MANAGING DIRECTOR EMEA, GOOGLE CLOUD SECURITY**

Addressing these potential threats with a strong cybersecurity posture not only protects Atlético de Madrid's digital infrastructure but also improves every interaction that players, employees, and fans have with the club and the sport. Cybersecurity also plays a key role in preventing online scams and protecting fans from fraudulent ticket sales and merchandise offers. Even inside the stadium, robust security ensures that essential systems like electronic access controls and signage remain operational, providing a seamless experience for everyone.

"The safety and trust of our digital ecosystem are at the heart of everything we do," said **René Abril, CIO, Atlético de Madrid**. "Cybersecurity plays a critical role in ensuring that every interaction with Atlético de Madrid - whether purchasing tickets, engaging online, or accessing club services - is secure and seamless. Working alongside Google Cloud has already given us valuable insights that we can use to strengthen our defenses and knowledge about the kind of threats facing every football club around the world."

Moving forward, Google Cloud will continue to work alongside Atlético de Madrid to strengthen its security capabilities, explore new ways to innovate, and ensure the club remains protected in today's fast-evolving threat landscape. For Atlético, this partnership goes beyond just implementing security measures, it's about creating a safe and positive experience for everyone who interacts with the club.

WALLIX LAUNCHES UAE-HOSTED WALLIX ONE SAAS PLATFORM

WALLIX, a leading European cybersecurity vendor specialising in identity and access management solutions for digital and industrial environments, announced the launch of its UAE-hosted WALLIX One SaaS platform. This expansion represents a significant milestone in WALLIX's commitment to providing secure, locally-hosted cybersecurity solutions that meet the data sovereignty requirements of UAE-based organisations.

Organisations in the Middle East face increasing pressures to enhance their security while adhering to data residency regulations. The UAE-hosted WALLIX One meets this demand by offering a robust SaaS solution for Privileged Access Management (PAM). The platform enables customers to efficiently manage and secure privileged accounts, safeguard critical data, and mitigate insider and external threats, all within a framework that aligns with UAE data governance standards.

The WALLIX One SaaS platform includes essential services designated to safeguard the digital operations of UAE-based companies. With WALLIX One, employees, external service providers, IT administrators, PLC maintainers, machines, and robots can access IT or OT infrastructures, equipment, applications, and data only after their identity and granted permissions undergo verification.

Afi Hashim, Middle East Regional Manager at WALLIX, said: "We are committed to supporting the security, governance, and compliance objectives of Middle Eastern organisations and we are proud to bring the WALLIX One SaaS platform closer to our customers in the UAE. Our solution provides enterprises, government entities, and SMBs across the region with a world-class cybersecurity solution that meets the highest security standards and protects their critical digital assets while complying with local data residency requirements."

"OUR SOLUTION PROVIDES ENTERPRISES, GOVERNMENT ENTITIES, AND SMBS ACROSS THE REGION WITH A WORLD-CLASS CYBERSECURITY SOLUTION THAT MEETS THE HIGHEST SECURITY STANDARDS AND PROTECTS THEIR CRITICAL DIGITAL ASSETS WHILE COMPLYING WITH LOCAL DATA RESIDENCY REQUIREMENTS."

– AFI HASHIM, MIDDLE EAST REGIONAL MANAGER AT WALLIX

Afi Hashim, Middle East Regional Manager, WALLIX

By outsourcing the management of their identity and access security software to the UAE-hosted WALLIX One platform, security managers retain control over access to critical company resources. This approach helps combat risks associated with theft and identity compromise, allowing them to concentrate on implementing and enforcing their security policies.

WALLIX One, UAE cloud-native SaaS solution offers rapid deployment, effortless updates, and scalable features, making it adaptable to the evolving security demands of modern enterprises. The platform provides tailored protection for several industries, including finance, government, healthcare, and manufacturing, addressing their unique cybersecurity challenges. The UAE-hosted WALLIX One solution also stands out with its identity and access security capabilities, automatic updates, and seamless integration of WALLIX innovations. Its flexibility allows organisations to scale resources and users efficiently while benefiting from an annual subscription model with straightforward pricing. Customers can access various complementary solutions within the WALLIX software portfolio, ensuring a comprehensive cybersecurity strategy.

POSITIVE TECHNOLOGIES EXPERTS UNCOVER NEW MALWARE CAMPAIGN IN THE MIDDLE EAST

Sets a new industry standard with the only quantum-ready zero trust network access solution with broader protocol support coming mid-2025

Cloudflare, Inc., the leading connectivity cloud company, will expand end-to-end support for post-quantum cryptography to its Zero Trust Network Access solution. Available immediately, organizations can securely route communications from web browsers to corporate web applications to gain immediate, end-to-end quantum-safe connectivity.

By mid-2025, Cloudflare will extend this support to include all IP protocols, significantly broadening compatibility across most corporate applications and devices. With this, organizations will be able to rely on Cloudflare to transition their Internet communications between users, devices, and applications to post-quantum cryptography without the complexity of individually upgrading each corporate application or system.

"Cloudflare has long committed to making post-quantum security the new baseline for Internet security, delivering it to all customers so we can bolster defenses against future quantum threats. Now, we're offering that protection built directly into our Zero Trust solutions," said Matthew Prince, co-founder and CEO at Cloudflare. "We want every Cloudflare customer to have a clear path to quantum safety, and we are already working with some of the most innovative banks, ISPs, and governments around the world as they begin their journeys to quantum security. We will continue to make advanced cryptography accessible to everyone, at no cost, in all of our products."

Today encryption is used to keep online data protected—everything from personal messages, to financial information, to customer data—and anything that people and organizations would want to keep safe from hackers. As quantum computers move closer to production, that data is at risk of being unlocked, breaking current encryption methods and potentially exposing data that was once secured. Conventional cryptographic algorithms used across the Internet securing everything from major financial organizations and healthcare providers to government agencies and consumer smart devices, are vulnerable to post-quantum attacks.

Matthew Prince, co-founder and CEO at Cloudflare

The National Institute of Standards and Technology (NIST) even made a landmark announcement to phase out conventional cryptographic algorithms and to adopt post-quantum cryptography by 2030, as experts now estimate significant risks could emerge in as little as five years. There is an urgent need to adopt post-quantum cryptography, and Cloudflare has led the industry by contributing to the creation of industry standards and making post-quantum security free, by default, for all of its customers.

CHAMPIONING CYBER RESILIENCE:

COMMVAULT'S VISION FOR SECURE DIGITAL FUTURE

YAHYA KASSAB, SENIOR DIRECTOR & GM – KSA & GULF, COMMVAULT, SHARES STRATEGIC INSIGHTS ON THE UAE'S CYBERSECURITY EVOLUTION; EMBRACING CYBER RESILIENCE; AND NAVIGATING HYBRID CLOUD LANDSCAPES.

The UAE continues to lead the region in redefining cybersecurity through a proactive, collaborative, and forward-looking strategy. With robust national frameworks championed by key bodies such as the Cybersecurity Council, and strong cooperation between public and private sectors, the country is setting a benchmark for resilience in the digital age.

Kassab outlines the UAE's approach in driving the transition from traditional disaster recovery to cyber resilience in an interview with Sandhya D'Mello, Technology Editor, CPI Media Group.

With over 20 years of experience in the IT industry, Kassab has developed deep expertise in new business development, customer relationship management, and strategic problem-solving, enabling him to effectively identify and address the needs of clients and partners.

He leads a team of dedicated professionals committed to delivering innovative and reliable data protection and cyber resilience solutions across various sectors and markets. Kassab's mission is to help customers successfully implement and execute their technology vision, whether in government, healthcare, utilities, transportation, education, or the private sector.

He is a firm believer in collaboration—both within and between organisations—leveraging technology to drive national agendas and business success.

Kassab's achievements are measured by customer outcomes and satisfaction, and he takes pride in building long-term partnerships with organizations that place technology at the core of their strategy.

How is the UAE's approach to cybersecurity evolving, and what lessons can other regions draw from its experience?

The UAE is indeed setting a commendable example through its collaborative approach to cybersecurity. The country has established significant initiatives led by authoritative bodies such as the Cybersecurity Council based in Abu Dhabi, complemented by efforts in Dubai, playing a pivotal role in defining national security standards and encouraging seamless cooperation between the public and private sectors. Recognizing cybersecurity as a collective responsibility rather than a single entity's task has been integral to their strategy.

We take pride in our active participation within this community, demonstrating our commitment through substantial local presence, technology deployment, and compliance with regional regulations. The UAE's proactive model highlights the importance of awareness, knowledge-sharing, and collaboration, serving as an excellent blueprint for other regions.

What is driving the transition from traditional data protection to cyber resilience?

Traditionally, organisations have relied on disaster recovery as the core of

"WE SUPPORT OUR CUSTOMERS IN DEVELOPING ROBUST CYBER DEFENSE STRATEGIES, ENSURING THEY CAN SWIFTLY RECOVER FROM CYBER INCIDENTS, UNDERSCORING WHY THIS TRANSITION IS CRITICAL."

their business continuity strategies. While disaster recovery remains essential, today's most significant threats are cyberattacks, which demand a different strategic mindset. Cyberattacks differ fundamentally from conventional disasters, requiring specialised responses beyond standard recovery methods. This shift towards cyber resilience addresses the growing necessity for comprehensive cybersecurity defenses and recovery solutions tailored specifically to counter cyber threats. We support our customers in developing robust cyber defense strategies, ensuring they can swiftly recover from cyber incidents, underscoring why this transition is critical.

How do you define cyber resilience, and why is this mindset transformation critical for organizations?

Cyber resilience can be succinctly defined as the capacity to effectively recover and continue operations following a cyber incident. This concept has gained prominence largely due to advancements in Artificial Intelligence (AI). While AI significantly contributes to digital transformation, it has also empowered malicious actors, increasing the likelihood and complexity of cyber threats. Hence, it is crucial for organisations to recognise that cyberattacks are a matter of when—not if. We strongly advocate for businesses to adopt cyber resilience plans, thereby enhancing their preparedness and recovery capabilities in case of cyber incidents.

How does Commvault support organizations in the Gulf region in enhancing their cyber resilience?

Commvault actively partners with major organisations in the Gulf to bolster cyber resilience. Our strategy involves creating awareness about the distinction between traditional disaster recovery and specialised cyber recovery plans. Furthermore, we assist organisations

in developing comprehensive plans incorporating people, processes, and technology. While our primary focus is providing advanced technological solutions, we also work closely with customers and partners to redefine roles, responsibilities, and operational procedures aligned with cyber resilience objectives. Through this multi-layered support, we significantly enhance organizations' defensive and recovery capabilities.

What key trends and challenges are currently shaping the cybersecurity landscape for organisations in the Gulf region?

A primary challenge in the Gulf region remains awareness. Despite ongoing advancements in technologies such as cloud, multi-cloud, AI, and blockchain, organisations frequently struggle to clearly delineate responsibilities, particularly in increasingly complex environments. For instance, multi-cloud environments offer significant agility benefits but simultaneously broaden the attack surface. To mitigate these challenges, we provide unified management solutions enabling simplified oversight and enhanced visibility across diverse workloads and platforms.

A dominant trend is the proliferation of artificial intelligence. While AI drives transformation, it also enables sophisticated cyber threats. Commvault counters this by leveraging AI within our solutions to enhance security, improve usability, and proactively defend against threats. Our goal is to empower organisations with tools that simplify complex multi-cloud environments while proactively safeguarding critical data and infrastructure.

Do businesses and customers in the Gulf region need to embrace hybrid cloud adoption, and if so, why?

Hybrid cloud adoption is increasingly essential in the Gulf region. Organisations benefit from deploying data where it makes strategic sense in terms of cost-efficiency, confidentiality, agility, and performance. Hybrid cloud architectures provide the flexibility to strategically allocate resources, enhancing business agility. Although hybrid and multi-cloud environments can initially present management complexity, Commvault addresses this through solutions offering comprehensive oversight via a single interface. This ensures effective management, security, and streamlined operations across complex hybrid cloud landscapes.

Could you explain the importance and benefits of a 'clean room'?

The 'clean room' represents an innovative solution designed to provide organisations with a secure, isolated environment to perform testing, cleaning, recovery, and operational drills without affecting the production environment. Initially introduced in the UAE through a partnership with Microsoft Azure, our cloud-based clean room solution is both cost-effective and compliant with regulatory requirements. It operates on-demand, significantly reducing costs and complexity associated with traditional dedicated recovery environments. By offering a secure space that mirrors the production environment, it allows operational and security teams to conduct essential activities safely and efficiently, reinforcing organisational resilience against cyber threats.

GITEX EUROPE Berlin x AI EVERYTHING — GERMANY —

21 – 23 MAY 2025

MESSE BERLIN – SOUTH ENTRANCE –

FEATURING

GITEX NORTH STAR EUROPE | GITEX CYBER VALLEY Europe | GITEX SMEDEX SME Digital Economy Expo | GITEX GREEN IMPACT | GQX GITEX QUANTUM EXPO | GITEX SCALEX Europe

Germany's Largest Tech, Startup & Digital Investment Event

2,000+ EXHIBITORS

1,000+ STARTUPS

800+ INVESTORS

100+ COUNTRIES

ENDORSED BY

BERLIN

Senate Department for Economics, Energy and Public Enterprises

GET INVOLVED

#GITEXEUROPE

gitex-europe.com

SOPHOS POWERS UP CYBERSECURITY IN THE UAE

GERARD ALLISON, SENIOR VICE-PRESIDENT OF SALES FOR EMEA AT SOPHOS, DISCUSSES CYBERSECURITY TRENDS, AI-DRIVEN SECURITY SOLUTIONS, AND THE EVOLVING THREAT LANDSCAPE IN THE UAE WITH **SANDHYA D'MELLO**, EDITOR, TECHNOLOGY DIVISION, CPI MEDIA GROUP.

Sophos, a global leader in cybersecurity, has established itself as a trusted provider of innovative security solutions for over three decades. Headquartered in the UK, the company serves millions of users worldwide, protecting organizations from sophisticated cyber threats.

In the UAE, Sophos leads cybersecurity efforts, tackling challenges of rapid digital transformation with AI-driven solutions, Managed Detection and Response (MDR), and Security as a Service. Its recent acquisition of Secureworks strengthens its unified approach to safeguarding businesses from evolving threats. Through regional partnerships, Sophos delivers tailored solutions to sectors like government, banking, and hospitality, while advancing machine-learning tools to ensure resilience against emerging risks.

Gerard Allison joined Sophos in December 2022 and is responsible for accelerating growth in the EMEA region and collaborating closely with the company's extensive partner network to deliver advanced cybersecurity solutions.

How would you describe the UAE's position in technology and digital expansion?

The UAE has always been at the forefront of technological advancement, driving digital transformation across all sectors. This rapid expansion creates immense opportunities but also increases cybersecurity risks. As digital infrastructure grows, the need for robust cybersecurity measures becomes more critical than ever.

What role does Sophos play in addressing cybersecurity challenges in the UAE?

At Sophos, we are committed to protecting organizations from ever-evolving cyber threats. Our recent acquisition of Secureworks has strengthened our capabilities, allowing us to offer a more integrated approach to cybersecurity. This ensures enterprises, mid-market companies, and SMBs have a unified platform to manage their security posture effectively.

What are the key cybersecurity concerns facing organizations in the region?

Ransomware remains one of the most prevalent threats, alongside the challenge of managing multiple security

Gerard Allison, Senior Vice-President of Sales for EMEA at Sophos.

platforms. Many organizations invest in high-end cybersecurity solutions but struggle with monitoring and responding to real-time threats. This is where our solutions come into play—we provide businesses with the tools to detect, mitigate, and prevent cyberattacks efficiently.

How does Sophos help businesses enhance their cybersecurity posture?
Cybersecurity is too complex and changes too fast to be effectively managed by most organizations alone. Our Security as a Service offering realizes an instant security operations center (SOC) for companies. The Sophos expert team stops advanced human-led attacks and takes immediate action to neutralize threats, enabling companies to focus on what matters most – driving the business forward. Sophos MDR (Managed Detection and Response) is one of the fastest-growing segments of our business, serving 28,000 customers globally. This solution enables organizations and partners to continuously monitor threats, leverage global threat intelligence, and strengthen their cyber resilience.

How important are regional partners in Sophos' cybersecurity strategy?
Regional partners are essential to our growth and success. They help us engage with customers across industries, including government, banking, and hospitality. Their role in implementing cybersecurity solutions and organizing industry events ensures we stay connected with the evolving needs of businesses in the UAE.

AI is transforming cybersecurity. How is Sophos integrating AI into its security solutions?
AI has been embedded in our cybersecurity platform since 2017, making us a pioneer in leveraging machine learning for threat detection and response. As cyber threats become more sophisticated, AI helps automate security processes, detect anomalies faster, and enhance overall protection against emerging attacks.

Beyond acquiring cybersecurity solutions, what should businesses focus on to strengthen their security posture?
Businesses need a comprehensive approach — investing in best-in-class security solutions is vital, but so is managing and monitoring security environments proactively. Understanding vulnerabilities, detecting threats in real-time, and implementing a strong cyber response strategy are critical to staying ahead of attackers.

What is your vision for the future of cybersecurity in the UAE?
The cybersecurity landscape will continue to evolve, and businesses must remain proactive. At Sophos, we are dedicated to advancing AI-driven security solutions and working closely with our partners to provide best-in-class protection for organizations in the UAE and beyond.

Liat Hayun, VP of Product Management and Cloud Security Research at Tenable

TENABLE FORECASTS DATA SECURITY IN THE CLOUD TO TAKE CENTRE STAGE AS AI ADOPTION ACCELERATES IN 2025

Tenable, the exposure management company, is highlighting the critical need for organisations to prioritise **data security in the cloud** amid the rapid rise of AI adoption in 2025. In the coming year, companies will face mounting pressure to secure AI initiatives at scale while safeguarding a growing range of data assets from cyber threats. Here are Tenable's key predictions for the future of cloud security:

AI adoption and increased security scrutiny

In 2025 and beyond, we'll see more organisations incorporating AI into their infrastructure and products as the technology becomes more accessible. This widespread adoption will lead to data being distributed across a more complex landscape of locations, accounts and applications, creating new security and infrastructure challenges. In response, CISOs will prioritise the development of AI-specific policies and security measures tailored to these evolving needs. Expect heightened scrutiny over vendor practices, with a focus on responsible and secure AI usage that aligns with organisational security standards. As AI adoption accelerates, ensuring secure, compliant implementation will become a top priority for all industries.

The growth of distributed data will be a boon for cybercriminals

As data volumes grow and become more distributed across multi-cloud environments, the risk of data breaches will rise significantly. With AI tools relying on vast amounts of customer data, cybercriminals will have more opportunities to target these systems, making data exfiltration and unauthorised access easier. Organisations will face an escalating risk as attackers exploit these expanding data environments to achieve malicious goals.

AI-powered attacks will outpace traditional security measures

Despite the best efforts of companies like OpenAI, Google and Microsoft to implement robust security protocols, cybercriminals now have powerful tools at their disposal, including AI-driven virtual assistants that can streamline and amplify their attacks. As data volumes continue to surge and become more accessible, the appeal and ease of targeting sensitive information will grow. This convergence of advanced attack tools and abundant data will make it increasingly difficult for organisations to stay ahead of evolving cyber threats.

Data is business fuel but secure AI adoption is critical

These predictions should not deter organisations from embracing AI. Instead, they underscore the importance of developing robust strategies for secure and responsible AI adoption. Organisations must focus on integrating AI into their systems securely rather than viewing it as a risky proposition.

"Organisations must understand that data is the fuel driving their business—it enables insights, fosters collaboration, and powers innovation," said Liat Hayun, VP of Product Management and Cloud Security Research at Tenable. "As AI adoption skyrockets and data storage demands grow, safeguarding distributed data has never been more critical. As we head into 2025, business leaders and security teams must strike a careful balance between innovation and security, ensuring that AI initiatives do not inadvertently open new doors for cyberattackers."

> **"ORGANISATIONS MUST UNDERSTAND THAT DATA IS THE FUEL DRIVING THEIR BUSINESS—IT ENABLES INSIGHTS, FOSTERS COLLABORATION, AND POWERS INNOVATION." – LIAT HAYUN, VP OF PRODUCT MANAGEMENT AND CLOUD SECURITY RESEARCH AT TENABLE**

MANAGEENGINE EXPANDS ITS INTEGRATION NETWORK WITH 100+ PREBUILT INTEGRATIONS FOR ENTERPRISE IDENTITY MANAGEMENT

THE COMPANY'S IAM PLATFORM, AD360, HELPS CONVERGE DISCONNECTED IDENTITIES

ManageEngine, a division of Zoho Corporation and a leading provider of enterprise IT management solutions, today announced that AD360, its identity and access management (IAM) platform, is further expanding its integration offerings, by adding over 100 new prebuilt integrations. This expansion is a decisive step in the company's endeavor to strengthen its converged IAM platform capabilities. In addition to the extension of support to popular HRMS, ITSM, SIEM, and other enterprise applications, AD360 also comes with REST API capabilities for custom integration with third-party and in-house applications.

- ManageEngine AD360 expands its integration support, with 100+ new ready-to-use integrations
- These integrations empower enterprises for seamless, scalable identity management across diverse IT applications

Why This Matters: The Enterprise Perspective

Large enterprises today face a major challenge: managing various tools with widespread, fragmented data. In a press release titled "Gartner Identifies the Top Cybersecurity Trends for 2025" (issued March 3, 2025), Gartner® highlights a common challenge for large enterprises: the need to optimize their cybersecurity toolsets for efficiency and security while balancing selections for an average of 45 cybersecurity tools available from over 3,000 vendors.

Although enterprises often operate in multi-vendor IT environments out of necessity, this is an added complexity that leads to fragmented identities, resulting in delays in access and increased IT overhead. For example, Gartner's 2024 IAM Leadership Survey found that 54% organizations have seen an increase in the number of identity-related breaches, with one in three organizations experiencing increased business interruptions, financial loss or regulatory penalties from such incidents. As many as 85% of identity-related breaches can be attributed to hacked machine identities such as service and automation accounts. Additionally, according to Verizon's 2024 Data Breach Investigations Report, around 31% of all breaches since 2013 involve stolen credentials.

With global compliance laws and regulations requiring organizations to maintain accurate and up-to-date identity and access data at all times, keeping these records updated is critical. Seamless integration of identities is no longer just an IT challenge for enterprises; it's a business imperative.

"Our vision is to eliminate identity fragmentation and radically simplify enterprise identity governance," said Manikandan Thangaraj, vice president at ManageEngine. "With AD360's expanded integrations, we're empowering businesses to build truly unified digital ecosystems. With this release, we want to help our customers transform identity management from an operational burden into a strategic enabler of productivity, agility, and security. Now, a hospital can auto-provision clinician access in Epic EHR the same day they're hired in Workday, with no coding and no delays."

Enabling Business Agility with Seamless Integrations

ManageEngine AD360's integrations leverage industry-standard protocols—including SCIM, SAML 2.0, OpenID Connect (OIDC), OAuth 2.0, and REST APIs—ensuring seamless compatibility across diverse IT

ecosystems. Through an intuitive no-code configuration interface, IT teams can effortlessly establish connections and design automated workflows without specialized programming knowledge, dramatically accelerating implementation timelines from months to mere days.

ManageEngine's extensive integration network for identity access management enables:

Accelerated Value Realization: Enterprises can quickly integrate and automate identity workflows, reducing operational costs, minimizing errors, and enhancing productivity through unified life cycle management and real-time identity synchronization.

Strategic Flexibility and Choice: Maintain the freedom to integrate with a vast range of enterprise applications without vendor lock-ins, ensuring compatibility, scalability, and support for diverse business needs.

Advanced Identity Automation: With businesses seeking productivity improvements, AD360 can implement sophisticated, no-code identity orchestration processes to automate critical activities such as user provisioning, access modifications, identity synchronization, and secure offboarding across a company's identity ecosystem.

Zero-Gap Compliance: Automatically align identity records across HR, IT, and security systems to pass audits for the GDPR, HIPAA, and SOX.

"The interoperability between critical business applications streamlines processes such as onboarding and offboarding, delivering measurable business value and accelerating ROI. Legacy IAM tools often treat integrations as an afterthought, requiring months to integrate an organization's IAM tech stack with ITSM or HCM tools. AD360 helps accomplish this with just a few clicks. It's not just about connecting systems, it's about fundamentally changing how enterprises manage identities while minimizing security risks," Thangaraj stated.

About AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security and ensures compliance with evolving regulatory standards.

"OUR VISION IS TO ELIMINATE IDENTITY FRAGMENTATION AND RADICALLY SIMPLIFY ENTERPRISE IDENTITY GOVERNANCE."

– MANIKANDAN THANGARAJ, VICE PRESIDENT AT MANAGEENGINE

VERTIV LAUNCHES NEW FREE COOLING EVAPORATIVE SOLUTION WITH LOW-GWP REFRIGERANT TO BOOST EFFICIENCY AND REDUCE CARBON FOOTPRINT FOR DATA CENTRES IN EMEA

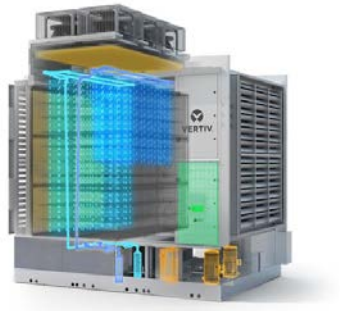
VERTIV LIEBERT EFC ALLOWS HYPERSCALE AND COLOCATION CLIENTS TO EASILY FLEX BETWEEN OPERATING MODES FOR ZERO WATER WASTE AND UTMOST EFFICIENCY

Vertiv, a global provider of critical digital infrastructure and continuity solutions, announced a significant upgrade of its thermal management product portfolio with the introduction of the next-gen Vertiv Liebert EFC free cooling unit with low-GWP (Global Warming Potential) refrigerant. The solution is designed to meet stringent environmental standards for data center applications, including colocation and cloud services, and is now available across Europe, Middle East and Africa (EMEA) with capacities ranging from 150 to 450 kW.

Vertiv Liebert EFC combines the capabilities of indirect air-to-air heat exchange and evaporative cooling principles in a single unit. The innovative patented polymer heat exchanger and the new low-GWP inverter driven compressor technology significantly enhance annual efficiency by up to 19% compared to previous technologies, allowing a pPUE (partial Power Usage Effectiveness) as low as 1.05.

One of the standout benefits of the Liebert EFC is its extreme flexibility. Based on onsite-specific conditions, a live toggling control feature allows users to seamlessly and securely reduce the use of critical resources like power or water via software controls, to leverage the free cooling mode. This flexibility empowers data centre owners to reduce their climate impact while enabling continuous cooling, regardless of site-specific resources. Models are available with full direct expansion (DX) back-up with a remote condenser, to supply the entire cooling capacity without any water requirements - offering full water independence, without impacting reliability.

"As businesses prioritize sustainability strategies, customers are increasingly seeking innovative cooling solutions that reduce resource consumption while offering operational flexibility and resilience," said Sam Bainborough, vice president, thermal business EMEA at Vertiv. "The Liebert EFC, with its game-changing and patented technology, addresses these needs with a flexible system that delivers an entirely new experience for the customer, maximizing time using free cooling and leveraging the natural power of evaporation."



The new Liebert EFC complies with current global regulations and bans (EU F-Gas regulation 2024/573, and IPCC AR4), offering a turnkey solution engineered for future scalability, easy maintenance, and durability. The polymer design offers improved corrosion resistance and also allows a wider range of water qualities during operation when compared to an aluminum heat exchanger. At the core of this cutting-edge solution is Vertiv™ Liebert® iCOM™ and its control algorithms, which manage automatic transitions between the most suitable working modes, enabling use of the preferred cooling source. The controls also enable seamless coordination of units, allowing them to function as a unified system, enhancing cooling continuity and reliability without the need for an additional plant management system.

> **"AS BUSINESSES PRIORITIZE SUSTAINABILITY STRATEGIES, CUSTOMERS ARE INCREASINGLY SEEKING INNOVATIVE COOLING SOLUTIONS THAT REDUCE RESOURCE CONSUMPTION WHILE OFFERING OPERATIONAL FLEXIBILITY AND RESILIENCE."**
>
> **– SAM BAINBOROUGH, VICE PRESIDENT, THERMAL BUSINESS EMEA AT VERTIV**

HPE AND E& UAE EXPAND THEIR PARTNERSHIP, INTRODUCING A NEW, FLEXIBLE SD-WAN AS-A-SERVICE SOLUTION

Alain Carpentier, Senior Vice President Worldwide Sales, Aruba and Hamad Al Marzooqi, Senior Vice President of Presales and Business Operations, e& UAE.

E& UAE, the flagship telecoms arm of e&, and Hewlett Packard Enterprise (HPE) announced the expansion of their partnership, paving the way for the launch of a flexible SD-WAN as-a-Service offering, based on HPE Aruba Networking EdgeConnect SD-WAN.

In November 2024, e& UAE and HPE disclosed their plans to offer tailored networking solutions and comprehensive services, based on HPE Aruba Networking technology.

The partners have now taken the next step in their collaboration, with the announcement of a new flexible solution for their SD-WAN customers, which will be based on the HPE Aruba Networking EdgeConnect SD-WAN. The onboarding of this new solution will further support e& UAE in its ambition to become the premier managed services portfolio in the UAE.

The new solution will provide e& UAE customers with key insights into their own SD-WAN consumption and help them manage costs.

"Throughout the past few months, we've seen an increasing demand highly performant, secure and reliable networking increasing, fuelled by significant developments the UAE's business and especially tech scene as innovations such as AI on the rise," said Zeeshan Hadi, Country Manager for UAE & Africa at HPE Aruba Networking. "The new flexible SD-WAN as-a-Service solution provided by e& UAE will directly address those needs, providing the key advantages of HPE Aruba Networking's EdgeConnect SD-WAN in a flexible as-a-service model. With e& UAE's wide network presence in the country, this will enable more organisations to fully embrace technological developments and scale based on their network usage needs."

The sentiments expressed by HPE Aruba Networking were echoed by e& UAE, who shared that the new offering will be supported through e& UAE's Network Operations Centre (NOC), which allows customers to reduce the burden on the IT team, increase efficiency, and lower overall cost, with a dedicated team of professional engineers managing IT operations end-to-end.

Ultimately, this will deliver more value for customers, increase their visibility and flexibility and overall deliver a better customer experience.

At e& UAE, we are committed to driving cutting-edge digital transformation by delivering scalable, secure, and high-performance networking solutions to our customers," said Hamad Al Marzooqi, Senior Vice President of Presales and Business Operations, e& UAE. "Our expanded collaboration with HPE Aruba Networking marks a significant milestone in offering flexible, as-a-Service SD-WAN solutions that optimize cost efficiency, enhance operational agility, and empower businesses to scale seamlessly. By integrating HPE Aruba Networking's EdgeConnect SD-WAN with our robust Network Operations Centre (NOC), we provide end-to-end managed services, allowing enterprises to focus on innovation while we ensure seamless network performance and security. This initiative aligns with our vision to be the premier managed services provider in the UAE, equipping businesses with the agility to thrive in an evolving digital economy."

UIPATH LAUNCHES TEST CLOUD TO BRING AI AGENTS TO SOFTWARE TESTING

UiPATH AGENTIC TESTING CAN SIGNIFICANTLY REDUCE THE 25% OF IT BUDGET TYPICALLY DEDICATED TO TRADITIONAL SOFTWARE TESTING METHODS

UiPath, a leading enterprise automation and AI software company, announced the launch of UiPath Test Cloud, a revolutionary new approach to software testing that uses advanced AI to amplify tester productivity across the entire testing lifecycle for exceptional efficiency and cost savings.

Through Test Cloud, agentic testing for quality assurance teams becomes reality, equipping professionals with AI agents such as UiPath Autopilot and testing agents built with Agent Builder to act as collaborative partners throughout the testing lifecycle. In augmenting testers with AI, businesses can enable faster time to market, improve production stability, and deliver higher-quality software to customers.

Manual testing and test automation with legacy tools is costly, slow, and resource intensive. In fact, one study found up to 25% of IT spend is dedicated to quality assurance and testing. Test Cloud represents a shift toward AI-augmented testing, focusing on collaboration between people and AI agents to enhance the complete testing process. It is designed to address both technical and personal challenges faced by testers in an increasingly complex software development landscape.

UiPath Test Cloud introduces agentic testing to quality assurance, engineering, and testing teams at any organization via:

- **Autopilot for Testers:** an out-of-the-box agent that harnesses a broad collection of built-in and customizable AI to accelerate the testing lifecycle, including agentic test design, agentic test automation, and agentic test management.
- **Agent Builder:** a toolkit for building custom AI agents tailored to unique testing needs, giving teams flexibility to create exactly what they need, when they need it, according to their own specifications.

According to a study by IDC commissioned by UiPath, organizations using Test Cloud have improved test efficiency by 36% and doubled the throughput of delivering new features as well as reduced outages by 50% and troubleshooting time by 93%. For example, Cisco is cutting its manual testing efforts nearly in half with Autopilot, freeing up valuable time for its testing teams to focus on challenges that benefit from human creativity, strategic thinking, and decision making.

"Agentic testing marks an exciting new era for companies to advance an area of their business that is still stubbornly manual and time intensive. With Test Cloud, testing teams engage interactively with AI agents that act like partners in collaborating, supporting, and working in tandem with testing professionals around the clock across the entire testing lifecycle," said Gerd Weishaar, General Manager and Senior Vice President of Testing Products at UiPath. "Traditional testing is recognized by CIOs and CTOs as the biggest bottleneck to delivering new innovations to customers rapidly. Implementing agentic testing with Test Cloud enables faster time to market and improves production stability, which increases customer satisfaction and helps companies grow revenue."

CAPABILITIES OF TEST CLOUD

UiPath Test Cloud is a full-featured testing offering that equips software testing teams with enterprise-ready, production-grade, resilient end-to-end automation for modern and enterprise applications as well as a deployment environment catered to the needs of testers.

Agentic testing extends, accelerates, and simplifies testers' work, increasing their productivity and job satisfaction. Together, Autopilot and Agent Builder form a powerful duo: built-in, customizable AI capabilities with Autopilot to get started fast, and the freedom and flexibility with Agent Builder to create the exact agents needed to accelerate testing. These agents are more than just conversational partners—they can perform tasks using tools teams equip them with like UI and API automations or even other agents.

With Test Cloud, organizations can unlock the benefits of a full-featured agentic testing offering:

- **Resilient end-to-end automation and production-grade architecture:** automate testing for any UI or API of modern web, mobile, and enterprise applications, such as SAP and Oracle, and leverage production-grade architecture with industry-certified secure application testing, auditing and role management, and centralized credentials
- **Open, flexible, and responsible AI:**

enterprise-ready agentic testing capabilities are open, flexible, and responsible within CI/CD integrations, ALM integrations, version control, and webhooks. In addition, the UiPath AI Trust Layer ensures that agentic testing capabilities meet the highest standards of security, safety, and governance

- **Powered by the UiPath Platform:** with enterprise-wide automation, users can share and reuse components across teams, and utilize marketplaces, snippets and libraries, object repositories, and asset management.

"AGENTIC TESTING MARKS AN EXCITING NEW ERA FOR COMPANIES TO ADVANCE AN AREA OF THEIR BUSINESS THAT IS STILL STUBBORNLY MANUAL AND TIME INTENSIVE. WITH TEST CLOUD, TESTING TEAMS ENGAGE INTERACTIVELY WITH AI AGENTS THAT ACT LIKE PARTNERS IN COLLABORATING, SUPPORTING, AND WORKING IN TANDEM WITH TESTING PROFESSIONALS AROUND THE CLOCK ACROSS THE ENTIRE TESTING LIFECYCLE."

– GERD WEISHAAR, GENERAL MANAGER AND SENIOR VICE PRESIDENT OF TESTING PRODUCTS AT UIPATH

FORTINET EXPANDS OT SECURITY PLATFORM TO STRENGTHEN PROTECTION FOR CRITICAL INFRASTRUCTURE

UPDATES TO THE INDUSTRY'S MOST COMPREHENSIVE OPERATIONAL TECHNOLOGY SECURITY PLATFORM INCLUDE ENHANCED VISIBILITY, SEGMENTATION, AND SECURE CONNECTIVITY.

Fortinet, the global cybersecurity leader driving the convergence of networking and security, has advanced its OT Security Platform to further support the protection of critical infrastructure and industrial sites from evolving cyberthreats. New enhancements go beyond traditional OT visibility solutions and include deeper OT-specific threat visibility with the FortiGuard OT Security Service, expanded ruggedized solutions for segmentation and 5G in harsh environments, and an upgraded OT SecOps portfolio for automated threat response and regulatory compliance tracking.

"Fortinet has been building an industry-leading OT Security Platform for 20-plus years and remains at the forefront of OT security innovation," said Nirav Shah, Senior Vice President, Products and Solutions at Fortinet.

"As cyberthreats against critical infrastructure and across industries such as energy, transportation, and manufacturing continue to grow, Fortinet remains committed to delivering comprehensive security solutions tailored for operational technology environments. These latest enhancements give organizations the tools they need to improve their OT security posture and adhere to regulatory requirements—all managed through a single, unified platform," added Shah.

KEY ENHANCEMENTS TO THE FORTINET OT SECURITY PLATFORM

The latest Fortinet OT Security Platform updates introduce powerful new capabilities to enhance OT security:

- **New FortiGate Rugged NGFWs** combined with new enhancements to the **FortiGuard OT Security Service** provide unparalleled security enforcement in OT environments, allowing organizations to detect threats across over 3,300 OT protocol rules, nearly 750 OT IPS rules, and 1,500 virtual patching rules. These capabilities protect against known exploited vulnerabilities (KEVs) and other cyber risks while delivering advanced threat protection through virtual patching for legacy OT systems. Additional new secure networking OT capabilities include updates to **FortiSRA**, enhancing secure remote access with improved secrets and password management for OT environments.
- To ensure secure segmentation, Fortinet has also introduced the **FortiSwitch Rugged 108F and FortiSwitch Rugged 112F-POE**, expanding its portfolio of industrial-grade small form-factor switches. These ruggedized switches allow for granular security enforcement at the port level, preventing unauthorized lateral movement across OT networks while maintaining seamless integration with Fortinet's broader security ecosystem. These switches, built on Fortinet's unified FortiOS operating system, streamline network and security management.
- For secure and resilient connectivity, Fortinet has also launched **two ruggedized 5G solutions: the FortiExtender Rugged 511G**, an IP67-rated 5G wireless WAN gateway that delivers high-speed, secure connectivity to remote OT sites; and the **FortiExtender Vehicle 511G**, an IP64-rated 5G router designed for fleet vehicles. Both solutions feature embedded Wi-Fi 6 and new eSIM capabilities, removing the need for physical SIM cards and simplifying carrier selection.
- Fortinet is also **strengthening its AI-driven security operations** (SecOps) capabilities for OT. Enhancements to FortiAnalyzer 7.6 and FortiDeceptor 6.1 provide deeper insights into security threats and simplify compliance reporting for OT security teams. Updates to FortiNDR Cloud include a new OT protocol support for threat hunting, while FortiNDR (on-premises) adds several new features, including a Purdue Model view and new device inventory that includes OT and the Mitre ATT&CK ICS Matrix.

The Fortinet OT Security Platform provides unified visibility and security capabilities to manage OT and remote-site security, simplifying and empowering customers' ability to assess, secure, and report on risk, including complex regulatory compliance requirements.

"FORTINET HAS BEEN BUILDING AN INDUSTRY-LEADING OT SECURITY PLATFORM FOR 20-PLUS YEARS AND REMAINS AT THE FOREFRONT OF OT SECURITY INNOVATION."

– NIRAV SHAH, SENIOR VICE PRESIDENT, PRODUCTS AND SOLUTIONS AT FORTINET

Only Fortinet offers seamless segmentation capabilities and an end-to-end ruggedized portfolio of OT security solutions powered by a single operating system, FortiOS. Deep integration with the Fortinet Security Fabric makes the OT Security Platform the most comprehensive in the industry, providing the most effective, efficient, and holistic offering for OT security and compliance adherence that goes beyond the industry standard.

INDUSTRY RECOGNITION AND CUSTOMER SUCCESS

The Fortinet OT Security Platform is widely trusted by global organizations looking to seamlessly integrate IT and OT security. The company was recognized as the sole leader in the Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator™, reinforcing its market leadership.

"Together, Fortinet and Honeywell help strengthen cybersecurity for critical infrastructure and operational technology environments. As cyberthreats intensify, industrial and commercial buildings operators need integrated end-to-end protection more than ever. Our relationship with Fortinet enhances Honeywell's cybersecurity and ICT offering portfolio providing several strategic advantages in securing and managing risk for remote and on-campus customer sites; as well, reinforcing our commitment with Fortinet," said *Manish Goyal, General Manager,* ***Honeywell Connected Cybersecurity.***

NIST ADDS SANDBOXAQ'S HQC ALGORITHM TO ITS LIST OF POST-QUANTUM CRYPTOGRAPHY STANDARDS

HQC IS SANDBOXAQ'S SECOND CO-INVENTED CRYPTOGRAPHIC ALGORITHM SELECTED BY NIST, UNDERSCORING ITS LEADERSHIP IN DEFINING THE GLOBAL STANDARD FOR QUANTUM-RESISTANT CYBERSECURITY

SandboxAQ announced that the National Institute of Standards and Technology (NIST) has officially selected HQC (Hamming Quasi-Cyclic) as the fifth algorithm in its suite of post-quantum cryptographic (PQC) standards. Out of these five algorithms, three will be used for signatures. The other two, HQC and ML-KEM, will be the NIST-approved algorithms that will protect the confidentiality of communications across the Internet, cellular networks, payment systems, and more.

The selection of HQC marks SandboxAQ's second major contribution to NIST's post-quantum standardization effort, a key step in ensuring the protection of the world's most critical data. This landmark decision represents a significant milestone in the global transition to a robust, quantum-safe encryption future and further solidifies SandboxAQ at the forefront of cryptographic innovation.

HQC is a key encapsulation mechanism designed to secure the exchange of encryption keys in a quantum-resistant manner. Unlike traditional public-key encryption systems such as the widely-used public key cryptosystem, RSA, and elliptic-curve cryptography (ECC), which quantum computers render obsolete, HQC is built on the well-established mathematical foundation of error-correcting codes, which is not vulnerable to quantum attacks. It provides strong security guarantees while balancing performance factors such as computational efficiency and key size, which are primary considerations for large-scale real-world deployments. In NIST's final selection report, the HQC algorithm, co-invented by SandboxAQ team members, stood out as a robust and reliable candidate for wide-scale adoption across industries, following multiple rounds of global cryptanalysis and peer review.

Prior to HQC, the SandboxAQ team also played a significant role in the development of SPHINCS+, one of the initial algorithms already selected by NIST as part of its initial set of PQC standards in 2022. With HQC now formally accepted into the standardization process, SandboxAQ has contributed to two of the five critical PQC standards for key exchanges and signatures, demonstrating deep and sustained leadership in quantum-resistant cybersecurity and ushering in a safer digital world.

"HQC has foundations in coding theory that offer strong theoretical and practical protection against known quantum decryption methods, while its efficient performance profile makes it well-suited to real-world adoption," said Taher Elgamal, a partner at Evolution Equity Partners and senior advisor at SandboxAQ, who is colloquially called 'the father of SSL'. *"With SPHINCS+ and HQC both standardized by NIST, SandboxAQ has solidified its leadership in developing effective PQC solutions for enterprises and government agencies. This is not just a milestone for SandboxAQ, it's a win for global security in the face of future quantum disruption."*

"We began developing HQC in the 2000s, and by the 2010s, we had demonstrated that this protocol resolved a 40-year-old open problem in code-based key exchanges. Today, HQC stands as one of only two protocols securing the confidentiality of nearly all global communications," said Carlos Aguilar Melchor, chief cybersecurity scientist at SandboxAQ. "At SandboxAQ, we've long championed the importance of standardization, and contributing to two of the five NIST PQC standards reflects our commitment to shaping the future of cryptography."

SandboxAQ has a unique position to improve cryptographic postures and ensure better compliance, fewer outages, and robust cybersecurity. It produces world-class cryptographic research, internationally recognized standards, and widely adopted cryptographic innovations. Leveraging this world-leading expertise, SandboxAQ also offers an industry-leading cryptography management product, uniquely positioning it within the global cryptographic landscape. Our flagship cryptographic offering, AQtive Guard, is trained on billions of cryptographic findings, meticulously structured and enriched with supplemental data by our world-class cryptography team. By cross-referencing and augmenting our customers' inventories, we empower efficient exploration and actionable insights. Leveraging our distinctive AI approach, seamless third-party integrations, and comprehensive 360-degree coverage sensors, AQtive Guard delivers unparalleled visibility and effectiveness for the protection of enterprises and governments.

CLOUDFLARE NAMED LEADER IN WEB APPLICATION FIREWALL SOLUTIONS BY INDUSTRY RESEARCH FIRM

CLOUDFLARE RECEIVES HIGHEST SCORE AMONG ALL WAF PROVIDERS IN CURRENT OFFERING CATEGORY

Cloudflare, Inc, the leading connectivity cloud company, has been named by Forrester Research, Inc. as a Leader in The Forrester Wave: Web Application Firewall Solutions, Q1 2025 report. Cloudflare's Web Application Firewall (WAF) received the highest possible score in 15 out of 22 criteria including Innovation, Detection models, Product security, Partner ecosystem and more.

"Since our founding, Cloudflare's WAF has been a cornerstone offering for millions of customers who depend on us to buy valuable time to patch their systems before hackers can find and exploit vulnerable applications," said Matthew Prince, co-founder and CEO, Cloudflare. "We're proud to be recognized as a Leader by Forrester in this space, further underscoring for us our continued investment and success in building the best platform for protecting APIs and application web traffic– unmatched by any competitor."

The Forrester Wave: Web Application Firewall Solutions report notes that, "Cloudflare is a strong option for customers that want to manage an easy-to-use, unified web application protection platform that will continue to innovate." Additionally, the report notes that "Cloudflare stands out with features that help customers work more efficiently."

Cloudflare believes its placement as a leader underscores continued investment and innovation in solutions that help safeguard customers against an evolving threat landscape. Cloudflare's WAF uses unprecedented insights from Cloudflare's global network – one of the largest in the world – to ensure that threat actors can't find and leverage vulnerabilities in web applications and APIs to wreak havoc.

ring
an amazon company

e&
etisalat and

Smart Monitoring Solutions

Free Lifetime Video Recording
3 Year Warranty
Free Installation
Free after-sales service

Keep an eye on your home even when you are away

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

Starts at AED 20*

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

*Terms and conditions apply

COHESITY APPOINTS GREGG PETERSEN REGIONAL DIRECTOR - MIDDLE EAST

Cohesity, the leader in AI-powered data security, announced Gregg Petersen as Regional Director - Middle East for the organization. Following the company's combination with Veritas Technologies' data protection business, Petersen's new leadership remit will include the responsibility to drive all strategic initiatives across the region to enhance Cohesity's position as the leading provider of next-generation data security and management solutions.

As part of its growth strategy, Cohesity is doubling down on market engagement through its industry-leading partner alliance program, recognized as the strongest in the region among competitors. By fostering deeper collaboration with key channel partners, Cohesity aims to accelerate joint go-to-market initiatives, deliver tailored solutions, and provide businesses with the tools they need to navigate complex data security challenges. The company is committed to supporting customers in AI adoption, regulatory compliance, and sustainability, ensuring that organizations can seamlessly integrate advanced data protection while meeting evolving industry standards.

Petersen brings 26 years of experience in data security, cyber resilience, and AI-driven protection strategies, including 17 years in the Middle East. Throughout his tenure at Cohesity, he has been a strong advocate for innovative approaches to mitigating cyber threats, enhancing recovery capabilities, and fostering partnerships across the industry. As Regional Director for the Middle East at Cohesity in 2021, his leadership has contributed to Cohesity's regional expansion, supporting organizations to strengthen their security posture and accelerate digital transformation.

Gregg Petersen, Regional Director - Middle East, Cohesity

Johnny Karam, Managing Director & Vice President, International Emerging Markets at Cohesity, said: "Gregg's progression within our regional leadership team comes at a defining moment as we continue to drive innovation and leadership in AI-powered data security and cyber resilience. His extensive industry expertise and proven ability to develop high-growth strategies make him the ideal leader to strengthen our market position, deepen our partner ecosystem, and accelerate our vision of delivering next-generation data security solutions to enterprises across the region."

Reflecting on his new remit, Gregg Petersen, Regional Director - Middle East at Cohesity said: "As we unify our teams, our ambition is to become the most formidable force in AI-powered data security and cyber resilience across the Middle East. This is a transformative era for Cohesity, and I am committed to amplifying our impact as a global and regional leader. Our focus remains on empowering organizations with cutting-edge solutions to secure, manage, and recover their most critical data in an increasingly complex cyber landscape. A key priority will be strengthening our channel and alliance partnerships, ensuring that our expansive network continues to set the industry benchmark for excellence and innovation."

Prior to his role with Cohesity, Petersen had sales leadership roles at Veeam, Rackspace, and Dell EMC, which have provided critical experience to support organizations across the Middle East to accelerate their digital transformation journeys and ensure Cohesity remains at the forefront of cyber resilience, AI-powered data security, and sustainable innovation.

"THIS IS A TRANSFORMATIVE ERA FOR COHESITY, AND I AM COMMITTED TO AMPLIFYING OUR IMPACT AS A GLOBAL AND REGIONAL LEADER. OUR FOCUS REMAINS ON EMPOWERING ORGANIZATIONS WITH CUTTING-EDGE SOLUTIONS TO SECURE, MANAGE, AND RECOVER THEIR MOST CRITICAL DATA IN AN INCREASINGLY COMPLEX CYBER LANDSCAPE."

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

FORTINET

COLLABORATION MADE EASY USING A WORK MANAGEMENT PLATFORM

Effective collaboration between security operators, teams, and other departments is essential for the smooth functioning of any organization. However, as organizations grow in complexity, it becomes increasingly challenging for teams to coordinate. Factors such as staffing shortages, high turnover rates, and outdated collaboration tools exacerbate these challenges.

When staff rely on multiple disconnected tools for dispatch, reporting, and task tracking, operations often become fragmented, leading to delays and gaps in communication. In critical areas like safety and security, these inefficiencies can have serious consequences.

Work management solutions bridge these gaps by managing, tracking, and documenting activities, streamlining processes, and fostering real-time collaboration. Built specifically for security teams, these solutions enhance communication, boosts productivity, and improves overall operational efficiency through workflow automation.

Organizations in the Middle East operate in high-security environments where seamless collaboration is essential. A robust work management platform enables swift response and coordination across complex operational landscapes. This growing need for integration is driving more organizations to align their security and IT departments. According to a recent Genetec report, 78% of end users in

Firas Jadalla, Regional Director – Middle East, Turkey & Africa, Genetec Inc

the META region indicate that these departments now work collaboratively, reflecting a shift toward a more unified security approach.

Overcoming barriers to effective collaboration

Over time, many organizations accumulate a patchwork of databases, spreadsheets, and standalone systems to communicate, create reports, and track activities. Some still rely on outdated paper-and-pen processes, which aren't only time-consuming but also prone to errors. These disjointed methods hinder information sharing and coordination.

A digital work management platform consolidates these fragmented systems, offering teams a unified view of activities accessible on both desktop and mobile devices. To take full advantage of their security system data, security teams need to consider more than a generic work management solution.

An ideal work management solution for security teams should accommodate security activities such as guard tours, patrols, and maintenance inspections. It should also seamlessly integrate with existing security systems. For instance, a video operator should be able to create a work request with an attached camera snapshot and route it to the appropriate team in just a few clicks.

To ensure trustworthy audits and reporting, the work management system should be built with strong cybersecurity measures and ensure that data can't be manipulated after the fact by applying blockchain principles.

Benefits of work management systems

Implementing a work management system can transform security operations in several ways:

- **Improved Communication:** Teams gain real-time visibility into task progress, responsibilities, and pending assignments. Updates and alerts can be shared seamlessly to request assistance or provide situational awareness.
- **Enhanced Collaboration:** Every team member contributes to shared goals rather than isolated tasks. Custom API integrations can connect with other systems, such as employee apps, further fostering teamwork.
- **Time Savings:** Built-in reporting tools automate activity logs and compliance audits, freeing up time for other critical tasks.
- **Operational Efficiency:** Routine tasks, incident management, and resource tracking are streamlined. Tasks are assigned to personnel with the appropriate skills, tools, and knowledge, ensuring readiness and precision.
- **Workflow Automation:** Automations simplify recurring tasks, such as setting reminders, generating

reports, or notifying team leads when new requests are added.

- **Resource Optimization:** Features like work ticketing and asset management enable efficient resource allocation and management of internal and external requests.
- **Mobile Support:** Field officers benefit from mobile apps that enhance situational awareness, communication, and access to standard operating procedures on the go.

Today, governments across the region, including the UAE and Saudi Arabia, are heavily investing in smart security solutions as part of their national digital transformation strategies. A centralized work management platform not only supports these efforts but also helps businesses align with evolving security regulations, ensuring compliance and streamlining reporting processes.

Tips for successful implementation

Every organization has unique workflows, so selecting a customizable work management system is crucial. It's important to choose a solution that's customizable and intuitive to minimize the need for extensive training.

Integration is another key factor. A platform that deeply integrates with your existing security ecosystem provides a cohesive view of operations and eliminates the need for manual data transfers or redundant processes.

A well-designed work management system can break down silos, empower teams, and boost efficiency. To ensure a successful deployment, adopt a lean and agile approach: start small and gradually incorporate more features as your team becomes comfortable with the platform.

With initiatives like Saudi Vision 2030 and UAE's Smart City strategy, organizations are increasingly integrating AI-driven security and IoT-enabled monitoring into their operations. A work management platform with automation capabilities supports these advanced security frameworks.

"A ROBUST WORK MANAGEMENT PLATFORM ENABLES SWIFT RESPONSE AND COORDINATION ACROSS COMPLEX OPERATIONAL LANDSCAPES. THIS GROWING NEED FOR INTEGRATION IS DRIVING MORE ORGANIZATIONS TO ALIGN THEIR SECURITY AND IT DEPARTMENTS."

1ST IN THE REGION

PIONEERING CONVERSATIONAL AI AS A SERVICE

Our Industry Landscape

- Retail
- Healthcare
- Banking
- Education
- Oil & Gas

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

SCAN QR

LEARN MORE

OMNIX Conversational AI

MACHINE IDENTITIES ARE GROWING FASTER THAN HUMAN IDENTITIES - HOW THE UAE CAN STAY AHEAD OF THE THREAT

While organizations in the Middle East are increasingly savvy about the need for robust cybersecurity measures, there remains a worrying lack of knowledge about specific risks including the rapid proliferation of machine identities. In fact, machine identities are increasing at a frightening pace. Last year, they outnumbered human identities by a ratio of 45:1 and this has only been increasing, creating numerous challenges for organizations in the UAE and the wider Middle East.

This trend is being driven by the fast growth of cloud technologies, AI, and microservices. Each of these technologies relies on a unique identity to function securely, leading to a surge in machine identities.

The UAE has embraced advances in AI and machine learning, positioning itself as a global tech hub. However, this progress presents both opportunities and challenges.

While machine identities are essential for powering digital infrastructure, their proliferation is also being exploited by cybercriminals, and as the number of machine identities grows, so does the potential for cyberattacks. A report from 2024 revealed that 99% of UAE organizations experienced two or more identity-related breaches in the past year. But just how quickly are they growing?

Kevin Bocek

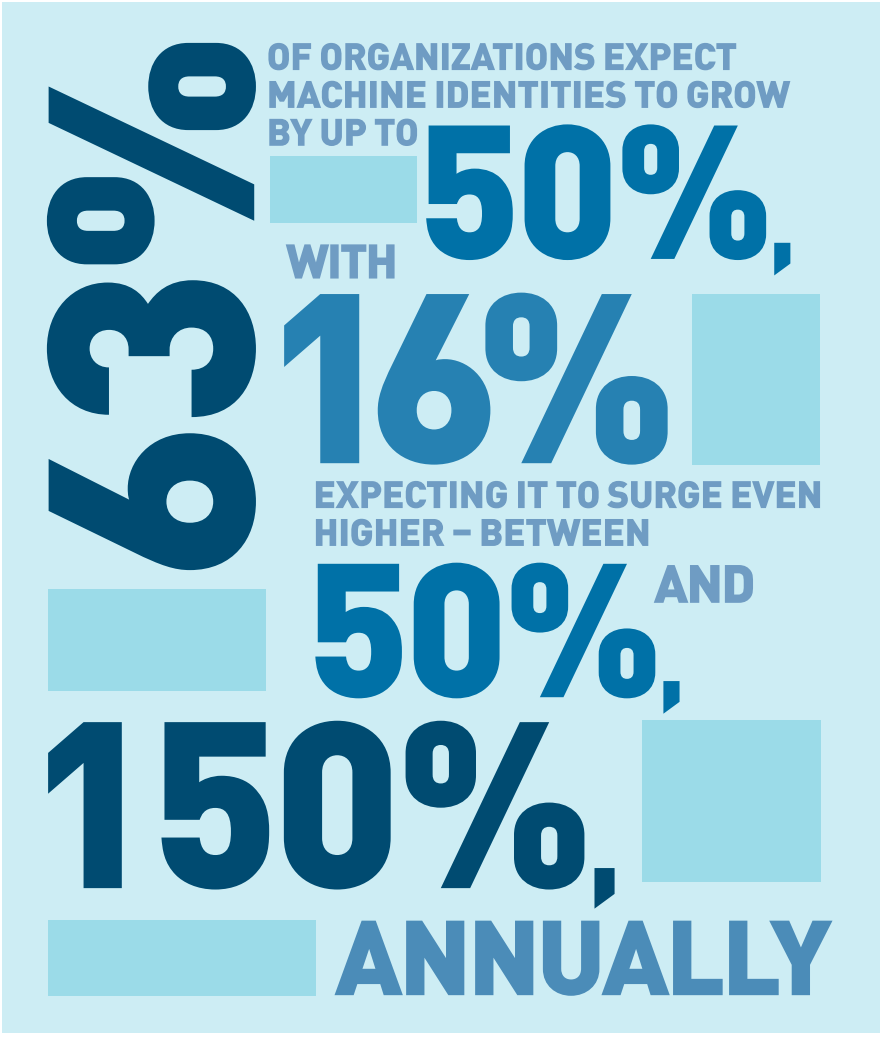
The Growing Number of Machine Identities

It's difficult to overstate how quickly machine identities are multiplying. The recent CyberArk Machine Identity Security report found that 79% of organizations expect the number of machine identities to keep growing at an overwhelming pace. Over the next year, 63% of organizations expect machine identities to grow by up to 50%, with 16% expecting it to surge even higher – between 50% and 150% annually.

Why Machine Identities Are Attractive to Hackers

Machine identities may seem like a technical detail, but in the wrong hands, they can be a goldmine for hackers. Cybercriminals exploit machine identities to gain unauthorized access to systems, steal data, or cause major disruption. A weak or expired machine identity is an easy entry point for attackers, and with so many organizations relying on machines to carry out critical operations, the risk is significant.

In March, the UAE experienced more than 600 cyberattacks targeting both public and private sectors within a matter of days. While these attacks – which were part of a global surge – were successfully blocked, it is vital that organizations anticipate and protect themselves from future incidents. This is especially important given the UAE's role as a leading global hub for key industries and smart city initiatives.



The Growing Gap Between Human and Machine Identity Security

Despite the rapid growth in machine identities, many organizations are still focusing primarily on securing human identities. In the UAE, where AI, IoT, and cloud-based systems are quickly being integrated into nearly every sector, the sheer volume of machine identities is outpacing the ability to monitor, manage and protect them.

As the number of machine identities grows, managing their security becomes increasingly complex, and those with a siloed approach can create further risks. When different tools are used across various departments to manage machine identity security, it creates inefficiency, complexity, and management challenges, which all equate to risk. For example, responsibilities for preventing machine identity-related compromises are often fragmented, split between security, development and platform teams. This lack of coordination can leave gaps in security, making it harder to protect critical systems effectively.

In addition, organizations now need to protect a wide range of machine identities, with API keys (36%) and SSL/TLS certificates (34%) being the most challenging to secure, according to the CyberArk report. With more companies adopting cloud technologies and IoT devices, these difficulties will only grow further.

Issues such as quickly revoking certificates, tracking who has access, and keeping up-to-date inventories are all major hurdles. Yet, despite these rising challenges, many organizations globally (34%) still rely on manual processes to manage machine identities, which makes it harder to spot risks and respond quickly.

Three Pillars to improve Machine Identity Security

It's crucial that organizations in the UAE take steps to continue safeguarding their operations to protect themselves, their customers and partners, and contribute to the UAE's digitization strategy. Here are three strategies organizations can take to improve their machine identity security posture.:

1. Invest in Machine Identity Security: Organizations must continue to prioritize investing in robust machine identity security tools. These tools should focus on strong encryption, lifecycle management, and automatic identity rotation to ensure machine identities are constantly secure.
2. Leverage AI for Cybersecurity: Organizations in the UAE have a unique opportunity to apply AI-driven solutions to their cybersecurity efforts. AI-powered systems can detect unusual patterns in machine identity behavior, helping to spot potential attacks before they escalate.
3. Cybersecurity Training and Awareness: As machine identities continue to grow, so does the need for specialized cybersecurity training. UAE businesses should focus on educating their teams about the complexities of machine identity security and ensure that professionals are equipped to handle these new challenges.

Machine identities are reshaping the way businesses operate, but they also come with a new set of risks. For the UAE, which is embracing technology at a rapid pace, securing these identities will be critical for maintaining a safe and thriving digital economy.

SECURITY UNSEEN: UNPACKING PRESENT AND FUTURE VALUE OF RADAR AND THERMAL IMAGING

When formulating a security or perimeter protection plan, Middle Eastern enterprises are inclined to utilise as many independent surveillance and monitoring technologies as possible. While organisations would simply purchase and set up a collection of CCTV cameras dotted across a building or facility in the past, the ever-changing security needs of organisations today demand a more comprehensive and holistic approach, as well as solutions that go beyond traditional visual surveillance. It's also relevant for organisations to rethink their approach to visual surveillance, especially amidst increased privacy concerns surrounding surveillance cameras and systems in the region.

Radar and thermal imaging technologies serve as key components of that security approach. By complementing network cameras with radars and thermal cameras, organisations can unlock additional value from their physical security strategies, as well as tap recent innovations such as artificial intelligence (AI) and analytics to enhance their physical security resilience.

Where we started...

Developed in the 1940s, primarily for military and defence purposes, radar technology has evolved and now boasts a wide variety of applications across multiple industries, most notably in physical security. In 2017, Axis launched the world's first radar solution for surveillance purposes. AXIS D2110-VE Security Radar utilises advanced radar technology and intelligent algorithms to detect, classify, and track intruders in any given area. It was designed to work in tandem with other Axis security products such as a PTZ camera. In this case, information is sent to the camera, which then automatically activates and tracks the potential intruder.

Radar technology and thermal imaging allow you to see what visual cameras cannot. Devices can detect moving objects (people, vehicles, etc.) regardless of lighting conditions, or in environments where weather or operating conditions do not allow for adequate visual surveillance. This way, operators can improve their understanding of the surveyed area and be more accurate when it comes to detecting multiple objects. Their deployment alongside traditional visual cameras also helps to create a wide buffer zone and well-defined perimeter line thanks to two-layered security.

An innovation that warrants attention is visual cameras that are integrated with radar. Radar-video fusion cameras combine radar and video data for the purpose of the visual image – radar detections fused into the video image – with analytics, where the input from both sources is merged to enhance the output.

Magnus Lundegård, Global Product Manager and Niklas Lindman, Global Product Manager at Axis Communications

Where we're going...

There's a debate to be had around which technology is superior or whether they work best separately or together. But the fact is that radar and thermal imaging solutions, used in conjunction with video surveillance, let operators enjoy total coverage of an area. To achieve this, many solutions are designed to be compatible with major video management systems (VMS). They are also a practical solution in the event video surveillance cannot be used due to privacy restrictions, as people and their faces cannot be identified with thermal cameras or radars. Thermal imaging cannot be used for reliable identification so, along with radar, it enables operators to abide by any restrictions they may have to adhere to, while the technology itself is inherently secure.

However, the applicability of radar technology and thermal imaging extends beyond perimeter protection. The technologies offer real promise for road, traffic, and vehicle monitoring and management, especially in the Middle East where traffic-related incidents cost lives and can have severe annual economic consequences to the tune of hundreds of millions of dollars.

Using radar devices strategically placed across highway systems, traffic management centres and officials can detect and identify vehicles, how many there are, and at what speeds or directions they are traveling, culminating in reliable data and statistics that can improve decision-making. Meanwhile, thermal cameras give officials a means to see vehicles 24/7, regardless of the weather conditions.

One innovation that takes radar technology and thermal imaging forward is AI. Combined with radar, AI allows for enhanced object detection and classification to the point that it serves as the basis for trends such as autonomous driving. The goal is to minimise false alarms, and AI-based human and vehicle classifications, combined with modern intrusion detection analytics, make that possible by ignoring variable illuminations and moving objects such as vegetation that may cause moving shadows.

All this goes to show that radar technology and thermal imaging are still evolving. Cutting-edge devices and solutions represent not just a value in terms of security, but also a value in forward thinking. With the help of trusted manufacturers and vendors, organisations in the Middle East can leverage the full power of these technologies for their operations and projects.

"COMBINED WITH RADAR, AI ALLOWS FOR ENHANCED OBJECT DETECTION AND CLASSIFICATION TO THE POINT THAT IT SERVES AS THE BASIS FOR TRENDS SUCH AS AUTONOMOUS DRIVING."

MODERN PAM – THE MUST-HAVES AND BEST PRACTICES OF CYBERSECURITY'S NEW HEART

Our identity is important to all of us. And all of our identities are under attack. Routinely, nefarious parties strip mine our online presences to find ways of breaching our walls and counterfeiting our digital selves for their own ends. From a simple joyride to a more sinister bank heist, the modern citizen has much to fear from identity theft. But as much as we have to lose as individuals, our employers have even more at stake. Data-breach dollar-costs can reach the millions, and smaller companies may never recover. According to one report, in 2023 almost a third (32%) of businesses in the United Arab Emirates (UAE) endured an identity-fraud attack involving a deepfake video. From the perspective of cybersecurity, the protection of our identities must be given the highest priority.

To fulfil that promise, security teams often focus on accounts that have been granted privileged access to critical areas — systems, data, applications, and others — but IT infrastructure has become much too advanced for this approach to be effective on its own. Some instances of privilege are not etched in stone to be discovered by a simple survey. Some of today's environments confer access through on-premises privilege models or through roles and entitlements in cloud systems. Privileged Access Management (PAM) platforms, however, are still used by organizations to focus controls almost exclusively on administrative privileges that are directly assigned. But malicious actors rarely start their intrusions at the top. They frequently hijack non-admin user accounts and move laterally, worming their way towards greater and greater privilege.

User groups, misconfigurations, and overlooked cloud permissions — these are all features of the modern IT environment. The sprawling nature of the average tech stack offers more Paths to Privilege™ than ever but while the Paths are easy to exploit by attackers, they are obscured from the SOC's view. Traditional PAM is focused on internal visibility and on control of assigned privileges; and the tunnel vision of traditional identity-security tools means they offer little to plug the gaps. And so, we see growing numbers of non-IT users with high privilege levels. They are spread across the environment. They expand the attack surface. They must be addressed.

But how? Managing identity security across a hybrid IT environment that includes multiple domains is difficult when one also has the goal of enhancing productivity. Just as IT environments have changed, PAM must change. This adapted, modern PAM must plug the critical identity security gaps that traditional solutions cannot. Modern PAM must expand visibility, bolster protection measures, and tighten controls beyond those accounts with directly assigned privileges. It needs to provide coverage across on-premises, cloud, SaaS, OT, and more. It must be the ultimate authority over what is accessed by whom or by what.

To frame modern PAM into a broad check sheet, there are four must-haves that will form the foundation of all effective platforms.

A secret-keeper

Modern PAM must be capable of managing any type of secret, from the something-you-knows, like passwords, to the something-you-haves, like keys. The platform must be able to do this in any type of environment — on-premises data centers, remote work locations, and cloud environments, whether they be IaaS, PaaS, or SaaS.

Michael Byrnes, senior director – solutions engineering, META, BeyondTrust

A single-pane solution

Modern PAM should be holistic and allow for all use cases. It should deliver access management; it should deliver session monitoring. And everything should be available to security personnel through a single platform. There should be no need to hop from screen to screen to get a full view of the identity ecosystem.

A best-practice champion

Modern PAM must, of course, embrace the prevailing industry wisdom on identity security. Zero-trust, least-privilege, and just-in-time principles must all be in effect. The region's regulators must also be respected through advanced compliance reporting. With best practices in place, PAM is a silo no longer, but operates as a fully integrated component of a larger security strategy.

A firm foundation

Modern PAM sits at the heart of modern security suites, helping to redefine identity security and providing a foundation for securing all aspects of the identity and access management fabric.

More nooks, more crannies

PAM has always been preventative and will remain so. Modern PAM looks into more nooks and presses itself into more crannies than its predecessor. It proactively shrinks the attack surface by using the latest tools in its fight against aggressors. Modern PAM's defining trait is its proactiveness. What better tools to leverage in detecting and mitigating threats than AI- and ML-powered intelligence. Through AI, PAM becomes a core part of identity threat detection and response (ITDR).

Modern PAM is more than a toolbox. It is an enabler of productivity for IT admin, help desks, and end users. Far from being an obstacle to access, it enables faster access for those who need it — fewer authentication steps, less admin workload, and fewer raised tickets — all while creating a hardened, more identity-aware security posture. For example, traditional PAM finds it problematic to deliver just-in-time (JIT) access in cloud environments without the need for high-burden authentication that eats into productivity. Modern PAM is ideal in these scenarios because it is built around streamlined workflows that maintain security and auditability.

Our identities have always been under threat. There is no better way for fraudsters to defraud and thieves to thieve than to wear the skin of their victims. As environments have evolved, criminals have shown an uncanny knack of evolving with them. As potential victims, we too must evolve, and so must the tools of our defense. Modern PAM puts this notion into practice by employing a more intelligent approach to identity and privilege management. It eradicates identity-security blind spots, removes standing privileges, and decomplicates least-privilege. Turbocharged by AI, modern PAM clears the fog in front of the SOC, shines lights into hidden corners, and lays down the law on behalf of business strategists without ever blocking roads to achievement. Modern PAM is the new indispensable ally in our daily cyber-skirmishes.

"PRIVILEGED ACCESS MANAGEMENT (PAM) PLATFORMS, HOWEVER, ARE STILL USED BY ORGANIZATIONS TO FOCUS CONTROLS ALMOST EXCLUSIVELY ON ADMINISTRATIVE PRIVILEGES THAT ARE DIRECTLY ASSIGNED."

STRENGTHENING FACTORY OF THE FUTURE: HOW MIDDLE EAST MANUFACTURERS CAN SECURE DIGITAL FUTURE

At the onset of 2025, the outlook for the region's manufacturing sector looks bright. Manufacturing output is estimated to be around US$130 billion in Saudi Arabia and US$132 billion in the United Arab Emirates (UAE). Industry players understandably want to share in the growth inspired by government programs such as the UAE's Operation 300bn.

But though they may bring undeniable strides towards competitiveness, some popular emerging technologies enabling this growth are not without their caveats. Manufacturers continue to couple IT (information technology) and OT (operational technology) more tightly, turning to solutions in the edge-computing, IoT, and automation spaces. In an industry that can ill afford disruption, the cyberattack surface is expanding through the very modernisation of connectivity that was intended to make it more resilient.

In March 2024, a survey backed by the UAE Cyber Security Council revealed 155,000 vulnerable assets in the country. Alarmingly, more than 40% of their critical vulnerabilities had been unaddressed for more than five years. And a PwC report on the state of cyber-readiness in Saudi Arabia cited a 2022 finding of 110 million threats detected in the Kingdom in a single year. As regional surveys continue to predict inflated cyber-budgets and overwhelmed CISOs continue to express concern over the shifting threat landscape, manufacturing stands as one of the major sectors of concern.

Risk e-business

The problem lies in selective modernisation. For manufacturers, being offline is unthinkable, so they may connect IT and OT without due regard for the Internet-facing exposure of their mission-critical equipment. Assets that were difficult to patch in the past may have been left untouched and since they were unconnected to the outside world, such decisions did not result in any harm to the business. But with so many unpatched legacy assets now within reach of threat actors, the risk profile of the manufacturing enterprise has changed.

Concerns within the cybersecurity community are growing over the merger between OT and IT. Threat actors never leave an opening unexplored for long. If we are talking about it, they are thinking about it. And recent reports have flagged an uptick in incidents involving critical infrastructure and OT in both the UAE and Saudi Arabia. CIOs and CISOs in manufacturing firms will now have to work together to ensure they are not among the early victims of this new opening for threat actors.

The problem in protecting OT has always been skills. Equipment can be so specialised that even replacing a maintenance engineer can be a challenge. But to find cybersecurity skills in IT staff, much less engineers, is rare. And to find deep and proprietary engineering knowledge in a CISO is just as unlikely. This is where collaboration across IT, OT, and security will be critical for regional manufacturers. But do they have all those skills on hand? And if they do, do they have enough people in each position to ensure not only 24-7, 365-day coverage but also the right approach to strategy and IT/OT policy? A threat actor can keep trying to hammer on the door. They only need to find it unlocked once to prevail. Cyber-defenders must get it right every time. And with both skills gaps and heightened connectivity in play, threat actors are the most likely victors in the long run.

Look to the cloud

With some manufacturing solutions crossing cloud boundaries, the problem becomes all the more acute. It is impossible for a business with growth ambitions to ignore the scalability and

"MANUFACTURERS CONTINUE TO COUPLE IT (INFORMATION TECHNOLOGY) AND OT (OPERATIONAL TECHNOLOGY) MORE TIGHTLY, TURNING TO SOLUTIONS IN THE EDGE-COMPUTING, IOT, AND AUTOMATION SPACES."

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

cost benefits of the cloud. There are also collaboration advantages that are very attractive in a design-heavy sector like manufacturing. Additionally, it is in the cloud that modern businesses most commonly find advanced technologies like AI and machine-learning. But the cloud also represents a significant expansion of the attack surface, putting the onus on manufacturers to enhance their risk management so they can enjoy the full potential of cloud computing without falling prey to cyberthreats.

To add another layer of complexity, AI is just as ubiquitous a tool among threat actors as it is among legitimate organisations. Its global appeal in law-abiding circles, however, makes it another point of entry as well as an attack weapon. For the manufacturer, AI must therefore be thought of as a defensive tool but also as a tool to be defended. AI assets must be used responsibly by business users and used innovatively by technical users as they write business code and as they sift out and deploy countermeasures against malware in real time.

Manufacturers must examine their toolbox for weapons of defence. Many cloud-based solutions are equipped with security features out of the box that are sensitive to AI systems. Cloud platforms have similar offerings that can dial down risk while actually accelerating AI adoption. CIOs, OT specialists, and security professionals must work together to harden devices, patch software, and protect users. The right tool for the right asset is a challenging prospect in an environment with so many different types of assets. Sometimes it will not be possible to place technical protections on equipment because to do so would be too disruptive to the manufacturing process. In this event, its people are an enterprise's greatest defence. New skillsets must be developed to maintain trust between manufacturers and regulators. It will be up to technical and non-technical leaders to ensure employee training concentrates on the most relevant threats, like social engineering and credentials theft.

The PPT triad

People, processes, and technology. If regional manufacturers build their security posture around these fundamental elements, they can derisk their digital transformation and share in the industrial growth ahead.

2025 DEMANDS SMARTER BACKUP STRATEGY FOR INDIVIDUALS, BUSINESSES

"TAKE THE PLEDGE" TO PROTECT YOUR MOST VALUABLE DIGITAL ASSETS. DON'T BE AN APRIL FOOL. BACK UP YOUR FILES. YOUR FUTURE SELF WILL THANK YOU.

In a world increasingly dependent onc one accidental click, one failing hard drive, or one malicious ransomware attack can spell disaster. Imagine a photographer losing irreplaceable wedding photos due to a laptop crash, or a small business owner waking up to a completely wiped-out database. These scenarios, while terrifying, are all too real — and preventable. Enter World Backup Day, a global reminder on March 31 every year that in the digital age, safeguarding our data isn't just important, it's essential.

World Backup Day is more than a yearly reminder — it's a movement to instill digital resilience in a tech-centric world. Whether you're a student, an entrepreneur, or an IT manager, data loss can hit you hard. But the good news? Prevention is simple. A few minutes invested in a solid backup plan can save you from weeks of regret and thousands in losses.

What Is World Backup Day?

Held every year on March 31, World Backup Day was established in 2011 by concerned internet users on Reddit. Purposefully scheduled the day before April Fools' Day, the event carries a light-hearted but powerful message: losing your data is no joke. The campaign urges individuals and organizations to take a proactive approach to data protection by setting up and maintaining reliable backup systems.

Why It Matters More Than Ever in 2025

With 2025 marking new highs in cloud usage, mobile computing, and remote work, the sheer volume of digital data we generate daily is staggering. Simultaneously, the threats we face have also evolved: cyberattacks, phishing scams, natural disasters, and plain old human error. A recent industry report revealed that more than 40% of businesses that suffer major data loss shut down within a year. This isn't just about IT hygiene —

it's about long-term survival.

Backing up data regularly ensures that even in worst-case scenarios, your digital footprint — and everything it represents — remains intact.

Not all data is created equal, but anything important, irreplaceable, or business-critical deserves a place in your backup plan:

- For individuals: family photos and videos, personal documents, school or work files, emails, and contacts.
- For businesses: client information, employee records, financial statements, source code, digital assets, and customer communication histories.

A good practice is to categorize your data into tiers: what must be backed up daily, weekly, or monthly.

Backup Strategies That Work

The gold standard is the 3-2-1 Backup Rule:

- Keep three copies of your data.
- Store it on two different types of media (e.g., hard drive and cloud).
- Keep one copy offsite or in the cloud to protect against local failures.

This approach helps protect against multiple failure points. For example, if your laptop dies and your external drive is lost in transit, your cloud backup ensures your data isn't lost forever.

Tools and Services to Consider in 2025

The digital ecosystem is rich with powerful backup tools designed for every need:

For Personal Use:

- Google Drive: Seamless for Android users with powerful syncing.
- Apple iCloud: Ideal for iOS and Mac ecosystems.
- Dropbox and OneDrive: Reliable and easy to integrate.

For Businesses:

- Backblaze: Known for simplicity and affordable unlimited backup.
- Acronis: Comprehensive protection including anti-malware.
- Carbonite: A go-to for SMBs with automated backups.
- Veeam and AWS Backup: Enterprise-grade solutions with high scalability and security.

Look for features like automated scheduling, versioning, ransomware protection, and end-to-end encryption.

Mistakes to Avoid

Despite the availability of tools, many still fall into these common traps:

- Assuming cloud storage is backup: Cloud syncing tools like Google Drive mirror changes — including deletions.
- Not testing your backups: A backup that can't be restored is useless.
- Ignoring mobile devices: Phones hold immense personal and business data.
- Outdated media: Relying on CDs or old hard drives risks data corruption.

Backups & Cybersecurity: A Strategic Alliance

Cybersecurity and backups go hand-in-hand. Ransomware attacks are on the rise, and their impact can be catastrophic. Backups provide a crucial lifeline: instead of paying the ransom, companies can wipe affected systems and restore from a clean copy. Immutable backups — data that can't be altered once written — are particularly effective in these scenarios.

Your Digital Reset

- Audit your current backup strategy.
- Test your restoration process.
- Set or update automated schedules.
- Talk to your family, team, or business about data safety.

According to World Backup Day press release, people now create and generate over 1.8 zettabytes of data per year. That's a lot of data that we need to protect! Unfortunately, nearly 30% of people have never even backed up their data.

"I'm thrilled with the response to World Backup Day, and I hope it's made a difference in people's lives," said World Backup Day founder Ismil aJadun. "We all know someone who has lost critical data, whether it was their videos, photos,

music, book reports, or personal stuff. Hopefully this day will make everyone think about their situation, learn about the various options and get their files backed up. I hope that World Backup Day sparks conversations about the enormous task of saving our digital heritage for future generations."

Tahawaultech spoke to the following industry experts:

Ezzeldin Hussein

Regional Senior Director, Solution Engineering, META, SentinelOne

"Data loss isn't a question of "if"—it's "when."

This World Backup Day, proactive backups are your strongest defense against ransomware, accidental deletions, and system failures.

In an era of relentless cyber threats, businesses and individuals alike must ensure their critical data is secure, recoverable, and resilient. Whether through cloud-based solutions, offline storage, or immutable backups, a robust backup strategy is essential for business continuity and digital peace of mind. Take the World Backup Day pledge: Don't leave your data unprotected—back it up today and stay ahead of tomorrow's threats."

Harish Chib

Vice President Emerging Markets, Middle East & Africa, Sophos

In today's digital-first world, data is the backbone of every organization and it remains a top target for cybercriminals. The Sophos State of Ransomware report reveals, 94% of ransomware attacks include attempts to compromise backups—57% of which are successful. This stark reality underscores the need for organizations to adopt a robust backup strategy that ensures data remains secure and accessible, even in the face of evolving cyber threats. We urge businesses to not only back up their critical data but also to safeguard those backups with strong security measures. A resilient defense requires a multi-layered approach, including proactive risk assessment, endpoint protection, 24/7 threat monitoring, and a well-practiced incident response plan. Cybercriminals are relentless, but with the right strategy, organizations can ensure that their data—and their future—remain protected.

Rob T. Lee

Chief of Research at SANS Institute

We talk a lot about backing up data. But here's the question no one likes to answer: where does data go when it's no longer needed?

It doesn't just disappear.

Back in the day, I used to recover data from used hard drives. What I found were full digital lives left behind. Tax records. Business plans. Medical information. All still there. Unsecured. Forgotten.

Today, the situation is worse. Data lives everywhere now. In the cloud. On laptops. Phones. USBs. Shared drives. Devices we barely think about. The risk isn't limited to old hardware sitting in a closet. It's the active and forgotten data sitting on systems we no longer track.

When companies upgrade systems, shut down apps, or employees move on, what happens to the leftover data? Are we wiping it securely? Are we even keeping an inventory?

If you don't know where your data is, you can't know where it ends up.

On World Backup Day, yes, back up your data. But also think about what you leave behind. Because forgotten data is still out there. And it is very much recoverable.

Here are three ways to stop your business data from haunting you later.

1. Create a Full Data Inventory - You can't secure or delete what you don't know exists. Start with a complete audit—track where data lives across cloud services, devices, backup systems, and even personal employee hardware.
2. Build Data Disposal Into Every Offboarding and Upgrade - Whether it's an employee leaving or an entire system being decommissioned, have a process to securely wipe or destroy data. This should be as routine as collecting a badge or laptop.
3. Automate Retention and Destruction Policies - Use tools that enforce data retention rules. Data that's no longer needed shouldn't stick around for "just in case." Automate secure deletion timelines and make sure sensitive data has a digital expiration date.

Ram Vaidyanathan

Chief IT Security Evangelist, ManageEngine

We are reminded that protecting data requires a proactive and strategic approach. After all, data is arguably the most valuable asset for any organization. Effective backups are not just about storing copies of data—they are a critical component of disaster recovery and cybersecurity. It ensures rapid data restoration, minimizes downtime, and enables business continuity in the event of cyberattacks or system failures.

A risk-based approach to backups ensures that organizations prioritize their most critical data, aligning recovery strategies with business impact.
This starts with a risk assessment to identify the most business-critical and sensitive data. From here, businesses must define Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to establish limits to acceptable data loss, and maximum acceptable time for recovery. The overall goal is to build a resilient backup framework. Regular automated backups, offsite replication, encryption, and immutable storage are key to minimizing exposure to ransomware and data corruption. In today's evolving threat landscape, backup is an essential cybersecurity control.

Michael Cade

Global Field CTO at Veeam Software

It's no surprise things have changed since World Backup Day was established over a decade ago. Backups used to be seen as an afterthought, a measure you

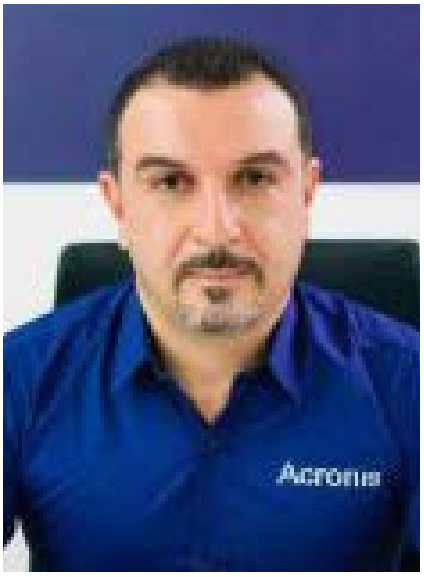
put in place and picked up when needed. But today, they need a core element of wider data resilience planning.Often targets of attacks themselves, backups need to level up to match these threats. Immutable backups need to be the standard, to keep backups tamper-proof, even when under attack. Following an attack, you need to be comfortable recovering from a backup you know is secure, with a tried-and-tested plan to get your systems operational again. While backups are vital, organizations can't just rely on backups alone, a business-wide cybersecurity plan needs to be in place as a first line of defence for ransomware attacks. Like backups themselves, World Backup Day needs to level up and evolve. It sparks great conversation, but it needs to go beyond talking just backups in isolation and cover the full data resilience picture.

Fred Lherault

Field CTO, EMEA / Emerging Markets, Pure Storage

Backing up data remains critical for data protection, but it's not enough. Implementing advanced data protection capabilities helps companies better plan for — and recover quickly from — ransomware and cyberattacks. This essentially requires a two-pronged approach: taking regular, immutable and indelible copies of data, and having the necessary infrastructure to rapidly restore from backups at speed and scale. In the event of a cyber attack, or any other event that compromises data or disrupts operations, companies can recover critical data from their immutable copies so that they can restore operations quickly — without having to succumb to the demands of cyber criminals. Proper immutability and indelibility means these copies cannot be changed in any way (such as encrypted), or as importantly, deleted by anyone, even if they manage to obtain the administrator's credentials. This makes them far more resilient and reliable in the event of a cyber attack.

Next comes the ability to restore data as fast as possible, as reliable backups are limited in their effectiveness if operations cannot be restored quickly. Some of the most advanced flash-based storage solutions dramatically increase the speed of data restoration. The leading solutions boast a recovery performance of up to many hundreds of TBs per hour at scale, enabling organisations to restore systems in hours — rather than weeks, so they can get up and running again with minimal impact.



Ziad Nasr

General Manager – Acronis Middle East

In an age where cyber threats, hardware failures, and accidental deletions are all too common, regular and tested backups are essential to ensure your data is safe and recoverable. At Acronis, we emphasize not only the importance of creating backups but also verifying them and keeping them secure. Backups are a cornerstone of any solid cybersecurity strategy — because when data loss happens, your backup is your best defense.

Rich Murr

Chief Customer Officer & Chief Information Officer at Epicor

What we're seeing is that moving to the cloud is a game-changer for businesses when it comes to compliance and data security. For businesses using cloud-based ERP software, having all their data in one place simplifies compliance with regulations like GDPR and CCPA. Regular risk assessments and proactive measures are easier to manage in the cloud. Compliance frameworks such as ISO 27001, SOC 2, and PCI DSS are often built into cloud solutions, helping businesses stay ahead of potential vulnerabilities. Most of our new business is now in the cloud, and it's clear why: it helps businesses avoid penalties and build a reputation for trust and integrity.

Robert Standing

Regional Vice President, Middle East & Africa, Rubrik

A strong cyber resilience strategy goes beyond backup and recovery—it involves continuous testing, real-time threat detection, and a proactive approach to security. Backup systems must be regularly tested and validated to ensure they are effective when needed most. This means more than just backing up data—it's about assessing the integrity of backups and recovery procedures through continuous simulations of real-world cyberattack scenarios. By doing so, you can ensure that your organization is truly prepared for the worst-case scenario.

Eun-Kyung Hong

Senior Specialist Product Marketing Management, Storage Products Division, Toshiba Electronics Europe GmbH

Data is increasingly recognised as one of our most valuable assets, the significance of data backup cannot be overstated – yet consumer awareness levels remain relatively low. Consumers need to take control of their digital lives. Our smartphones store photos, videos, contacts, passwords, and more. Most people use some form of cloud storage for backup, but relying on it as a sole solution is not recommended. It is best practice to perform regular backups using different methods.

WESTERN DIGITAL GLOBAL WORLD BACKUP DAY SURVEY FINDS WHOPPING 87% ACTIVELY BACKUP THEIR CONTENT

DESPITE POSITIVE MOMENTUM, MANY STILL FACE CHALLENGES WITH STORAGE LIMITS, TIME CONSTRAINTS AND AWARENESS

Consumers have become more reliant on personal data for everything from health records, financial documents, home video and photos, social media videos and more, and many are realizing the importance of backing up data.

Western Digital announced the results of a global research study by Researchscape, where 87% of respondents cite that they backup their data automatically or manually. The top reasons for backing up personal data are fear of losing important files (83%), to free up space on their device (67%) and to protect against cyber threats (42%). 19% do it because they were told to.

"It's fantastic to see more people recognizing the importance of protecting their data," said Nitin Kachhwaha, Director of Product Management at Western Digital. "World Backup Day is an important yearly reminder to everyone to backup their data and to educate the people who still aren't aware of the impact of failing to backup. It's also an

opportunity to reinforce just how critical it is to safeguard what matters most—because all it takes is one small accident for data to be lost forever. In fact, 63% of respondents have already experienced data loss due to device failure, accidental deletion or cyberattacks."

For those respondents who do not backup their personal data, 36% still think they don't need to backup their data, 30% don't have enough storage space, 29% think it takes too much time, and 23% don't know how. 63% of respondents agree that they would backup data more frequently if it was automatic and effortless.

A dependable backup practice is to follow the 3-2-1 backup strategy, where consumers should have three copies of data, stored on two different types of media with one copy stored offsite, like in the cloud.

With free cloud storage limits quickly maxing out, many consumers are turning to a hybrid approach to protect their data. In the survey, 78% of respondents reported that they rely on free cloud storage, 60% have run out of space in the past six months, and 56% have had to upgrade to paid plans. Additionally, 35% find cloud storage increasingly expensive. This is driving more people to adopt a combination of both cloud and local external storage to ensure data protection and cost efficiency. External HDD storage, offering up to 26TB in a single drive, provides a cost-effective solution to complement the cloud, and many consumers are already embracing this approach — 45% use an external HDD, while 19% rely on network-attached storage (NAS). By diversifying storage methods, users can maintain reliable backups while managing growing cloud costs.

Western Digital provides consumers and businesses alike with easy-to-use data storage solutions that streamline the backup process and meet today's growing storage needs. Western Digital recently unveiled higher capacities across its portfolio, including a 26TB1 WD Red® Pro CMR HDD for NAS environments and the WD My Passport, 20th Anniversary Edition with industry-leading 2.5" portable HDD capacity of up to 6TB. WD My Passport devices also include Acronis® True Image for Western Digital software to more easily schedule backups of precious data.

In addition to these storage solutions, Western Digital is offering exclusive deals on some of its most popular backup products, making it even easier to protect and manage digital data.

The results in this report are from an online survey of 6,118 respondents that was fielded from February 7 to 25, 2025 by Researchscape, an international market research consultancy. Respondents were from 10 different countries.

HOW TO PREVENT WHATSAPP ACCOUNT FROM BEING HACKED: KASPERSKY RECOMMENDATIONS

User's messaging app account might be of interest not only to jealous spouses and nosy coworkers, but also to cybercriminals. Stolen WhatsApp accounts are used for various types of criminal activity, ranging from spam distribution to sophisticated scam schemes. Cybercriminals constantly look for WhatsApp accounts and use various methods to gain access to them.

There are two ways cybercriminals can gain control of a WhatsApp account: they can add another device to an existing account using the "Linked devices" feature, or they can re-register the account on their own device as if the user had bought a new phone. In the first case, the user continues to use WhatsApp as usual, but the criminals also have access to all recent conversations. In the second case, the user loses access to their personal account. When trying to log in, WhatsApp notifies him that the account is already in use on another device, and the attackers can then control the account but not the past conversations.

"Messengers are a private space, as they often contain personal information about our lives and relationships with family and friends. They can also contain information about work and, in some cases, confidential information. If you notice any unusual activity, such as receiving replies to messages that you didn't send, or if your friends complain about strange messages coming from your account, it's important to take steps to protect your privacy immediately," said Seifallah Jedidi, Head of Consumer Channel, META, at Kaspersky.

While you can check instruction on what to do in case WhatsApp account was already compromised, here are the key steps on how to avoid WhatsApp account to be hacked:

- Enable two-step verification in WhatsApp and memorize your PIN — it's not a one-time code. To do this, go to Settings → Account → Two-step verification.
- Never, ever share your PIN or one-time registration codes with anyone. Only scammers ask for these details.
- WhatsApp recently introduced support for passkeys. If you enable this option (Settings → Account → Passkeys), logging in to your account will require biometric authentication, and instead of PIN codes, your smartphone will store a long cryptographic key. This is a very secure option, but it may not be convenient if you frequently change devices and switch between Android and iOS.
- Set up a backup email address for account recovery: Settings → Account → Email address.
- If you've already added an email address, log in to your email account and change your password to a strong, unique one. To store it securely, use a password manager, such as Kaspersky Password Manager.
- Enable two-factor authentication for your email account.
- Make sure you haven't fallen victim to a SIM swap scam. Contact your mobile carrier — preferably in person — and verify that no duplicate SIM cards have recently been issued for your number. Also, make sure there's no unauthorized call-forwarding set up on your number. Cancel any suspicious changes and ask the staff about additional security measures for

your SIM card. These may include prohibiting SIM-related actions without your being present, an extra password required for authentication, or other protections.

Available security measures vary significantly by country and mobile carrier.

Any security measures in WhatsApp will be of little use if your smartphone or computer is infected with malware. Therefore, be sure to install comprehensive protection like Kaspersky Premium on all your devices.

"MESSENGERS ARE A PRIVATE SPACE, AS THEY OFTEN CONTAIN PERSONAL INFORMATION ABOUT OUR LIVES AND RELATIONSHIPS WITH FAMILY AND FRIENDS. THEY CAN ALSO CONTAIN INFORMATION ABOUT WORK AND, IN SOME CASES, CONFIDENTIAL INFORMATION. IF YOU NOTICE ANY UNUSUAL ACTIVITY, SUCH AS RECEIVING REPLIES TO MESSAGES THAT YOU DIDN'T SEND, OR IF YOUR FRIENDS COMPLAIN ABOUT STRANGE MESSAGES COMING FROM YOUR ACCOUNT, IT'S IMPORTANT TO TAKE STEPS TO PROTECT YOUR PRIVACY IMMEDIATELY."

– SEIFALLAH JEDIDI, HEAD OF CONSUMER CHANNEL, META, AT KASPERSKY

SOPHOS REPORT FINDS IN 56% OF INCIDENT RESPONSE AND MDR CASES, ADVERSARIES LOGGED IN, INSTEAD OF BREAKING IN

IR AND MDR CASES HIGHLIGHT ATTACKERS ARE EXFILTRATING DATA IN JUST THREE DAYS COMPROMISED CREDENTIALS TOP ROOT CAUSES FOR SECOND YEAR

Sophos, a global leader of innovative security solutions for defeating cyberattacks, today released the 2025 Sophos Active Adversary Report, which details attacker behavior and techniques from over 400 Managed Detection and Response (MDR) and Incident Response (IR) cases in 2024. The report found that the primary way attackers gained initial access to networks (56% of all cases across MDR and IR) was by exploiting external remote services, which includes edge devices such as firewalls and VPNs, by leveraging valid accounts.

The combination of external remote services and valid accounts aligns with the top root causes of attacks. For the second year in row, compromised credentials were the number one root cause of attacks (41% of cases). This was followed by exploited vulnerabilities (21.79%) and brute force attacks (21.07%).

Understanding The Speed of Attacks

When analyzing MDR and IR investigations, the Sophos X-Ops team looked specifically at ransomware, data exfiltration, and data extortion cases to identify how fast attackers progressed through the stages of an attack within an organization. In those three types of cases, the median time between the start of an attack and exfiltration was only 72.98 hours (3.04 days). Furthermore, there was only a median of 2.7 hours from exfiltration to attack detection.

"Passive security is no longer enough. While prevention is essential, rapid response is critical. Organizations must actively monitor networks and act swiftly against observed telemetry. Coordinated attacks by motivated adversaries require a coordinated defense. For many organizations, that means combining business-specific knowledge with expert-led detection and response. Our

John Shier, field CISO, Sophos

report confirms that organizations with proactive monitoring detect attacks faster and experience better outcomes," said John Shier, field CISO.

Other Key Findings from the 2025 Sophos Active Adversary Report:

- **Attackers Can Take Control of a System in Just 11 Hours:** The median time between attackers' initial action and their first (often successful) attempt to breach Active Directory (AD) - arguably one of the most important assets in any Windows network – was just 11 hours. If successful, attackers can more easily take control of the organization.
- **Top Ransomware Groups in Sophos Cases:** Akira was the most frequently encountered ransomware group in 2024, followed by Fog and LockBit (despite a multi-government takedown of LockBit earlier in the year).
- **Dwell Time is Down to Just 2 Days:** Overall, dwell time – the time from the start of an attack to when it is detected – decreased from 4 days to just 2 in 2024, largely due to the addition of MDR cases to the dataset.
- **Dwell Time in IR Cases:** Dwell time remained stable at 4 days for ransomware attacks and 11.5 days for non-ransomware cases.
- **Dwell Time in MDR Cases:** In MDR investigations, dwell time was only 3 days for ransomware cases and just 1 day for non-ransomware cases, suggesting MDR teams are able to more quickly detect and respond to attacks.
- **Ransomware Groups Work Overnight:** In 2024, 83% of ransomware binaries were dropped outside of the targets' local business hours.
- Remote Desktop Protocol Continues to Dominate: RDP was involved in 84% of MDR/IR cases, making it the most frequently abused Microsoft tool.

To shore up their defenses, Sophos recommends that companies do the following:

- Close exposed RDP ports.
- Use phishing-resistant multifactor authentication (MFA) wherever possible.
- Patch vulnerable systems in a timely manner, with a particular focus on internet-facing devices and services.
- Deploy EDR or MDR and ensure it is proactively monitored 24/7.
- Establish a comprehensive incident response plan and test it regularly through simulations or tabletop exercises.

TREND MICRO PREDICTS RISE OF DEEPFAKE-POWERED MALICIOUS DIGITAL TWINS

OVER 188 MILLION THREATS WERE BLOCKED IN THE REGION DURING H1 2024 BY TREND MICRO, WHILE ANTICIPATING A SURGE IN AI-POWERED ATTACKS AND RANSOMWARE TACTICS IN 2025.

Trend Micro Incorporated, a global cybersecurity leader, has unveiled its 2025 cybersecurity predictions report, titled, The Easy Way In/Out: Securing The Artificial Future. The report highlights a surge in AI-powered attacks and the emergence of hyper-personalized, deepfake-driven threats.

As cybercrime is projected to cost over $10 trillion in 2025, consumer data is expected to be a prime target, fueling the underground economy. Criminals are anticipated to continue evolving their tactics to exploit vulnerabilities, with AI accelerating these efforts to enhance, speed up, and improve malicious operations, particularly through social engineering schemes that prey on user vulnerabilities.

Trend Micro predicts the emergence of malicious "digital twins," leveraging leaked personal information to create AI models mimicking individuals' behaviors. When paired with deepfake video/audio and compromised biometric data, these twins could drive advanced social engineering scams, such as business email compromise (BEC), fake employee schemes, and large-scale misinformation campaigns.

The 2025 Trend Micro Security Predictions report underscores Trend Micro's strong commitment to cybersecurity. This dedication is further evidenced in the Trend Micro Mid-Year Cybersecurity Report for H1 2024, which details how the company's sophisticated solutions successfully detected and blocked over 188 million threats in the MENA region.

"Cybersecurity in an AI-driven world demands foresight and expertise," said Tarek Jammoul, North Gulf & Levant Country Director, Trend Micro. "Our deep understanding of emerging threats enabled us to craft the 2024 Security Predictions Report, equipping businesses with the insights needed to face the future with confidence. This same expertise powers our cutting-edge solutions, which detected and blocked over 4.9 million threats in Kuwait alone during H1 2024, reaffirming our commitment to securing the region's digital future."

The 2025 Security Predictions Report also highlights critical areas of concern, including vulnerabilities like memory corruption bugs, API exploits, and legacy issues such as cross-site scripting and SQL injections, as well as the cascading risks from vulnerabilities in widely adopted systems like connected vehicle ECUs. In ransomware, threat actors are expected to outpace endpoint detection and response (EDR) advancements by exploiting under-protected environments such as cloud systems, IoT, and edge devices, while using techniques like disabling security tools, and disguising harmful codes. These developments signal the rise of faster, stealthier, and more sophisticated attack chains, underscoring the need for robust, proactive security strategies.

"CYBERSECURITY IN AN AI-DRIVEN WORLD DEMANDS FORESIGHT AND EXPERTISE."

– TAREK JAMMOUL, NORTH GULF & LEVANT COUNTRY DIRECTOR, TREND MICRO

تحت الرعاية السامية لصاحب الجلالة الملك محمد السادس

Under the High Patronage of His Majesty King Mohammed VI

GITEX AFRICA Morocco

UNDER THE AUTHORITY OF | IN PARTNERSHIP WITH | ORGANISED BY

14 - 16 APRIL 2025 MARRAKECH

Defining Africa's Future with AI Impact

AFRICA'S LARGEST TECH AND STARTUP EVENT JUST GOT BIGGER

45,000 ATTENDEES

1,500 EXHIBITING & STARTUP COMPANIES

650+ GOVERNMENT REPRESENTATIVES

130+ COUNTRIES REPRESENTED

435 MEDIA ATTENDEES

660+ SPEAKERS

FEATURING THE LASTEST SOLUTIONS & THOUGHT LEADERSHIP:

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

/gitexafrica

GET YOUR TICKETS TO VISIT

LAST CHANCE TO EXHIBIT


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