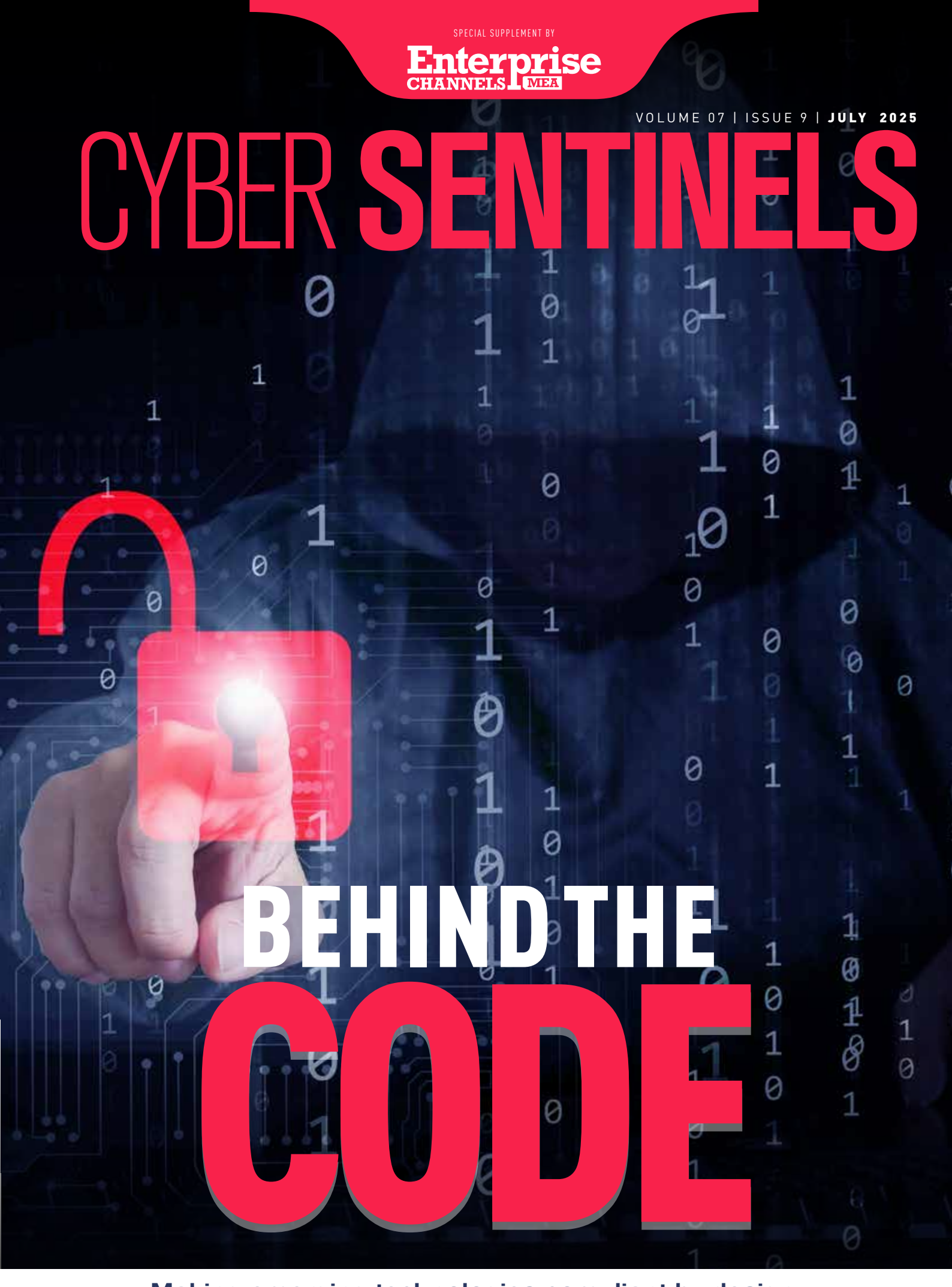
SPECIAL SUPPLEMENT BY
Enterprise CHANNELS MEA
VOLUME 07 | ISSUE 9 | JULY 2025

# CYBER SENTINELS



# BEHIND THE CODE

Making emerging technologies compliant by design.

GLOBAL CISO FORUM

PRESENTS

# GLOBAL SECURITY SYMPOSIUM

9TH EDITION

2025

# SEC_RITY IS NOT COMPLETE WITHOUT U!

16 APRIL - **KSA** | 10 MAY - **PAKISTAN**

19 JUNE - **QATAR** | 10 SEPTEMBER - **UAE**

11 NOVEMBER - **INDIA (MUMBAI)**

**#AI-Driven Security, Governance, Risk and Compliance**

EDITORIAL

# A new era of accountability

**JEEVAN THANKAPPAN**
jeevan@gcemediagroup.com

The GCC countries are stepping into a new era—one marked not just by digital innovation, but by a long-overdue reckoning with personal data protection and privacy.

Until recently, data privacy frameworks across much of the GCC were either limited in scope or nonexistent. But the tides are turning. Several GCC states are now implementing comprehensive, standalone data protection laws, aligning themselves with global standards such as the EU's GDPR. This transformation is not only redefining the regulatory landscape but also compelling enterprises to rethink how they manage, store, and process data—especially in the age of AI and IoT.

AI and IoT systems are at the forefront of the GCC's digital transformation efforts, but they present unique compliance challenges. AI models often rely on massive datasets that include personal, health, and behavioral data. IoT devices, meanwhile, collect and transmit private information at an unprecedented scale—often outside the boundaries of traditional IT oversight. In a region as interconnected as the GCC, where cross-border data flows are essential for economic integration, this creates a privacy minefield.

As IoT becomes ubiquitous—from smart homes to industrial control systems—the volume and sensitivity of data it generates raise difficult questions about sovereignty and individual rights. Who owns the data? Where is it processed? And under what jurisdiction? These questions are no longer hypothetical—they are being codified into law.

To safeguard user privacy in an AI- and IoT-heavy environment, GCC regulators must ensure that their laws not only mirror international standards but also address local and regional nuances. This includes building clear rules around data residency, cross-border transfers, consent mechanisms, and the right to be forgotten.

For enterprises operating in the GCC, this regulatory shift requires more than just compliance checklists—it demands a cultural shift toward "compliance by design." Technologies that power innovation must now integrate privacy and security at every level, from data ingestion and storage to model explainability and lifecycle governance.

CYBER **SENTINELS**

**PUBLISHER**
TUSHAR SAHOO
tushar@gecmediagroup.com

**CO-FOUNDER & CEO**
RONAK SAMANTARAY
ronak@gecmediagroup.com

**MANAGING EDITOR**
Jeevan Thankappan
jeevan@gcemediagroup.com

**ASSISTANT EDITOR**
Rehisha Pallikkathodi
rehishap@gcemediagroup.com

**CHIEF STRATEGY OFFICER**
ANUSHREE DIXIT
anushree@gecmediagroup.com

**GROUP SALES HEAD**
RICHA S
richa@gecmediagroup.com

**PROJECT LEAD**
JENNEFER LORRAINE MENDOZA
jennefer@gecmediagroup.com

**SALES AND ADVERTISING**
RONAK SAMANTARAY
ronak@gecmediagroup.com
Phone: + 971 555 120 490

**Content Writer**
KUMARI AMBIKA

**IT MANAGER**
VIJAY BAKSHI

**DESIGN TEAM**
**CREATIVE LEAD**
AJAY ARYA

**SENIOR DESIGNER**
SHADAB KHAN

**GRAPHIC DESIGNER**
TUBA KHAN

**PRODUCTION, CIRCULATION, SUBSCRIPTIONS**
info@gecmediagroup.com

**DESIGNED BY**
THE C2S
DESIGN • MARCOM • BRANDING

**SUBSCRIPTIONS**
info@gecmediagroup.com

**PRINTED BY**
Al Ghurair Printing & Publishing LLC.
Masafi Compound, Satwa, P.O.Box: 5613, Dubai, UAE

GEC Global Enterprise Connect

**(UAE)** Office No #115
First Floor , G2 Building
Dubai Production City
Dubai, United Arab Emirates
Phone : +971 4 564 8684

**(USA)** 31 FOXTAIL LAN,
MONMOUTH JUNCTION,
NJ - 08852
UNITED STATES OF AMERICA
Phone :+ 1 732 794 5918

**A PUBLICATION LICENSED BY**
International Media Production Zone, Dubai, UAE

OPX TECHNOLOGY

# DRIVING OPERATIONS AND PERFORMANCE EXCELLENCE

YOUR PARTNER FOR

Cloud & Digital Transformation

Enterprise Applications

Analytics & Automation AI & ML as a Service

Cyber Security Solutions

Management Consulting, Advisory and Quality Assurance

An unit of

OPX AMERICA

"Delivery centres in US, Middle East and India"

Phone: +971528732716 | Email: hello@opx–america.com | www.opxtechnology.com

# CONTENTS

JULY 2025


## OPINION



## INTERVIEW

**Rob Harrison,**
Senior Vice President, Product Management at Sophos

# Sophos Managed Risk adds Internal Attack Surface Management to help mitigate internal vulnerabilities

Sophos, a global leader of innovative security solutions for defeating cyberattacks, announced the expansion of its Sophos Managed Risk capabilities with the introduction of Internal Attack Surface Management (IASM) with technology powered by Tenable.

Many organizations face critical blind spots in their cyber defences. In fact, the Sophos State of Ransomware 2025report found 40% of organizations impacted by ransomware in the last year reported falling victim due to an exposure they were unaware of. Sophos Managed Risk, now with both internal and external attack surface management, addresses this challenge, providing comprehensive visibility into internal and external weaknesses that could be exploited by threat actors.

"With Sophos Managed Risk, organizations gain an attacker's-eye view to identify and prioritise remediation of risks before adversaries can exploit them. The solution offers a unified view of both internal and external exposures, prioritised by risk and paired with clear remediation guidance," said Rob Harrison, Senior Vice President, Product Management at Sophos. "This enables organizations to focus their efforts where it matters most, on the most critical vulnerabilities, resolving them rapidly."

The latest release of Sophos Managed Risk introduces unauthenticated internal scanning, which assesses a system from the perspective of an external attacker without user credentials or privileged access. This enables organizations to identify and mitigate high-risk vulnerabilities, such as open ports, exposed services, and misconfigurations that are accessible and potentially exploitable by attackers.

# SentinelOne recognized as a 2025 Gartner Peer Insights strong performer for cloud security posture management tools

**Ely Kahn,**
Vice President of Product Management at SentinelOne

SentinelOne, a global leader in AI-powered security, announced that it has been named a 'Strong Performer' in the 2025 Gartner Peer Insights 'Voice of the Customer' for Cloud Security Posture Management tools (CSPM) report.

It's the latest recognition for SentinelOne which recently was positioned as a 2025 Customers' Choice in the Voice of the Customer for Extended Detection and Response (XDR), a 2024 Customer's Choice in the Voice of the Customer for Cloud-Native Application Protection Platforms (CNAPP), and a 2024 Customer's Choice in the Voice of the Customer for Managed Detection and Response (MDR).

Users provided reviews of Singularity Cloud Security in the Cloud Security Posture Management Tools category on Gartner Peer Insights as of February 2025. 100% said they would recommend and 100% rated the solution four stars or better.

"We believe that being named as a Strong Performer in the Gartner Peer Insights Voice of the Customer for Cloud Security Posture Management is a testament to the value our platform delivers every day. Cloud environments are growing more complex, and organizations need solutions that go beyond traditional security tools. At SentinelOne, we're redefining CSPM with an AI-powered, unified approach that enables continuous monitoring, automated policy enforcement, and actionable threat intelligence at scale.

This recognition underscores our commitment to helping customers gain the visibility, control, and confidence they need to protect their cloud infrastructure with speed and precision." said Ely Kahn, Vice President, Product Management, SentinelOne.

# Tenable research finds rampant cloud misconfigurations exposing critical data and secrets

**Ari Eitan,**
Director of Cloud Security Research, Tenable

Tenable, the exposure management company, released its 2025 Cloud Security Risk Report, which revealed that 9% of publicly accessible cloud storage contains sensitive data. Ninety-seven percent of such data is restricted or confidential, creating easy and prime targets for threat actors.

Cloud environments face dramatically increased risk due to exposed sensitive data, misconfigurations, underlying vulnerabilities and poorly stored secrets – such as passwords, API keys and credentials. The 2025 Cloud Security Risk Report provides a deep dive into the most prominent cloud security issues impacting data, identity, workload and AI resources and offers practical mitigation strategies to help organizations proactively reduce risk and close critical gaps.

"Despite the security incidents we have witnessed over the past few years, organizations continue to leave critical cloud assets, from sensitive data to secrets, exposed through avoidable misconfigurations," said Ari Eitan, Director of Cloud Security Research, Tenable.

"The path for attackers is often simple: exploit public access, steal embedded secrets or abuse overprivileged identities. To close these gaps, security teams need full visibility across their environments and the ability to prioritise and automate remediation before threats escalate. The cloud demands continuous, proactive risk management, and not reactive patchwork."

# Nearly half of companies in the UAE opt to pay the ransom, Sophos report finds

Sophos, a global leader of innovative security solutions for defeating cyberattacks, released its sixth annual State of Ransomware report, a vendor-agnostic survey of IT and cybersecurity leaders across 17 countries that studies the impact of ransomware attacks on businesses. This year's survey found that nearly 50% of companies globally paid the ransom to get their data back – the second highest rate of ransom payment for ransom demands in six years.

While 43% of organizations in the UAE that had data encrypted paid the ransom, 30% of them paid less than the original demand. Globally, in 71% of cases where the companies paid less, they did so through negotiation – either through their own negotiations or with help from a third party. In fact, while the median global ransom demand dropped by a third between 2024 and 2025, the median global ransom payment dropped by 50%, illustrating how companies are becoming more successful at minimising the impact of ransomware.

Overall, the median ransom payment in the UAE was 1.33 million dollars, although the initial demand varied significantly depending on organization size and revenue. Across the globe, the median ransom demand for companies with over $1 billion in revenue was five million dollars, while organizations with $250 million revenue or less, saw median ransom demands of less than $350,000.

**Chester Wisniewski,**
Director, Field CISO, Sophos

**Ric Smith,** President of Product, Technology, and Operations, SentinelOne

## SentinelOne teams with AWS to bring best in class cloud security protection to customers

SentinelOne, a global leader in AI-powered security, announced that it is a launch partner for the new AWS Security Hub. The new collaboration builds on a long standing partnership between the two companies focused on co-developing the best AI-powered cybersecurity for customers running and scaling their businesses on AWS.

Designed to detect, prioritise, and help remediate critical risks, AWS Security Hub correlates signals from multiple sources such as threat detection and vulnerability management. It enriches these signals with visualisations, natural language summaries, and automated response workflows to help organizations improve security posture, enhance decision-making, and minimize operational disruptions.

As part of the partnership, highly enriched and correlated data findings in the AWS Security Hub can be ingested into SentinelOne's Singularity Platform for AI-powered detection and response leveraging agentic AI capabilities in SentinelOne's Purple AI as well as automated security workflows with Hyperautomation.

"Co-building with AWS is one of the most valuable ways we plan to help customers meet their evolving security goals," said Ric Smith, President of Product, Technology, and Operations, SentinelOne. "Our partnership with AWS Security Hub brings deep integrations that deliver the clarity, speed, and automation security teams need to defend complex cloud environments."

## UAE employees outpace EMEA peers in cyber confidence and readiness, new Cohesity study reveals

**Johnny Karam,** Managing Director Vice President of International Emerging region at Veritas Technologies

**Mark Molyneux,** EMEA Chief Technology Officer at Cohesity

Cohesity, a leader in AI-powered data security and resilience, released the findings of a new study examining employee preparedness in the face of cyber threats. The research shows that the UAE workforce is ahead of its EMEA peers across several indicators of cyber-readiness, underscoring the country's progress toward its national vision for digital resilience and AI-enabled defence.

Conducted among full-time office workers in the UAE, United Kingdom, France, and Germany, the study assessed how confident employees feel in identifying and responding to cyberattacks. Among the standout results, 86 percent of UAE employees expressed confidence in recognising a cyber threat—compared to 81 percent in the UK, 80 percent in Germany, and just 62 percent in France. Nearly nine in ten (89%) UAE respondents also said they trust their organisation's ability to prevent and recover from attacks.

Beyond awareness, the study reveals encouraging signs of action-oriented behaviour. Two-thirds of UAE employees say they would report suspicious activity to their cybersecurity team, showing an apt response, in comparison to respondents from the UK (61%), Germany (53%), and France (48%). Amongst other UAE employees, over half would notify their IT department. This instinct to act is supported by ongoing education: 66 percent have received some form of cybersecurity training in the past year.

# Mindware adds defense-grade cybersecurity to its portfolio through Everfox distribution deal

Mindware has signed a distribution agreement with Everfox (formerly Forcepoint Federal), strengthening its cybersecurity offering with a portfolio of high-assurance solutions trusted by government and critical infrastructure sectors worldwide. Under this agreement, Mindware will distribute Everfox's advanced cybersecurity technologies across the United Arab Emirates, Saudi Arabia, Oman, Kuwait, Bahrain, Pakistan, Yemen, Qatar, Egypt, Jordan, Lebanon, Iraq, Libya, Algeria, Tunisia, Côte d'Ivoire, Mali, Mauritania, Senegal, Cameroon and Congo. With a proven track record spanning more than 25 years, Everfox specialises in defense-grade cybersecurity solutions that safeguard sensitive data and networks from sophisticated threats. Its portfolio—spanning Cross Domain, Threat Protection and Insider Risk solutions—enables government and enterprise organizations to secure data access and movement across environments without compromise. Through this partnership, Mindware's channel partners can now offer clients cutting-edge tools designed to combat insider threats, contain malware, and protect against zero-day attacks in the most demanding operational contexts.

Nicholas Argyrides, Vice President – Gulf & East Africa at Mindware (L) and Shaun Bierweiler, Chief Revenue Officer at Everfox (R)

"Partnering with Everfox adds a new layer of strength to our cybersecurity portfolio," said Nicholas Argyrides, Vice President – Gulf & East Africa at Mindware. "Their high-assurance solutions are a natural fit for our region, where governments and enterprises are demanding advanced protection against increasingly complex threats. With this addition, we're equipping the market with technologies trusted to secure some of the world's most sensitive environments."

# Cloudflare thwarts record-breaking 7.3 Tbps DDoS attack

In mid-May 2025, Cloudflare blocked the largest DDoS attack ever recorded: a staggering 7.3 terabits per second (Tbps). This comes shortly after the publication of the company's DDoS threat report for 2025 Q1 on April 27, 2025, where it highlighted attacks reaching 6.5 Tbps and 4.8 billion packets per second (pps).

The attack targeted a Cloudflare customer, a hosting provider, that uses Magic Transit to defend their IP network. Hosting providers and critical Internet infrastructure have increasingly become targets of DDoS attacks, as was reported in Cloudflare's latest DDoS threat report.

37.4 terabytes is not a staggering figure in today's scales, but blasting 37.4 terabytes in just 45 seconds is. It's the equivalent to flooding your network with over 9,350 full-length HD movies, or streaming 7,480 hours of high-definition video nonstop (that's nearly a year of back-to-back binge-watching) in just 45 seconds. If it were music, you'd be downloading about 9.35 million songs in under a minute, enough to keep a listener busy for 57 years straight. Think of snapping 12.5 million high-resolution photos on your smartphone and never running out of storage—even if you took one shot every day, you'd be clicking away for 4,000 years — but in 45 seconds.


This attempted takedown was not just a technical anomaly—it was a serious threat to the stability of the digital world. Cloudflare's advanced protection systems automatically detected and neutralized the massive wave of malicious traffic in real time, without any disruption to the targeted services.

**Greg O'Connell,**
VP, Federal Sales, Public Sector at Nutanix

## Nutanix study finds public sector embraces generative AI, but faces security, skills, and infrastructure gaps

Nutanix, a leader in hybrid multicloud computing, announced the findings of its seventh annual global Public Sector Enterprise Cloud Index (ECI) survey and research report, which measures enterprise progress with cloud adoption in the industry. The research showed that 83% of public sector organizations have a GenAI strategy in place, with 54% actively implementing, and 29% preparing for implementation.

As public sector organizations ramp up GenAI adoption, 76% of IT decision-makers say their current infrastructure needs moderate to significant improvement to support modern, cloud native applications at scale. This year's public sector ECI found that infrastructure modernization emerged as a top priority, underscoring the growing demand for systems capable of meeting GenAI's requirements for enterprise-ready data security, data integrity, and resilience.

This year's report also revealed that public sector leaders are increasingly leveraging GenAI applications/workloads into their organizations. Real-world GenAI use cases across the public sector gravitate towards constituent/employee support and experience solutions (e.g., chatbots) and content generation. However, concerns remain with 92% of public sector leaders highlighting the need for their organizations to do more to secure GenAI models and applications. The results of that need, according to 96% of respondents, is security and privacy becoming higher priorities for their organizations.

## F5 introduces post-quantum cryptography solutions to protect customers from emerging threats

**Kunal Anand,**
Chief Innovation Officer at F5

F5, the global leader in delivering and securing every app and API, is helping customers prepare for the foundational cybersecurity shift presented by quantum computing. New comprehensive post-quantum cryptography (PQC) readiness solutions are seamlessly integrated into the F5 Application Delivery and Security Platform, equipping organizations with the tools they need to secure applications and APIs while maintaining high performance and scalability.

The quantum era presents a significant cybersecurity inflection point, as the previous limits of classical computing will no longer apply. According to Gartner: "The motivation for IT departments to adopt post-quantum cryptography is grounded in the fact that advances in quantum computing will make asymmetric cryptography unsafe by 2029. By 2034, asymmetric cryptography will be fully breakable with quantum computing technologies."

Post-quantum cryptography marks a critical transformation in how sensitive data is secured. Unlike typical upgrades or patches, the transition to PQC represents a fundamental architectural shift in cybersecurity, requiring proactive planning and execution. A poorly managed transition can cause outages and disrupt operations, especially across hybrid, multicloud, and legacy systems. Without the right approach, organizations risk costly downtime, slower applications, compliance issues, and frustrated users.

# Most organizations miss business context when assessing cyber risk, finds new research from Qualys

According to new research commissioned by Qualys and conducted by Dark Reading, despite rising investments, evolving frameworks, and more vocal boardroom interest, most organizations remain immature in their risk management programs.

Nearly half of organizations (49%) surveyed for Qualys' 2025 State of Cyber-risk Assessment report, today have a formal business-focused cybersecurity risk management program. However, just 18% of organizations use integrated risk scenarios that focus on business-impacting processes, showing how investments manage the likelihood and impact of risk quantitatively, including risk transfer to insurance. This is a key deficiency, as business stakeholders expect the CISO to focus on business risk.

"The key takeaway from the research isn't just that cyber risk is rising. It's that current methods are not effectively reducing that risk by prioritizing the actions that would make the greatest impact to risk reduction, tailored to the business. Every business is unique; hence, each risk profile and risk management program should also look unique to the organization. Static assessments, siloed telemetry, and CVSS-based prioritization have reached their limit," commented Mayuresh Ektare, Vice President, Product Management, Enterprise TruRisk Management, Qualys.

**Mayuresh Ektare,**
Vice President, Product Management, Enterprise TruRisk Management, Qualys

"To address this, forward-leaning teams are adopting a Risk Operations Center (ROC) model: a technical framework that continuously correlates vulnerability data, asset context, and threat exposure under a single operational view. The ROC model provides a proven path forward for organizations ready to manage cyber risk the way the business understands it and expects it to be managed," Ektare continued.

# AWS WAF reduces web application security configuration steps and provides expert-level protection

AWS has announced general availability of the AWS WAF simplified console experience that reduces web application security configuration steps by up to 80% and provides expert-level protection to help optimize application security.

AWS WAF helps protect web applications and APIs against common web exploits and bots that could affect availability, compromise security, or consume excessive resources. Security teams can now implement comprehensive protection for applications within minutes through pre-configured protection packs that incorporate AWS security expertise and are continuously updated to address emerging threats. These templates provide extensive security coverage including protection against common web vulnerabilities, malicious bot traffic, application layer DDoS events, and API-specific threats, all customized to your application type.

With the new console experience, select the application type, such as E-commerce platforms or transaction processing applications, to automatically apply expert-curated protection rules optimized for the specific use case.

The unified dashboard provides consolidated security metrics, threat detection, and rule performance data, enabling security teams to quickly identify and respond to potential threats while maintaining full security control. Key security controls, including rate limiting, geographic restrictions, and IP reputation filtering, can be customized through an intuitive single-page interface that reduces configuration time.

# Okta and Palo Alto Networks unify AI-driven security to fight identity attacks

As attacks grow more sophisticated and demand real-time response, verifying who accesses data and from what device has become essential to protecting it. Okta and Palo Alto Networks announced an expanded partnership with new integrations to deliver a unified security architecture, enabling customers to automate threat response, secure application access on any device and reduce security roadblocks. The native integration between Okta Workforce Identity and Palo Alto Networks Prisma Access Browsercreates a new conditional access method to restrict access to SSO apps by using only the secure browser. A second integration between Identity Threat Protection with Okta AI and Palo Alto Networks AI-driven Cortex SecOps platform provides organizations with a unified view of identity-related risks across their entire attack surface. This integration extends to Cortex XSIAM and Cortex XDR, creating a comprehensive response to the most advanced attacks.

"AI is supercharging attacks on user credentials, requiring a 'fight AI with AI' approach that brings identity directly into an organization's security infrastructure for a real-time and unified response," said Stephen Lee, VP of Technology Partnerships at Okta."With Palo Alto Networks, Okta is proud to enhance the interoperability of our AI-powered platforms to prevent risks of siloed tools, providing nearly 2000 joint customers with a comprehensive view of their security posture, context-aware access controls, and secure authentication to stay ahead of today's threats."

# Outdated cybersecurity practices endanger industrial operations

**Azeem Aleem**
Global Executive Director, Cyber Resilience Services, CPX

CPX Holding, a leading provider of cutting-edge cyber and physical security solutions and services, released a new whitepaper titled "Securing Operational Technology with Trust and Collaboration."

The paper provides a comprehensive overview of the unique cybersecurity challenges facing Operational Technology (OT) environments and outlines practical recommendations for organizations seeking to modernize securely. As critical infrastructure sectors such as energy grids, transportation, manufacturing and water treatment plants become increasingly connected through cloud, IoT and AI, the study highlights that implementing traditional IT security frameworks is not only inadequate but can be risky when applied to OT. From the Triton malware targeting safety systems to the 3CX supply chain compromise and the recent Norwegian Dam breach that revealed hidden vulnerabilities, these incidents underscore that OT cybersecurity must be approached differently.

There is an urgent need for organizations to embed a 'cybersecurity by design' approach early in the Engineering, Procurement and Construction lifecycle rather than bolting on controls after systems are deployed to promote safer, more resilient industrial operations.

# New report from Mercury Security reveals top trends transforming access controller technology

Mercury Security, a leader in access control hardware and open platform solutions, has published its Trends in Access Controllers Report, based on a survey of hundreds of security professionals across North America and Europe. The findings highlight the controller's vital role in a physical access control system (PACS), where the device not only enforces access policies but also connects with readers to verify user credentials—ranging from ID badges to biometrics and mobile identities. With 72% of respondents identifying the controller as a critical or important factor in PACS design, the report underscores how the choice of controller platform has become a strategic decision for today's security leaders. While the report reflects global trends, its insights hold strong relevance for the Middle East and GCC regions. With Gulf countries accelerating investments in smart infrastructure, digital identity and cyber resilience, organizations across the UAE, Saudi Arabia, and the wider GCC are increasingly prioritizing access systems that are secure, scalable, and cloud-connected, particularly in key sectors such as finance, healthcare, education and government.


# ManageEngine enhances AD360 with risk exposure management and local user MFA features

ManageEngine, a division of Zoho Corporation and a leading provider of enterprise IT management solutions, announced the general availability of identity risk exposure management and local user MFA features in AD360, its converged identity and access management (IAM) platform. The release enables security teams to detect privilege escalation risks and secure unmanaged local accounts, two common identity attack vectors that attackers continue to exploit at scale. Identity remains the primary attack vector in modern enterprises, as shown by Verizon's 2025 Data Breach Investigations Report, which found that credential abuse was the initial access vector in 22 % of breaches. The report also highlighted widespread abuse of poorly managed local accounts and privilege paths across over 12,000 confirmed breaches.

**Manikandan Thangaraj**
Vice President of ManageEngine

"With this release, ManageEngine AD360 moves beyond traditional IAM by embedding identity threat defenses into core identity operations. By turning identity data into actionable security insights, we're helping customers make IAM the first line of defense, not a check box," said Manikandan Thangaraj, vice president of ManageEngine.

While most IAM tools focus on provisioning and policy enforcement, AD360 adds risk exposure mapping via attack path analysis as well as local MFA enforcement, helping enterprises close attack paths that often go undetected. This marks a key step in identity management evolving from an access control layer into an active security control.

# **Zero trust,** zero excuses

ThreatLocker CEO Danny Jenkins on why endpoint security has never been easier.

**Everyone's talking about Zero Trust now—it's a buzzword. But implementing it, especially on endpoints, isn't always easy.**

Actually, when it comes to endpoints, it's incredibly easy—at least in 99% of cases. The idea behind Zero Trust is very simple. It's not about a single product, though products can help support it. The principle is this: access is only granted to what's needed.

And it's not just about users. For example, Bob only needs access to financial files—so he only gets access to those. Sally only needs access to sales—so that's all she can see. Microsoft Office only needs access to documents—so it only gets that access. It can't touch PowerShell.

When we apply this to endpoints, we ask: What software is allowed to run? Is everything blocked by default? Can one piece of software communicate with another? Can it access your files?

That's the philosophy—only what is needed should be allowed.

We've done 20,000 endpoint implementations with just 30 hours of manpower. That's possible because of learning algorithms, AI advancements, and the intelligence we've built into the system. All of that has made it incredibly easy to implement Zero Trust at the endpoint level.


**Danny Jenkins**
CEO
ThreatLocker

**So, you're leveraging AI and ML in your portfolio.**

Yes, we use both machine learning and AI quite extensively. In fact, we've developed our own models that are continuously learning and evolving.

The challenge with implementing Zero Trust is that you need to understand how software is supposed to behave. That's where our models come in. With millions of endpoints deployed worldwide, we're able to observe and learn typical behavior patterns—for example, how Office behaves, how Chrome behaves, how Adobe behaves.

We identify what each application needs to do—and nothing more. That insight is what makes our Zero Trust approach so effective.

**Is your platform automated?**

Yes, absolutely. Once deployed, the platform automates most of the process. It identifies all the applications in the environment. While there is a small manual component and the customer may need to do a bit of manual work, around 99.9% of the deployment is fully automated. That's also thanks to the fact that we have a team continuously feeding data into the system to keep it optimized.

Our goal is to continue expanding these partnerships and build strong educational collaborations across the region.

**Do you also play in the EDR space?**

We have full EDR capabilities. Zero Trust is at the core of what we do,

and EDR is a critical part of the overall strategy. But EDR should always be the backup, not the first line of defense.

Think of EDR like a house alarm. You wouldn't rely solely on the alarm and leave your doors unlocked. You lock your doors first—that's your proactive protection—and then you set the alarm as your second layer of defense.

### Are you seeing a lot of AI-driven exploits?

Yes, a huge amount. We're observing two key trends: First, there's a significant rise in phishing attacks—highly convincing and intelligently crafted. Second, we're seeing the creation of new, previously unseen malware that's bypassing traditional defenses.

### What are your views on AI in cybersecurity?

AI is a double-edged sword. Attackers use it, and so do defenders. But when it comes to intent detection, AI falls short. For example, backup software and malware might both move data to the cloud—but AI can't tell whether it's malicious or not. That's why AI is more effective at behavioral profiling—understanding what's normal vs. abnormal—rather than trying to guess intent.

### Do you also cover cloud-native and endpoint security?

Yes, we do. For instance, we now support Microsoft 365. We're building consolidated log views that help detect anomalies—say, if someone logs into Microsoft 365 in Dubai but accesses GitHub from Florida minutes later, we flag that as suspicious behavior.

### What are you bringing to the table? What would you say differentiates your solution?

I'd say our biggest differentiator is the control we give organizations over what runs in their environment. We're ring-fencing applications, limiting what they can do, and applying strict rules with binary decisions around data access.

This means you're no longer guessing whether the latest threat will be detected. Instead, the approach is: if it's not explicitly allowed, it simply doesn't run. That's real security.

### Can your solution be easily integrated into existing security stacks?

Yes, absolutely. In fact, we frequently integrate with SIEMs. While we offer our own EDR, XDR, and MDR capabilities, I'd say about half of our customers use our Zero Trust platform alongside another EDR solution.

### Do you think SIEM is still necessary?

If you need to keep logs, then yes—of course, SIEM is still important. I believe SIEM has two main purposes. First, it's a central log aggregator, giving you visibility into everything that's happening in your environment in the event of an incident. Second, it's critical for compliance.

It's also meant to help with threat identification by running rule sets on the data. That said, I think it was over-prioritized in many organizations. You still have people investing in SIEM while allowing untrusted software to run freely—which, frankly, is a bit backward. You'd think Zero Trust would be the first step.

### What does the current threat landscape look like? Are there any new trends, or is it still the usual suspects—ransomware, phishing, and malware?

We're definitely seeing a lot of new ransomware gangs emerge. There's more data exfiltration, and we're also seeing an uptick in AI-driven malware. So while it's not necessarily a radically new threat landscape, it's certainly evolving—with more actors, more malware variants, and greater use of AI to drive attacks.

### Do you provide threat intelligence or insights to your customers?

Yes, we do. While we don't provide a direct list of threats, we cross-reference customer data against threat intelligence sources to identify suspicious activity. That correlation helps customers understand their exposure without overwhelming them with generic threat feeds.

### What opportunities do you see in this market? Are you targeting any specific verticals?

This is the fourth market we've entered, and it's growing faster than any of the previous ones. A big part of that is our maturity—we're now used by over 54,000 businesses worldwide, including some of the world's largest airports, banks, and financial institutions. That level of trust certainly helps.

But I also think companies in this region are becoming more aware of how heavily targeted they are. Given the geopolitical tensions and rising cyber activity, there's growing urgency to close existing security gaps.

### What's your key message to CISOs in this region?

Focus on removing unnecessary permissions. Whether through application whitelisting, ring-fencing, or revoking excessive user privileges—this is where you'll have the most impact. Prevention through access control is far more effective than detection after the fact.

# BEHIND THE CODE

## Making emerging technologies compliant by design

The accelerated adoption of emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) is opening new frontiers for businesses across industries. From intelligent automation to real-time analytics, the opportunities are transformative. However, this wave of innovation also ushers in significant compliance challenges, placing mounting pressure on enterprises to manage risk, meet evolving regulations, and safeguard trust.

One of the most pressing concerns is the sheer volume, variety, and velocity of data generated by AI and IoT systems—often in real time and from diverse, distributed endpoints. Managing, protecting, and governing this data to align with regulatory mandates is becoming increasingly complex.

### Data privacy at the core of AI and IoT deployments

"AI systems frequently rely on large datasets, which may include sensitive or personally identifiable information," explains Islam Afifi, Regional Director, Technical Sales Middle East & CIS at Veeam. "Ensuring

proper data privacy, data retention, and auditability is critical—not only to comply with regulations like GDPR or CCPA but also to maintain trust with customers and stakeholders."

In the case of IoT, compliance complexity increases further. IoT-generated data often originates outside traditional IT environments and across jurisdictions with differing legal and regulatory frameworks. "This makes data residency and sovereignty an ongoing challenge," Afifi adds.

The constantly shifting landscape of global and regional regulations adds another layer of difficulty. As governments respond to new threats and technological advancements, organizations must stay agile and ready to pivot. Updating access controls, modifying data storage policies, and implementing new reporting tools all become essential capabilities.

"For emerging technology domains, cybersecurity regulations are rapidly evolving," notes Kylie Watson, Head of Cybersecurity and Field CISO – APJ MEA, DXC Technology. "Companies must regularly consult local legislation to ensure

**Ivan Milenkovic,**
Vice President – Cyber Risk Technology, EMEA at Qualys

**Meriam ElOuazzani,**
Senior Regional Director, Middle East, Turkey, and Africa at SentinelOne

**Sascha Giese,**
Global Technical Evangelist, SolarWinds

compliance, particularly in areas relating to privacy, safety, or critical infrastructure."

Gulf nations like Saudi Arabia and the UAE have introduced robust regulatory frameworks aligned with international standards such as ISO 27001 and the NIST Cybersecurity Framework. Where local laws are silent or underdeveloped, these globally recognised standards offer a structured and reliable approach to managing cybersecurity risk and ensuring regulatory alignment.

## The technical side of compliance

From a technical standpoint, AI adoption introduces additional complexities. Data privacy becomes especially difficult to manage when AI models rely on large volumes of data from distributed endpoints—such as wearables, sensors, and location trackers. These sources often carry sensitive personal, health, or behavioural information.

Organizations must therefore ensure that AI systems ingest data only from approved and governed sources. "This becomes particularly important given the sprawl of APIs and the diversity of data flows across numerous third-party suppliers," says Afifi. To address these challenges, enterprises must establish strong governance mechanisms, enforce data anonymization protocols, and implement proof-of-provenance systems to ensure traceability and audit readiness.

## Data sovereignty in a hyperconnected world

"As AI and IoT technologies become increasingly intertwined in modern digital infrastructure, data privacy and sovereignty emerge as top concerns," warns Meriam ElOuazzani, Senior Regional Director, META, SentinelOne. "IoT devices continuously collect sensitive personal and operational data, while AI systems analyze and infer patterns from this data—sometimes uncovering insights that users have not explicitly consented to share."

In regions such as the GCC, new regulations like the UAE's Personal Data Protection Law (PDPL) and Saudi Arabia's Personal Data Protection Law are placing stricter obligations on data localization, lawful processing, and cross-border governance. These developments require organizations to be more intentional in designing and maintaining their data architecture.

## Responsible AI and the black box problem

AI's impact on compliance goes beyond data handling. Another critical challenge is model explainability. Many AI algorithms—especially those used in sensitive domains such as healthcare, surveillance, and finance—operate as "black boxes," making it difficult for organizations to justify their outputs.

With laws like the EU AI Act and growing momentum around responsible AI, businesses must be prepared to demonstrate how their AI systems arrive at decisions. "The challenge becomes even greater when models are retrained or updated dynamically, raising issues with version control, auditability, and legal accountability," ElOuazzani says.

According to Morey Haber, Chief Security Advisor at BeyondTrust, a core issue lies in the rapid pace of AI development. "The biggest compliance challenges around technologies like AI stem from their fast evolution and the lack of technical understanding among enterprise users," he says. "In contrast, IoT and OT, which have been around longer, have benefited from clearer regulatory frameworks and a more mature ecosystem of security controls."

## Innovation and compliance: A strategic balancing act

So how can enterprises pursue innovation

**Morey Haber**
Chief Security Advisor
- BeyondTrust

**Kylie Watson,**
Head of Cybersecurity and Field CISO –
APJ MEA at DXC Technology

**Sreedharan Srinivasan,**
Director of Compliance at ManageEngine

while remaining compliant?

"It requires a compliance-by-design approach," says Sreedharan Srinivasan, Director of Compliance at ManageEngine. "Regulatory considerations must be embedded at every stage of the product life cycle—from design and development to deployment and scaling."

This includes conducting data protection impact assessments (DPIAs), using privacy-enhancing technologies, and deploying comprehensive data governance frameworks. Cross-functional collaboration between legal, engineering, product, and compliance teams is essential to ensure innovation aligns with regulatory requirements.

Transparency, Srinivasan adds, is vital. Enterprises must provide clear disclosures on data use and implement consent mechanisms to build user trust. Best practices like encryption, Zero Trust architecture, and regular security audits further help mitigate risk while supporting continuous innovation.

## Testing and regulatory sandboxes

In the UAE, organizations can explore sandboxes and pilot environments to test emerging technologies in controlled settings. "Regulatory sandboxes—especially those available in the UAE's financial sector—allow AI and IoT solutions to be trialled under monitored conditions," says Ivan Milenkovic, Vice President – Cyber Risk Technology, EMEA at Qualys.

These pilots, often run with synthetic data or a limited user base, enable compliance teams to assess risks, identify biases, and refine controls before a broader rollout. For instance, a bank using AI for customer profiling might launch it initially within a sandbox to fine-tune the model and document its compliance posture.

Early engagement with regulators is also encouraged. "Regulatory bodies such as the UAE Data Office welcome proactive collaboration," Milenkovic says. "This helps organizations align their innovations with current frameworks and receive informal guidance that can smooth the path to full compliance."

## Global compliance at scale

For multinational companies, maintaining compliance across jurisdictions is particularly challenging. "Organizations need to work closely with their legal departments and, when necessary, consult external legal counsel in other regions," advises Sascha Giese, Global Tech Evangelist for Observability at SolarWinds. "Global policies rarely work without local adaptation—what's acceptable in one geography might be problematic in another."

As compliance requirements evolve, supply chain and vendor accountability is becoming more significant. "With the emphasis on supply chain security and third-party risk, vendors are now subject to the same regulatory scrutiny as the enterprises they serve," adds Srinivasan.

A robust Governance, Risk, and Compliance (GRC) framework becomes essential for tracking regulations, aligning with partner obligations, and remaining agile. Businesses that build a strong foundational compliance program can then tailor it to meet specific regional or industry requirements.

In a landscape defined by rapid technological change, compliance is no longer just a legal necessity—it is a strategic differentiator. Enterprises that embed governance into their innovation cycle, invest in transparency, and remain proactive in their engagement with regulators will be better positioned to lead in the AI- and IoT-driven digital economy.

# **Shaping the next** generation of talent

Positive Technologies organizes the Positive Hack Camp annually—an international cybersecurity education program for students and aspiring young professionals. Yuliya Danchina, Customer and Partner Training Director and Head of Positive Education at Positive Technologies, shares how the company is tackling the global cybersecurity skills shortage.

**? Can you tell us about the key focus areas of your cybersecurity education programs?**

We operate as the cybersecurity education division within Positive Technologies. Our primary focus is delivering education programs—both for professionals already working in the field and for those who are just getting started. That's our first stream.

We offer training programs across various tiers for cybersecurity and IT specialists. For example, in ethical hacking (white-hat hacking), we teach participants how to identify and address vulnerabilities, how to secure infrastructure, and how to build secure IT environments within companies. The range of topics we cover is broad, and the skills we impart are practical and industry-relevant.

The second part of our work involves collaborating with institutions—universities, schools, and even individual educators. Our logic is simple: to build a strong cybersecurity ecosystem, we must engage the full talent pipeline—from early education to advanced technical training.

We run programs for schools that train teachers to introduce students to ethical hacking. Children as young as 10 years old are already capable of understanding how hackers think, and they can grasp basic concepts and techniques. We also work with high schools, where our involvement includes curriculum support, workshops, and collaborative projects.

At the university level, we've partnered with around 600 universities across Russia, though our primary focus is on top-ranked STEM universities—especially those specializing in cybersecurity and IT. We work directly with faculty members to co-develop programs, share training content, and provide guidance on current industry needs.

For example, with IT universities, we've helped integrate credit-bearing courses into their curricula across a few key disciplines.

One of the main areas is white-hat hacking, because we strongly believe that anyone studying IT or cybersecurity needs to understand how hackers think. Another subject we've helped implement is secure development by design—a methodology-based course that has now been added as a credit in several Russian universities, based on our recommendations.

That's one part of the story. The second part is that many universities

**Yuliya Danchina**
Customer and Partner Training Director and Head of Positive Education at Positive Technologies

lack access to modern, practical tools.

We all understand the industry is moving much faster than academia. So, universities often turn to us for technological tools and training environments.

**What does that mean in practice?**

We provide advanced cyber ranges and labs—tools and exercises designed to support hands-on learning. We believe that practical, real-world training is essential in cybersecurity education, so we make these tools available to students and educators.

The third part of our involvement is training university faculty. For the past three years, we've been running a professional development project designed to train professors who teach IT and cybersecurity at Russian universities. The result of this program is a complete transformation of current educational curricula. Over the course of six months, participants—university faculty—go through intensive training, and the outcome is that they significantly revise and modernize their teaching programs.

During the program, we focus on several key areas. First, we teach them what's currently happening in the cybersecurity landscape—not only in Russia but globally. Our experts and white-hat hackers have access to a vast amount of real-time data about how cyberattacks are carried out today. That's exactly what we share: how hackers operate and how to defend against those attacks effectively, using real-world tactics and high-level security strategies.

In addition to our work with academia, we also offer education programs for working professionals in IT and cybersecurity. We regularly engage with international audiences through events like Hack Talks—localized meetups where cybersecurity professionals and white-hat hackers come together to share insights, trends, and challenges they face in the field.

Last year, we launched a truly exciting and innovative educational program called Positive Hack Camp—a program designed specifically for beginners and young talent who are just starting their journey in IT. This year, the second edition of the camp will take place in August here in Moscow.

The response last year was incredible. We received a number of applications from students and professionals in the Gulf region, including Saudi Arabia, Bahrain, UAE, Egypt, and across the Middle East. In total, we had 70 participants from 20 countries attend the camp.

It was a two-week, intensive, on-site program focused on hands-on training and real-world cybersecurity scenarios. The camp is held physically, not online, giving participants a chance to engage directly with instructors, peers, and our cybersecurity experts

**Are you working with any universities outside of Russia?**

Last year, we've signed a partnership with the Amity University in Dubai, and we also began a partnership with SGU University in Indonesia. That marked the beginning of our academic engagement in the region.

Currently, we're in active discussions with several other universities, particularly in Saudi Arabia. We're also in talks with the Cybersecurity Federation of Programming and Drones. Representatives from the Federation have expressed interest in working with us and have recommended that we explore partnerships with universities and colleges in the Kingdom.

Our goal is to continue expanding these partnerships and build strong educational collaborations across the region.

# **Rethinking business continuity in** a hyperconnected world

Shazali Taha, Regional Director – META at AppyThings, shares why securing APIs is essential for business resilience in an increasingly hyperconnected world.

In May 2024, a global PC and technology provider disclosed a breach affecting 49 million customers, with the attacker exploiting weaknesses in its partner account portal. This high-profile case is one of many reminders that no organisation is immune in today's hyper-connected world. The projected global cost of cybercrime is expected to hit $13.28 trillion by 2028, underscoring the urgency to act. Cyber resilience has emerged as a critical business priority. Unlike traditional cybersecurity, which focuses on preventing breaches, cyber resilience assumes incidents are inevitable. It's about preparing for, responding to, and recovering from attacks while ensuring business continuity. In this way, resilience becomes more than a protective measure—it becomes a strategic enabler of agility, trust, and long-term growth. Unlike traditional cybersecurity, which focuses on preventing breaches, cyber resilience assumes incidents are inevitable. It's about preparing for, responding to, and recovering from attacks while ensuring business continuity. In this way, resilience becomes more than a protective measure—it becomes a strategic enabler of agility, trust, and long-term growth.

## Evolving Threat Landscape in the META Region

Across the Middle East, organisations face escalating threats. The average cost of a breach in the region has climbed to $8.75 million, nearly double the global average. The most common method of attack was the use of malicious software. The rise of hybrid cloud, remote work, and rapid API adoption has expanded the attack surface, often faster than security teams can respond.

Compounding the issue are insider threats—23% detected in organizations in a GCC country stem from internal actors, whether intentional or accidental.

This evolving landscape calls for a resilience-first approach, integrating proactive protection, real-time monitoring, and fast recovery strategies. Globally, top cyberattacks now include ransomware, distributed denial-of-service (DDoS) attacks, quantum technology threats, breaches in healthcare systems, misuse of AI and AI agents, and even cybersecurity risks related to space infrastructure, each raising the stakes for results-driven cyber resilience planning.

Why APIs are Ground Zero

APIs, or Application Programming Interfaces, are the digital glue holding modern ecosystems together. APIs act as messengers that allow different software systems to talk to each other. For example, when you use a ride-hailing app, APIs help connect the app to maps, payment gateways, and messaging services seamlessly. They enable businesses

**Shazali Taha**
Regional Director - META, AppyThings

to integrate services, connect applications, and unlock new revenue streams with greater speed and flexibility. In fact, a recent industry report highlights that 83% of IT professionals see API integration as mission-critical for achieving their business objectives. However, because APIs connect so many essential services, they also become high-value targets for cyber attackers looking to exploit vulnerabilities and disrupt operations.

With rapid digital expansion, APIs are now created faster than they're secured. This sprawl leads to shadow and zombie APIs, often outdated, undocumented, or forgotten, that widen the threat landscape.

Many suffer from poor access controls,

lack of visibility, or insufficient rate limits—issues that attackers eagerly exploit to gain unauthorised access, exfiltrate data, or launch denial-of-service (DoS) attacks.

The advent of IoT and AI-driven tools give attackers more sophisticated ways to detect and exploit API weaknesses. The consequences can be severe: exposure of Personally Identifiable Information, financial loss, legal repercussions, and long-lasting reputational damage. Yet, many organisations still underestimate API risk, struggling with the cost, complexity, and awareness of API security.

## Building Blocks of Cyber Resilience

A recent report shows that 98% of security professionals believe the resilience gap is widening, exposing critical sectors and SMEs to greater risk. To achieve true cyber resilience, organisations must focus on three interdependent layers: API security testing and audits: Conducting regular testing can identify vulnerabilities in API endpoints and code. Responses can protect the entire API lifecycle. Regular audits enable IT teams to assess the overall security of an API, including reviewing configurations, access controls, and compliance with security policies and standards.

Real-time traffic monitoring: By continuously monitoring API traffic, IT teams can identify unusual patterns that could indicate an attempted attack on an API vulnerability.

Event Streaming Platforms offer real-time anomaly detection and alerting, enabling swift incident response and data recovery. These platforms are essential for detecting lateral movement within networks and suspicious activity patterns.

API Security includes strong authentication, encryption, input validation, and rate limiting. Tools like OAuth (Open Authorization), JWT (JSON Web Token), and TLS (Transport Layer Security) protect data in transit, while throttling controls resource consumption to maintain service availability during high-load or attack scenarios.

Importantly, the focus is shifting from protection to resilience—ensuring continuous uptime, rapid recovery, and adaptability in the face of dynamic threats.

## Business Continuity Through Integration-Driven Resilience

Integration is not just a technical need—it's a resilience strategy. Secure cloud integration ensures system failover, load balancing, and uninterrupted workflows during cyber events.

When integrated with event-driven architecture, it allows organisations to automatically detect problems and take corrective actions immediately. This setup also enables systems to adjust their capacity on the fly, helping avoid crashes or slowdowns during peak usage.

For example, a global financial services provider avoided major downtime during a DDoS attempt by redirecting API traffic in real time, thanks to built-in failover protocols and automated throttling measures. These capabilities were rooted in smart integration strategies implemented early in their transformation journey.

By embedding resilience into software development lifecycles—through secure coding, DevOps-integrated security testing, and automated patch management—organisations reduce panic fixes later and increase confidence in every code push.

## Developing a Cyberattack Conscious Culture

Organisations that treat it purely as an IT concern are missing the bigger picture. True resilience requires shared responsibility, continuous learning, and the willingness to adapt at speed.

Resilience starts at the top. It's not just about investing in the right tools, but about cultivating a mindset that spans teams and departments. Business leaders must champion cross-functional collaboration between IT, risk, and operations teams to embed cyber resilience across the business.

> "With rapid digital expansion, APIs are now created faster than they're secured.

Training, simulation exercises, and board-level reporting on resilience metrics are all essential. Culture—not just technology—is the foundation for sustainable security.

## Looking Ahead in the Age of AI and Hyperconnectivity

As the digital fabric tightens with AI, IoT, and 5G, the complexity of protecting critical assets grows exponentially. But so do the opportunities to get ahead. AI and predictive analytics are now being used to detect anomalies, prioritise response, and automate recovery faster than ever before.

In a region where digital adoption across industries has reached approximately 75% to 80% (McKinsey & Co), emerging paradigms like zero-trust architecture, decentralised APIS, and quantum-safe encryption are setting the stage for next-gen resilience. At the same time, hyperconnectivity brings jurisdictional challenges—data often must be hosted within national borders, particularly in countries like the UAE and Saudi Arabia. Many governments operate closed or restricted networks, meaning that connecting to services like financial apps requires navigating approved infrastructure already accessed by other government entities. Forward-thinking regulators like the Dubai Electronic Security Center (DESC) are advancing cyber resilience at a citywide level through risk assessments, cross-sector coordination, and comprehensive recovery planning. To thrive in this future, organisations must adopt a continuous improvement mindset, which includes frequent testing, risk reviews, and adapting to new threats without delay.

## From Reactive to Resilient

The future belongs to organisations that can operate confidently in an unpredictable environment. Cyber resilience isn't just a defensive posture—it's a business enabler that turns uncertainty into advantage.

To start the journey, assess the current resilience posture. Consider partnerships with integration specialists who understand the full API lifecycle and can help embed resilience at every layer. In an age where cyberattacks are inevitable, it's not the breach that defines the company, but how quickly, securely, and intelligently you bounce back.

# **From positivity** to pitfalls

Ashley Woodbridge, CTO, Lenovo, META, on navigating impacts of Gen AI on cybersecurity

Generative AI (Gen AI) is transforming industries across the globe, at an unprecedented speed, and cybersecurity is stranger to the new age digital evolution. This powerful technology, capable of creating new content from text and images to code, however, presents both unprecedented opportunities and significant challenges for protecting digital assets.

While Gen AI has already been shown to enhance threat detection, automate security tasks, and improve incident response, it concurrently empowers cybercriminals with sophisticated tools for crafting more convincing phishing campaigns, developing evasive malware, and launching large-scale attacks.

Understanding this dichotomy is key for organisations to navigate the evolving cybersecurity landscape effectively.

## The Promise of Gen AI in Cybersecurity: A Shield Against the Dark Arts

Gen AI no doubt offers a range of capabilities that can significantly bolster cybersecurity defences; one of the most promising areas of which is enhanced threat detection. Its algorithms can analyse vast amounts of data from various sources, including network traffic, system logs, and threat intelligence feeds, to identify patterns and anomalies that indicate malicious activity. And unlike traditional rule-based systems, Gen AI learns from new data and adapts to evolving threats, enabling it to detect sophisticated attacks that might otherwise go unnoticed.

Lenovo Cybersecurity Services, for instance, leverages advanced machine learning models to analyse network behaviour and identify suspicious patterns indicative of insider threats or advanced persistent threats (APTs). Crucially, these models are continuously trained on real-world data to improve their accuracy and reduce false positives.

Beyond threat detection, though, Gen AI excels at automating many routine cybersecurity tasks – vulnerability scanning, patch management, and security configuration – freeing up security professionals to focus on more complex and strategic initiatives, improving overall efficiency and reducing the risk of human error.

According to forecasts by Statista, the global cost of cybercrime is projected to reach $15.63 trillion annually by 2029, but automating security tasks with Gen AI can help organisations mitigate these costs by reducing the time and resources required to maintain a strong security posture. Likewise, Gen AI contributes significantly to an improved, accelerated incident response by automating the analysis of security alerts, identifying the root cause of incidents, and recommending remediation steps. In simple terms, this enables security teams to respond to threats more quickly and effectively, minimising the impact of attacks.

**Ashley Woodbridge**
CTO, Lenovo, META

Prevention, of course, is better than cure, and that's another area where Gen AI shines: proactive vulnerability discovery. By analysing code and simulating attack scenarios, the intuitive technology can uncover hidden flaws and weaknesses in software and systems that might be missed by traditional security testing methods, before they can be exploited by attackers.

To this end, researchers at Google have developed a Gen AI model called AlphaCode that can generate code that is competitive with human programmers, and which could be used to automate the process of vulnerability discovery by generating code that tests the security of software systems.

Still, human error persists, with 60% of data breaches involve a human element,

according to Verizon's 2025 Data Breach Investigations report. Personalised security awareness training powered by Gen AI, though, can help organisations address this issue by educating employees about common attack vectors and best practices for staying safe online. By delivering targeted training content that is relevant to their daily tasks, companies can improve employee awareness of cybersecurity risks and reduce the likelihood of human error even further.

## The Dark Side of Gen AI: A Double-Edged Sword

While Gen AI offers significant benefits for cybersecurity, it also presents new challenges and risks, where cybercriminals are increasingly leveraging the technology to develop more sophisticated and effective attacks.

One of the most concerning threats is enhanced phishing attacks – Gen AI-generated highly realistic and personalised phishing emails that are difficult to distinguish from legitimate communications – used to trick employees into revealing sensitive information or influencing clicks on malicious links. In a recent experiment by SoSafe, data revealed that AI-written phishing emails were opened by 78% of humans, with 21% of those clicking on malicious content within. Alarmingly, 65% of humans were tricked into revealing personal information in input fields on the linked websites by AI-generated emails.

At its most basic, the results demonstrate that humans cannot distinguish AI-generated phishing emails from manually captured phishing attacks, highlighting further the potential for Gen AI to significantly increase the effectiveness of phishing attacks.

Another considerable threat is evasive malware development, with Gen AI employed to develop insidious programs that traditional antivirus software find more difficult to discover and defeat. By generating polymorphic code and using advanced obfuscation techniques, cyber attackers via Gen AI create malware capable of bypassing endpoint detection and response (EDR) systems, evading detection and remaining hidden on infected systems.

Automated social engineering is an additional growing concern. With deep fakes redefining likeness and identity, Gen AI can realistically be used to create social media profiles that are difficult to distinguish from real profiles, engaging in conversations with potential victims, which in turn could be used to launch large-scale social engineering campaigns targeting specific individuals or organisations. This grants attackers access to path that builds trust and rapport with targets, making victims even more susceptible to scams and phishing attacks.

Deeper still, on a larger scale, Gen AI could be used to create smear campaigns – generate fake news articles, videos, and audio recordings – that are designed to spread disinformation and manipulate public opinion, damage reputations, manipulate elections, and sow discord. And its sinister influence has no ceiling. Consider the 2020 US presidential election, where Gen AI was used to great effect in creating deepfake videos of political candidates intended to mislead voters and undermine democratic processes.

Worryingly, cyber attackers can even poison the training data used to develop Gen AI models, causing them to make incorrect predictions or generate malicious content, compromising further the integrity of AI-powered security systems making them less effective at detecting threats. Researchers, too, have demonstrated that AI model poisoning attacks can be used to compromise the accuracy of facial recognition systems, which prompts serious implications for security applications that rely on facial recognition, such as access control and surveillance.

> “Alarmingly, 65% of humans were tricked into revealing personal information in input fields on the linked websites by AI-generated emails.

## Navigating the Gen AI Cybersecurity Landscape: A Strategic Approach

Fortunately, we're not helpless. But to effectively navigate the evolving Gen AI cybersecurity landscape, organisations need to adopt a strategic approach that addresses both the opportunities and the challenges.

The first step is to invest in AI-powered security solutions that can leverage the benefits of Gen AI to enhance threat detection, automate security tasks, and improve incident response. Lenovo Cybersecurity Services, for example, offers a comprehensive suite of AI-powered security solutions that can help entities protect their digital assets from evolving threats.

It's also vital a Gen AI security strategy that addresses the risks posed by this technology is developed; including policies and procedures for the responsible use of Gen AI, as well as measures to protect against AI-powered attacks. Training, too, plays its part, where employees are made inherently aware of the security risks associated with Gen AI, with an emphasis on the importance of critical thinking and scepticism when encountering online content. Gen AI is always learning, and so should we be.

Continuous monitoring of AI model performance, including regular testing and validation of model outputs, will remain essential to detecting signs of model poisoning or other attacks, with various organisations sharing threat intelligence with each other to stay ahead of the evolving Gen AI risk landscape; collaboration, in essence, that helps identify new attack vectors and develop effective countermeasures.

As the Middle East continues to embrace AI-driven innovation, it is imperative for organisations to prioritise cybersecurity and adopt a strategic approach to managing the risks and challenges posed by Gen AI. By investing in AI-powered security solutions, developing a comprehensive Gen AI security strategy, and training employees on the latest threats, the region's organisations can unlock the full potential of Gen AI while protecting their digital assets.

# **The new** bot war

Everyone you know might be fake, warns Lori MacVittie, F5 Distinguished Engineer

Bot farms used to be a joke. A few thousand spam accounts, broken English, crude engagement tactics. Easy to spot. Easy to dismiss.
Not anymore.

Today, bot farms operate at industrial scale, deploying thousands of real smartphones to run scripted accounts that behave like real users. They like, share, and comment just enough to trigger platform engagement algorithms.
It's not hacking. It's using the system exactly as designed, only faster, at scale, and without the authenticity those systems were meant to assume.

Once a post gets traction, platforms like X and Meta boost it further. They amplify engagement, not accuracy. X's 2023 transparency report makes it clear: what moves gets promoted. Even with ML-based detection systems in place, AI-driven bots blend seamlessly into organic traffic.

From there, real users take over. Visibility creates perceived legitimacy. If something looks popular, it feels trustworthy.
Fake engagement creates the illusion. Real people build the fire. And AI makes that fire harder than ever to trace.

## The impact of AI

Where bot farms once needed armies of workers pushing repetitive posts, AI tools can now generate coherent, varied, and highly believable content.

According to NewsGuard's 2023 report, AI-generated propaganda is increasingly indistinguishable from authentic commentary, even down to regionally specific language and emotion.

This isn't junk content anymore. It's plausible, contextual, and reactive. It looks like grassroots support, but it's manufactured influence at industrial scale.

And the platforms still reward it. They were built to amplify what performs, not to assess what's real. Moderation tools and human reviewers are not keeping up

Meta's 2024 report on taking action against coordinated, inauthentic behavior emphasizes just how difficult it has become to detect these coordinated campaigns in real time.

This isn't a fringe issue. It includes politics, marketing, financial speculation, even brand trust. In 2021, the U.S. Securities and Exchange Commission warned of social-media-driven market pumps fuelled by bots.

Meanwhile, systems that rely on visibility and engagement (trending lists, "suggested for you" panels) are now easily hijacked.

The tools designed to surface what matters now surface whatever someone pays to make matter.
Today's bots don't break rules. They follow them. They mimic human behaviour and generate conversation. They build credibility over time and operate across networks. Because they

**Lori MacVittie**
F5 Distinguished Engineer

don't violate technical policy, they often go undetected.

This exposes a deeper flaw: systems were designed to evaluate behaviour, not motivation. We trusted patterns. If it looked normal, it was assumed to be safe.

But AI doesn't behave abnormally. It behaves convincingly.

## AI shifts signals up the stack

The signal has shifted up the stack. Away from headers and rates. Into payloads, content semantics, and system-level coordination. AI-generated influence looks clean to traditional defences. The anomaly is no longer in the envelope. It's in the message.

Efforts to address the problem are underway. DARPA's Semantic Forensics program is working to detect AI-generated content using intent and linguistic markers. X's 2024 updates mention enhanced bot removal efforts. But these systems are still early-stage. The tools are not yet scalable or responsive enough to outpace AI-driven influence campaigns. And now the threat is evolving again.

> "Beyond simple bots, AI-driven agents are being deployed. These agents do more than automate.

Beyond simple bots, AI-driven agents are being deployed. These agents do more than automate. They coordinate. They pivot. They analyse response data and adjust tactics in real time. A 2022 DFRLab study documented how state-backed campaigns used AI agents to orchestrate disinformation across platforms, adapting dynamically to detection.

Meanwhile, legitimate businesses are adopting agents for customer support, marketing, and workflow automation. Lyzr.ai says 70% of AI adoption efforts focus on action-based AI agents, not just conversational bots.

This blurs the lines. When agents speak for both companies and attackers, trust erodes. A fake support bot posing as a brand representative could phish users or spread misinformation, indistinguishable from the real thing unless you know what to look for.

This is no longer a bot problem. It's an authenticity crisis.

## AI evolution challenges assumptions

The new bot war, powered by advanced AI tools and coordinated agents, has redrawn the map. We are not defending against noise. We are defending against synthetic credibility that is crafted to look human, scaled to manipulate systems, and optimised to pass undetected.

The underlying assumptions we've built around security and scale are breaking down in the face of this shift away from infrastructure and into the exploitation of algorithms, semantics, and perceived legitimacy.

Solving it means rethinking the foundation. Tools built to enforce rules must evolve to interpret behaviour, language, and coordinated patterns as part of a broader system of intent.

Until then, scepticism is our baseline and restoring trust will require more than detection.

It will take active collaboration between platforms, enterprises, and researchers to rebuild integrity into the systems we rely on every day and ensure their tactics don't seep into the enterprise where synthetic influence could quietly corrupt decision-making, hijack automation, and erode user trust from the inside out.

# **The real threat in** modern workflows

The next frontier of cybersecurity is an app that is most utilized and often the most overlooked, says Nikola Kukoljac, VP – Solutions Architecture, Help AG.

When scale adoption of digital and business transformation by global and regional enterprises and the associated cybersecurity vulnerabilities, has driven the realization of the importance of keeping cybersecurity at the same levels as other strategic priorities of the enterprise. asked which application is used most within an organization, most people instinctively point to Outlook, Teams, Word, or Excel. But they're wrong. The most utilized, and often the most overlooked, application is the browser.

Hiding in plain sight, the browser is a pressing concern for cybersecurity.

The browser has quietly become the primary access point to enterprise applications, cloud services, emails, and sensitive data. Yet despite its ubiquity, it was never designed with enterprise-grade security in mind.

Historically, we've tried to secure the browser indirectly, wrapping it in layers of defenses: proxies, DLP tools, sandboxes, endpoint monitoring and more. These were all an attempt to control an application that sits at the heart of modern workflows, yet outside the traditional security perimeter.

Compounding the challenge is the rise of unmanaged devices. According to the State of the Market Report 2025 by Help AG, over 50% of devices accessing corporate apps via browsers are not managed by IT. These are personal laptops, mobile phones, or remote systems that operate beyond the control of corporate policy.

Worryingly, more than 90% of malware infections originate from these unmanaged endpoints. And nearly 80% of data breaches stem from applications and emails that are both accessed primarily through browsers.

This convergence of risks leads to a single, clear conclusion: the browser is the new endpoint, and it must be secured as such.

Enter the Secure Enterprise Browser, a transformative approach to an age-old blind spot. Rather than fortifying the perimeter and hoping for the best, this solution embeds security directly into the browser itself. It allows organizations to enforce consistent policies across devices, whether managed or not, and offers centralized visibility and control without disrupting the user experience.

The shift is already underway. Gartner predicts that by 2028, a quarter of all enterprises will deploy at least one Secure Enterprise Browser to bridge specific security gaps in remote access and endpoint protection.

Some tech vendors such as Palo Alto Networks go even further, suggesting that by 2030, secure browsers will become the primary platform for both workforce productivity and protection, seamlessly supporting hybrid work environments.

What sets the Secure Enterprise Browser apart is its ability to offer trusted encryption, isolate risky sessions, prevent screen scraping or keylogging, and restrict access to only approved enterprise environments. It ensures files downloaded from sensitive systems remain encrypted and can only be opened in secure browser sessions. It protects data inside collaboration apps, ensuring uploads happen only to corporate-approved accounts. And crucially, it delivers all of this without the operational overhead or cost of legacy VDI systems.

**Nikola Kukoljac**
VP – Solutions Architecture,
Help AG

The implications are profound. Organizations can now enforce Zero Trust principles at the browser level, even across unmanaged devices. They gain transparency, agility, and resilience, without sacrificing productivity or user freedom.

As hybrid work becomes the norm and digital boundaries continue to blur, it's time we recognize that the browser isn't just a window to the internet, but the front door to the enterprise. And like any front door, it must be secured.

The Secure Enterprise Browser may well be the cybersecurity breakthrough this decade has been waiting for. The future will decide whether this is a game-changer in the cybersecurity world. But if you ask me, I'm placing my bet that it is.

GEC Global Enterprise Connect

# The AI Times

INSIGHTS FOR A SMARTER WORLD

# Transforming property management

Firas Jadalla, Regional Director – Middle East, Turkey & Africa, Genetec, on how security technology enhances safety and efficiency.

According to Numbeo's 2025 Safety Index, the UAE was ranked the second safest country in the world, while Saudi Arabia placed 14th. With a strong regional emphasis on safety and security, demands on property managers continue to grow. From rising tenant expectations and evolving government regulations to increasing pressure to align with smart city initiatives, property managers across the Middle East face mounting complexity. At the heart of these challenges is the need for improved security—not just protecting physical assets, but also ensuring tenant safety, safeguarding data, and streamlining operations. Increasingly, unified security platforms are emerging as the preferred solution.

For years, property security relied on a patchwork of disconnected systems: one for access control, another for surveillance, a third for alarms. This fragmentation created more problems than it solved. Operators had to juggle multiple interfaces, training was inefficient, and critical time was lost switching between platforms during incidents. Siloed systems also made it harder to investigate incidents. Video footage might not sync with access control logs, making it difficult to reconstruct what happened. In an environment where time is critical, whether responding to an emergency or providing evidence for legal purposes, this disconnection can become a major liability.

## DNS: An Overlooked Open Door

A unified security platform combines core functions like video surveillance, access control, license plate recognition, and communications into a single, cohesive system. Everything works together through one interface, with centralized monitoring and streamlined operations.

This unified approach offers several practical benefits. It ensures faster response times because security staff can instantly access video feeds, access logs, and alarms from one dashboard. Investigators can quickly correlate data across systems, simplifying evidence collection and reducing case resolution times. Staff only need to learn one system, making onboarding easier and reducing human error. With automation and integrated workflows, property managers can spend less time on manual tasks and more time focusing on tenants and strategy.

## Avoiding proprietary system pitfalls

Open-platform solutions offer flexibility, allowing property managers to adopt best-in-class tools, support phased deployments, and scale over time without disruption. This is especially valuable for multi-site portfolios or budget-conscious teams, enabling gradual improvements aligned with strategic priorities. Open architecture also improves the adaptability of investments, making it easier to integrate emerging technologies like AI-based analytics, smart sensors, or cloud storage without replacing the entire system.

## Enhanced tenant satisfaction

Tenants expect more than just a place to live or work; they expect a safe, responsive environment. Unified security systems play a key role in meeting those expectations. For example, mobile access control lets tenants unlock doors with their phones, reducing the hassle of lost or stolen keycards. Visitor management systems streamline guest access without compromising security.

Advanced surveillance and real-time monitoring contribute to a heightened sense of safety. All of these features can enhance tenant satisfaction and retention rates.

## Data-driven decision-making

Modern unified security platforms aren't just about security — they're also about insights. They enable remote management, a huge advantage when property managers might oversee multiple sites or work from different locations. Additionally, analytics can show patterns of building use, parking congestion, tenant foot traffic, and more. These insights can guide operational decisions, from staffing levels to building maintenance schedules. Data-driven property management isn't a future concept; it's happening now.

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

## Preparing properties for the future

The technology landscape is evolving rapidly. With a unified platform built on open architecture, property managers gain flexibility to adopt innovations as they emerge without overhauling their entire system. Whether integrating smart building tech, new forms of biometric access, or AI-based threat detection, a unified approach ensures that properties can adapt to future needs.

CAAS©

# GLOBAL CIO EXPERTISE, DRIVING INNOVATION FOR PEOPLE AND PLANET

**CONSULTING | RESEARCH | ON DEMAND**

www.iamcaas.com

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

# **No more** blind trust

In modern data-upload security, detection and mitigation are not enough; we must interrogate every file, writes Saif Alrefai, Solution Engineering Manager, OPSWAT

To most observers, the United Arab Emirates (UAE) is the home of economic progress — of the interminable development of society, infrastructure, and technology. In fact, without technology, many of the great things achieved by the Gulf nation would not have been possible, including its world-famous voyage to Mars. But in 2025, even a space-faring country like the UAE can fall prey to the cyberthreat landscape. In 2023, one report claimed 87% of UAE-based businesses had suffered a cyberattack. Last year, the UAE Cyber Security Council released a report highlighting some 155,000 vulnerable digital assets within national borders, and warning that 40% of critical vulnerabilities had, at the time, been unpatched for more than five years. Business leaders' attitudes to cybersecurity have come a long way from the days of questioning whether it was really needed. Now probing questions are being asked, such as those surrounding the sharing of files with employees, partners, and consumers. File uploads are an essential part of many business processes and to eliminate them would be to invite crashes in productivity and service levels.

But any file, even (indeed, especially) those that appear genuine — resumes, invoices, and the like — can contain malicious content. OPSWAT's global Web Application Security report shows file-borne malware to be on the rise, with 76% of survey participants telling us they were more concerned about it than previously. The analysis of incoming files has become a business-critical issue.

## Policy and policing

When sitting down to tackle the problem of securing file uploads, the first hurdles are those of policy. What is acceptable and what is not? What restrictions can protect the environment without impacting productivity? And what of users? If they are trained, what guarantees are there that they will follow that training strictly in their day-to-day work? Then the process of file validation must be examined for flaws.

Is the preprocessing function tamperproof? Also, is sandboxing used? If so, how accurately does it reflect the production environment?

These questions will focus on the organization's strategy for file-upload security. Moving on to use cases, it is important to ask when and why users upload files, and what the most common formats are. Business stakeholders of all stripes must collaborate to quantify the risks of allowing each type of file in the door. Some common considerations may include those around the necessity

**Saif Alrefai**
Solution Engineering Manager, OPSWAT

of permitting embedded JavaScript in PDFs or admitting entry to documents that contain hyperlinks, macros, OLE objects, or ActiveX controls. Policymakers may also spend some time on the problem of determining the authenticity of an image file.

Whatever policy decisions are the result of these strategy discussions, the next step is to determine how to enforce them. AI has made technology solutions smart enough to implement the most detailed governance frameworks. The CDR agent to identify embedded content like macros, hyperlinks, and OLE objects. It examines file extensions to prevent complex files from masquerading as simpler ones. All common file formats — PDF, Microsoft Office, HTML, and many more — are supported.

The next stage in CDR is to purge malicious content from files and to do so in a way that does not disrupt business operations. Quickly and accurately, file elements are separated into discrete components. Identified in consultation with the latest threat intelligence, potentially dangerous elements are removed, and the file is meticulously reconstructed. All the legitimate elements of the file, including its metadata, remain intact, allowing it to be used safely with no loss of functionality.

## Forward-thinking

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

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


ability to scan for vulnerabilities and to detect malware are musts, but to go the extra mile, organizations should look for technologies that can neutralize threats on a file-by-file basis. Content Disarm and Reconstruction (CDR) is such a technology.

## Would you step over here, please?

CDR is deserving of its reputation as a data-sanitization technique. It is threat prevention at its most advanced because it dissects files, removes harmful content, and then stitches files back together. Its strength lies in the fact that while its roots are in zero-trust philosophy, it does not rely on detection. Zero trust demands that we treat all traffic as suspicious. CDR does this as part of a three-step process.

First, files are pulled aside like passengers in an airport. In its role as a customs official, CDR opens every suitcase looking for contraband. It is thorough, leaving no possibility overlooked. Based on its type, each file is compared against thousands of industry formats to evaluate its consistency. Multiple scans allow the

> When sitting down to tackle the problem of securing file uploads, the first hurdles are those of policy.

## Enjoy your stay

There are no other stages. The power of CDR is that its complexity remains hidden. To an end user, the file has been delivered intact with no interference — every sock and toothbrush in the suitcase is where it was. Even complex files like PowerPoint decks show no signs of tampering. And yet the user has taken delivery of a copy. The original has been quarantined for further examination. In such a way, robust security and optimum productivity can coexist.

# **The Rise of AI-Powered Cybercrime:** Are Your Defenses Ready?

**Rehisha Pallikkathodi Erathali**
Assistant Editor,
GEC Media Group

Cybercrime has always been a big problem, but now it's getting smarter—and faster—thanks to artificial intelligence (AI). Criminals are no longer just relying on old tricks. They are using AI tools to plan and launch attacks in ways that are harder to spot and stop.

## What does this mean?

Imagine a phishing email that looks almost perfect. It doesn't have the spelling mistakes or strange language we used to see. That's because AI tools can write messages that sound exactly like your boss, your bank, or your favorite online shop. These emails can trick people into clicking harmful links or sharing passwords without thinking twice. Hackers are also using AI to automate their attacks. Instead of working manually, they can let AI scan thousands of systems to find weak spots in minutes. This makes attacks faster, cheaper, and more targeted.

## Why should we care?

These AI-powered threats mean that the old ways of defending our systems may not be enough. Firewalls and antivirus software still help, but they can miss clever, AI-generated attacks. Even employees who are usually careful can get fooled by realistic messages or fake websites.

## How can we stay safe?

Here are a few simple steps every organization—and every person—should consider:
**Train people regularly:**
Teach employees to look out for unexpected emails or requests, no matter how real they seem.
**Use multi-factor authentication:**
This adds another layer of protection, so stolen passwords alone won't give criminals access.
**Keep systems updated:**
Many attacks target outdated software. Regular updates fix known security gaps.
**Invest in smarter security tools:**
Modern security solutions can also use AI to detect unusual behavior and block threats faster.
**Have a response plan:**
If an attack happens, know exactly who will do what to reduce damage quickly.

AI is changing many industries for the better, but it also gives cybercriminals new powers. The good news is that defenders can use AI too. By staying alert and using the right tools and training, we can keep our systems—and our data—much safer.

www.futureitsummit.com

Unveiling the future at
#futureitsummit

GEC Global Enterprise Connect

11TH EDITION

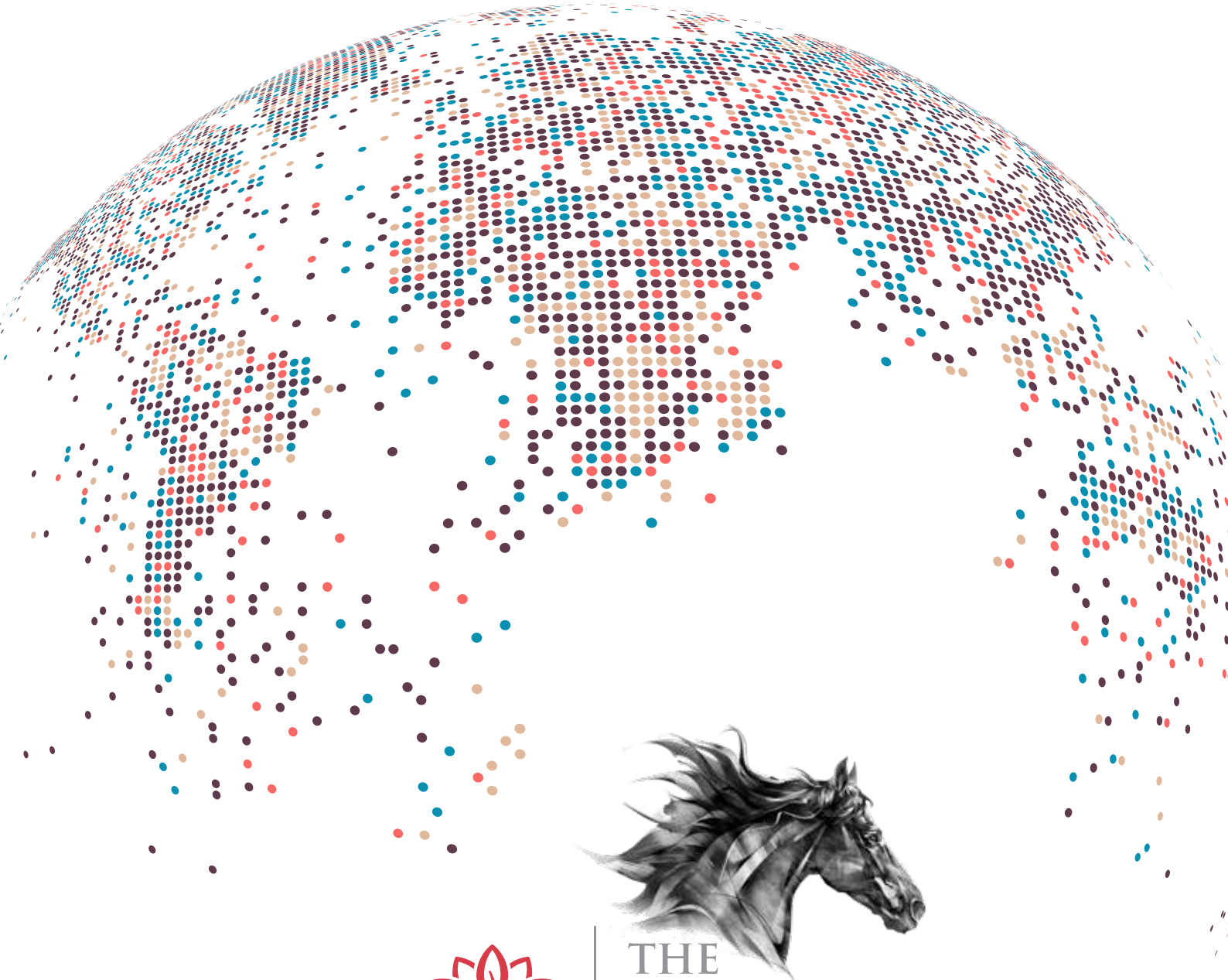
# FUTURE IT SUMMIT 2025

UAE - 18 FEB • KSA - 16 APR • PHILIPPINES - 22 OCT •
SINGAPORE - 24 OCT • INDONESIA - 27 OCT • MALAYSIA - 29 OCT •
INDIA (MUMBAI) - 12 NOV • INDIA (BENGALURU) - 14 NOV •
KENYA - 19 NOV •

POWERED BY

BOTS | GLOBAL CIO FORUM

GEC Global Enterprise Connect



# THE WORLD CIO 200 SUMMIT

## 2025 ROADSHOW

APRIL-SEPTEMBER 2025

# BOLD. UNSTOPPABLE.