

SECURITY INSIGHTS

VOLUME 02 / ISSUE 1

MIDDLE EAST

Avinash Advani, Founder
and CEO, CyberKnight

Vivek Gupta, Co-Founder
and COO, CyberKnight

REWIRING RESILIENCE

CyberKnight on elevating
cyber first and driving smarter
security bets

A special supplement by



Barracuda AI Security

Discover, assess and
govern AI risk, without
adding complexity.



CONTENTS

06 **BARRACUDA**

07 **CENSYS**

08 **CHECKPOINT**

09 **D3**

10 **CYBERKNIGHT**

14 **F9 INFOTECH**

16 **FINESSE**

18 **FORTINET**

20 **MANAGEENGINE**

21 **SANS**

24 **TENABLE**

25 **TEKSALAH**

28 **TIGER TECH**

30 **TXONE**





CyberKnight



معرض ومؤتمر الذكاء المالي، تأمين المعلومات
GISEC
GLOBAL

The Next Move In Cybersecurity Starts Here

MEET CYBERKNIGHT AT GISEC GLOBAL 2026

Meet Our Cybersecurity Innovators

 CROWDSTRIKE

 xage
SECURITY

 CYWARE™

 immersive

 harness

 FORESCOUT

 advenica

AppGate

invicti

 NETWITNESS

netwrix

 REZILENS
Confidence in Resilience

 SOLARWINDS

 SWIMLANE

 Counter
Craft

CERTES

16-18 Sept 2026 | Dubai Exhibition Centre (DEC), Expo City

Hall 9 | Booth A170

www.cyberknight.tech

PRESSURE POINTS

Security has spent years trying to close every gap. The harder reality is that the enterprise now creates new ones faster than any control environment can fully contain.

Cloud has dispersed infrastructure. AI is introducing systems that can act with growing independence. Machine identities now sit alongside human ones. Data moves across more applications, partners and platforms than ever before.

The challenge is no longer simply keeping attackers out. It is maintaining control when the boundaries of the organisation are constantly being redrawn.

That changes what a strong security posture looks like. Today, it is increasingly measured by how clearly an organisation understands its exposure, how quickly it can judge what matters, and how well it can keep operating when something goes wrong. Resilience sits at the centre of that equation, not as a recovery plan, but as a measure of whether the business can absorb disruption without losing direction.

Trust is changing too. It can no longer rest on fixed assumptions about users, devices or systems. In increasingly automated environments, access has to be justified continuously, and security decisions need context rather than another layer of alerts.

This edition of *Security Insights ME* examines a cyber environment in which accumulation is giving way to judgement: fewer disconnected decisions, better use of intelligence, and a much closer relationship between security and business continuity.

The real test of security will not be whether every threat can be stopped. It will be whether the organisation can recognise what matters, act before disruption spreads, and continue to perform when its assumptions are tested. That is where resilience stops being a security objective and becomes a measure of the enterprise itself.

Published by



Publication licensed by
Sharjah Media City
©Copyright 2026 Insight
Media and Publishing

Managing Editor

Adelle Geronimo
adelleg@insightmediame.com
+97156 - 4847568

Production Head

James Tharian
jamest@insightmediame.com
+97156 - 4945966

Commercial Director

Merle Carrasco
merlec@insightmediame.com
+97155 - 1181730

Administration Manager

Fahida Afaf Bangod
fahidaa@insightmediame.com
+97156 - 5741456

Operations Director

Rajeesh Nair
rajeeshm@insightmediame.com
+97156 - 4110215

Designer

Anup Sathyan

BEYOND DEFENCE

Elie Kortbawy, Sales Director – Middle East, Barracuda Networks, explores why cyber resilience now depends on stronger identity, integrated security, faster response, and the ability to recover when prevention falls short

G ISEC 2026 is built around “Cyber First: The New Digital Order”. If cyber is genuinely to come first, which business or technology decisions need to be made differently from the outset?

A “Cyber First” strategy means cybersecurity can no longer be treated as a control layered onto projects after deployment. Security, resilience, and recoverability must become core design principles for every business decision, whether launching a digital service, adopting AI, migrating to the cloud, or modernising infrastructure.

Organisations need to begin by assuming compromise is possible and designing accordingly. This means adopting Zero Trust principles, enforcing identity-centric security, ensuring continuous monitoring, and embedding recovery capabilities from day one.

Equally important is reducing operational complexity. Security teams cannot effectively defend increasingly distributed environments using disconnected tools and fragmented visibility. A unified security platform can provide the context and automation required to manage risk at scale while improving cyber resilience.

What is the industry still getting wrong about resilience,



“The most resilient organisations focus on operational preparedness, unified visibility, and continuous validation of their security controls”

particularly when prevention can no longer be treated as the only measure of success?

Many organisations still equate resilience with prevention.

True cyber resilience is measured by how quickly an organisation can detect, respond, contain, recover, and continue operating during an attack. Success is not simply about avoiding incidents, but minimising business disruption when they occur.

We continue to see organisations overinvest in point solutions while underinvesting in visibility, response automation, managed detection, and recovery readiness. The most resilient organisations focus on operational preparedness, unified visibility, and continuous validation of their security controls. Managed XDR, identity resilience, and data recovery capabilities are therefore becoming as important as traditional preventative controls.

From your organisation’s position in the ecosystem, where can you have the greatest impact on the cyber challenges emerging in 2026?

Barracuda’s greatest impact lies in simplifying cybersecurity while improving resilience.

Organisations face growing pressure from AI-powered attacks, expanding attack surfaces, skills shortages, and security tool sprawl. Barracuda addresses these challenges through an integrated platform approach that brings together email security, application protection, network security, SecureEdge, AI governance, data protection, and Managed XDR within a unified operational framework.

By reducing complexity and providing AI-powered visibility, threat detection, and response, we help customers achieve stronger security outcomes without significantly increasing the operational burden. Our focus is on enabling organisations to strengthen resilience rather than simply adding more tools. 

BEYOND THE BLIND SPOT

Meriam ElOuazzani, Vice President for Middle East, Turkey, and Africa, Censys, discusses the growing importance of continuous visibility as digital environments become more interconnected

How is Censys approaching GISEC GLOBAL this year, and what role does the region play in its broader strategy?

At GISEC, Censys is looking at how to make the idea of “Cyber First” tangible by connecting national cybersecurity strategies with the practical requirements CISOs face within their organisations.

That includes AI-driven resilience, critical infrastructure exposure and the partner ecosystems influencing decisions across government, finance and energy.

Our focus is on turning external exposure into something organisations, partners and national cybersecurity teams can understand and act on. Across the META region, that means helping organisations assess what they actually have exposed to the internet and where the risks sit.

Ultimately, we want organisations visiting GISEC GLOBAL to leave with a clearer understanding of their external exposure.

What steps should organisations take to strengthen exposure management and build greater resilience against evolving cyber threats?

“Do we understand our attack surface?” is an important question business leaders need to ask.

Internet-connected infrastructure is expanding through cloud

“The priority is understanding what is genuinely exposed and acting before those exposures become incidents”

integration, third parties, mergers and acquisitions, and AI at a pace that traditional inventory processes often cannot keep up with. Moving from reactive security towards real-time exposure management requires visibility into the actual attack surface, how it is interconnected and how it is changing.

It does not mean eliminating every vulnerability. The priority is understanding what is genuinely exposed and acting before those exposures become incidents.

What security challenges are emerging as cloud, identity, IT and operational technology become increasingly interconnected?

The biggest gaps are not necessarily within the individual technologies themselves. Cloud, identity, IT and operational systems



can each have strong controls, but exposure often emerges in the connections between them, particularly as data, access and trust move across increasingly complex environments.

For CISOs across the region, the priority is not simply adding another dashboard. It is having a clear, continuously updated view of how systems connect, what is exposed, who is responsible and where potential risks can emerge. This becomes even more important as organisations align their cybersecurity strategies with frameworks in the UAE and the objectives of Saudi Vision 2030.

Cybersecurity strategies need to move from periodic assurance towards continuous visibility and active management of the entire digital estate. Internet Intelligence can provide that external perspective within existing security operations, while stronger coordination between identity, cloud, IT and OT teams can help organisations understand exposure across the wider environment.

The organisations best positioned to respond will be those that can identify changes in their external attack surface early, understand how assets are connected and quickly determine where action is required. [S2](#)

CHECK POINT

SECURING AUTONOMY

Ram Narayanan, Country Manager, Check Point Software Technologies, Middle East, on governing trust across AI-driven environments and making cyber a business priority

With security stacks becoming increasingly crowded, what deserves a permanent place in the architecture and what is becoming less relevant?

The security stack is moving away from a model where every new threat leads to another standalone tool. The capabilities becoming indispensable are those that can work together, share intelligence and apply prevention consistently across hybrid networks, cloud environments, users, devices and AI systems.

Products that operate in isolation and simply generate another stream of alerts are becoming harder to justify. That does not mean detection, response or specialist technologies are losing importance. They remain essential, particularly for

“As organisations connect more systems and adopt more autonomous technologies, security can no longer depend on static trust”

investigation and response, but they need to connect into a broader architecture.

Security teams need fewer disconnected decisions and more coordinated protection. The direction is towards a unified and open architecture where intelligence can move quickly between controls and preventive action can be taken before a threat develops into an incident.

Where do you believe Check Point can make the biggest difference as organisations respond to faster, more automated threats?

The greatest impact comes from making threat intelligence actionable at the point where an attack can be stopped. Check Point's role in the ecosystem is to help organisations secure their AI transformation with prevention-first protection across hybrid networks, cloud environments, digital workspaces and AI systems.

That matters because attackers are no longer operating at a pace that allows defenders to rely on manual investigation alone. Check Point's Cyber Security Report 2026 recorded an average of 1,968 attacks per organisation per week during 2025, a 70% increase from 2023.

The answer cannot simply be more analysts investigating more alerts. Threat intelligence, AI and automation need to work together across a unified



and open architecture so emerging attack techniques can be translated into preventive protection quickly, ideally before an attack becomes an incident.

What would it take for “Cyber First” to become a genuine business principle?

Cyber has to move upstream of the technology decision itself. If an organisation is deploying an AI service, connecting a new cloud workload or introducing another connected system, security cannot be a review that happens after the architecture is already in place. It should shape how the technology is designed, what it can access and how threats are prevented from escalating into a wider compromise.

That is the practical meaning of prevention-first security: applying protection where attacks can occur, before they become incidents. “Cyber First” should mean treating security as an architectural requirement from the outset, alongside performance, cost and business value. When security is designed in rather than added later, organisations can adopt AI, cloud and connected technologies with greater confidence and less complexity. 

D3

RECALIBRATING SECURITY

Faisal Qureshi, Sales Director, Dominant Digital Distribution (D3), discusses how cyber-first thinking is changing the way organisations approach security, risk and resilience

As the security stack continues to evolve, which capabilities are becoming indispensable, and which are losing relevance?

The security stack is shifting away from large numbers of isolated tools towards more integrated and intelligent platforms.

Capabilities such as identity and Zero Trust, AI-driven detection and response, XDR and SIEM, cloud and data security, continuous posture management, threat intelligence, and automated incident response are becoming increasingly important. AI-agent security is also emerging as a priority as organisations deploy more autonomous systems.

What is losing relevance is the traditional dependence on perimeter-only security, signature-based detection, manual monitoring, and disconnected point solutions. Modern security increasingly relies on behavioural detection, shared intelligence, automation, and visibility across identity, endpoint, cloud, network, data, and AI environments.

What role can D3 play in helping customers respond to the next phase of cyber risk?

Our greatest impact is in helping customers turn cybersecurity strategy into practical, integrated solutions.

As a technology distributor and channel partner, we can connect leading technologies with local



“Organisations should invest in capabilities that make them secure, adaptable, and recoverable, rather than simply better at preventing attacks”

market requirements, strengthen partner capabilities, and accelerate the adoption of AI-driven security, Zero Trust, data protection, and cyber resilience.

In 2026, our role is not simply to distribute products, but to help build an ecosystem that reduces complexity, enables faster responses to emerging threats, and supports business continuity.

Which capabilities should organisations invest in today to strengthen cyber resilience by 2030?

Organisations should invest in capabilities that make them secure, adaptable, and recoverable, rather than simply better at preventing attacks.

Priorities include Zero Trust and modern identity management, AI-driven detection and response, data security, cloud security, automated security operations, and strong backup and disaster-recovery capabilities. Identity will become increasingly important as AI and non-human identities expand.

AI governance, continuous risk monitoring, skilled cybersecurity teams, incident-response exercises, and stronger supply-chain and third-party resilience will also be critical.

By 2030, resilience will depend on an organisation's ability to detect disruption early, verify what can still be trusted, recover quickly, and continue delivering critical services during an attack.

What does putting cyber first actually demand from business and technology leaders?

“Cyber First” means cybersecurity must be built into business and technology decisions from the beginning, rather than added later. Organisations need to design secure architectures, protect data and identity from day one, assess vendors on security and resilience, govern AI carefully, and treat cyber risk as a board-level business issue.

For channel partners, this also creates an opportunity to move beyond selling individual products and become trusted advisers, delivering integrated solutions across cybersecurity, AI, data infrastructure, governance, and resilience. [S2](#)

REWIRING RESILIENCE

As cyber risk becomes more deeply embedded across the enterprise, **Avinash Advani**, Founder and CEO, and **Vivek Gupta**, Co-Founder and COO at CyberKnight, discuss what it takes to make cyber first a business priority, sharpen security decisions and invest where it matters most

Cyber risk is being created much earlier in the enterprise technology cycle. Decisions around AI, cloud workloads, connected industrial systems and digital services are defining part of an organisation's exposure before the security team ever selects a control. Regulation and geopolitical pressure are raising the cost of getting those decisions wrong.

"We founded CyberKnight in November 2019, and just a few months later COVID happened, which significantly accelerated the cybersecurity space," says Avinash Advani, CEO and Co-Founder, CyberKnight. "Since then, we've had geopolitical developments across the region continuing to influence the threat environment, while regulation has become a much bigger factor. More industries are coming under new cybersecurity and compliance requirements, so all of these forces are shaping the market at the same time."

For security leaders, the benchmark is also changing. Preventive controls remain essential, but resilience is increasingly measured by what happens once an incident begins affecting operations.

"Organisations have been improving their security posture step by step, from foundational security to advanced security and

then towards frameworks that give them a more mature adoption of cybersecurity, like zero trust," says Advani. "Resilience is really the stage where cybersecurity becomes a horizontal layer across the organisation. It becomes a board priority. It is no longer just about whether you are going to get attacked. It is about knowing you are going to get attacked, being able to recover as quickly as possible and aiming for business continuity."

A wider mandate

The organisational structure is beginning to reflect a much wider security remit.

"Historically, cybersecurity sat within IT, and the CISO, where the role existed at all, typically reported to the CIO," says Advani. "Today, the CISO has a much more distinct mandate and, in many organisations, direct visibility at board level."

More of the risk now sits outside the traditional IT estate, as individual business functions adopt their own technologies and handle increasingly sensitive data.

"Cybersecurity can no longer operate as a vertical function. It has to run horizontally across the enterprise because every part of the business, from finance and HR to operations and manufacturing, now carries some degree of cyber exposure," explains Advani.

GISEC 2026's Cyber First: The New Digital Order theme reflects how closely cybersecurity is now tied to the way organisations build, deliver and scale digital services. What was once treated largely as a technology concern is increasingly becoming a condition for doing business digitally.

"Cyber first has moved beyond technology. It is now fundamental to how businesses operate," says Vivek Gupta, COO and Co-Founder, CyberKnight. "The digital economy depends on trust, and cybersecurity is what helps create that trust. It is no longer about having security technology in place for its own sake; it is about enabling the business to operate and grow securely."

The harder question is how to prioritise when the attack surface keeps expanding and resources do not.

"Cybersecurity has become one of those areas that cannot simply be pushed down the priority list," says Gupta. "Budgets do come into play, but they cannot be looked at in isolation. You have to consider the risk the organisation carries, the data it holds, the number of touchpoints it has and the threats it is exposed to. You can broaden coverage over time, but the first priority is understanding where your real exposure sits and protecting the assets that matter most, whether that is data, identity or other critical systems."

Regulation is narrowing the room for discretion. National requirements around data privacy, government systems and financial services are becoming more prominent alongside established global standards, while penalties are giving organisations a clearer reason to address gaps.

Machine vs. machine

AI is adding another layer to an already expanding security brief, with adoption moving faster than many existing security models were built to accommodate.



**“We have long
championed zero
trust, and we
remain firmly
committed to it
because we see it
as fundamental
to modern
cybersecurity”**

Avinash Advani

"AI is increasing the frequency, intensity and sophistication of attacks at a pace we have not seen before," explains Advani. "Defenders have always had to catch up with attackers, but AI is accelerating that cycle and making the gap much harder to close."

CyberKnight is looking at AI across four areas, reflecting the different ways it is entering the security equation.

"AI is not just changing how organisations defend themselves. It is changing the attacks they face, the technologies employees are using and, increasingly, the systems being given the ability to act autonomously," says Advani. "That is why we are looking at four areas: how defenders use AI, how organisations govern it, how they secure AI agents and, ultimately, where AI can deliver real value in cybersecurity."

The first two cover defence and governance.

"For defenders, it is about using AI-powered tools to counter AI-driven attacks. At that level, it is increasingly AI versus AI," he says. "The second is governance: what data is going into these systems, how that data is controlled and how organisations prevent sensitive information from being exposed or misused."

Agentic AI carries a different risk because these systems can be authorised to act across corporate applications rather than simply generate information.

"The third is securing the agents themselves. If an AI agent is operating across finance, HR, marketing or other business functions, you need to understand what it can access and what it is allowed to do," adds Advani.

The fourth is about turning the technology into practical security value.

"Our role is also to help organisations identify the AI use cases that can genuinely strengthen their cybersecurity," he says. "AI SOC and offensive security are two of the highest-demand areas today, but I expect a much broader set of use cases to emerge very quickly."

Cutting through the stack

New security requirements keep producing specialist technologies just as customers are trying to simplify estates built up over years of point-product purchases.

"Tool sprawl is a huge problem for everybody, and every enterprise, large enterprise and government organisation is looking to consolidate," says Advani. "Where

platformisation is going to have the maximum effect is foundational security. SASE is a great example because it enables you to consolidate several tools into one platform. But advanced and next-generation security still require specialised capabilities and products."

Larger platforms can absorb many established functions, but specialist vendors continue to find opportunities where existing technologies leave gaps.

"Many times, the earlier tool was not providing that final bit, and there is a company that has found a gap in the market and is able to address it," says Gupta. "Those tools will continue to come up, but there has got to be consolidation rather than more and more tools coming in, because it becomes difficult for the customer to manage them."

For the channel, the value increasingly lies in filtering those options. CyberKnight evaluates multiple technologies every couple of months, looking for capabilities with proven use cases that can address requirements among regional enterprise and government customers.

"We try to look at path-breaking technologies that we could bring into the region," says Gupta. "Through our channel reach and our end-customer touchpoints, we are able to take technologies that have been helping customers in other parts of the world and give organisations here a view of the value they could add to their own ecosystem."

New ground for cyber

Cloud adoption across MEA remains uneven, with data privacy, residency and sovereignty requirements producing different models from one country to another. Local hyperscaler expansion is giving more enterprises and governments the ability to move workloads while meeting domestic requirements.

"The whole concept of how security needs to be looked at is going to change, and it goes beyond just cloud security," says Advani. "Cloud needs to be included by default. AI is also going to be important, and the third area for this region is OT and IoT."

The Middle East's sizeable industrial footprint gives IT, OT and IoT convergence particular weight. Across the wider MEA market, another source of demand is emerging as governments accelerate national digitisation programmes and bring more services and infrastructure online.





“The digital economy depends on trust, and cybersecurity is what helps create that trust”

Vivek Gupta

“National digital transformation strategies are driving the next level of growth,” says Gupta. “There are markets across Africa that will need much more cybersecurity as governments accelerate their own digital transformation agendas.”

In response, CyberKnight aims to strengthen its local technical capability and introduce technologies that address the region’s evolving security needs.

“We will continue investing in local teams in the countries where we see growth, and we will establish that presence before the growth arrives,” says Gupta. “Our commitment to developing local talent and giving the channel the support it needs to build the business will remain a top priority.”

Across those areas, zero trust remains the organising principle CyberKnight intends to carry forward.

“We have long championed zero trust, and we remain firmly committed to it because we see it as fundamental to modern cybersecurity,” says Advani. “When zero trust is embedded across the security estate and implemented effectively, organisations are far better positioned to achieve resilience. It is an ambitious goal, but a realistic one, and we want to help organisations make that journey.”

SECURING NEW FRONTIERS

Jayakumar Mohanachandran, Founder of Kerala Cyber Suraksha Summit and Co-Founder and CEO of F9 Infotech, reflects on the priorities that emerged from the event and what they reveal about the changing demands of cyber resilience



Enterprises have spent years investing in controls designed to keep attackers out. The harder question now is what happens when one gets through. Cloud platforms, AI, connected infrastructure and digital services are integral to day-to-day operations, which means a cyber

incident can stop production, disrupt supply chains, expose data and damage customer confidence. Prevention still matters, but it can no longer be the only measure of security.

Kerala Cyber Suraksha Summit 2026, held on 5 September in Kochi, brought together

government, law enforcement, CIOs, CISOs, technology companies, financial institutions, academia and entrepreneurs. The agenda ranged from AI security and national cyber preparedness to data protection, financial-sector resilience, identity, cloud, OT and citizen safety.

“Kerala Cyber Suraksha began with a very simple conviction: cybersecurity should not remain confined to boardrooms, SOC’s or technology conferences. It must ultimately protect every business, institution and individual,” says Jayakumar Mohanachandran, Founder of Kerala Cyber Suraksha Summit, and Co-Founder and CEO of F9 Infotech. “We felt somebody needed to create a platform where we could discuss both at the same table. That became the founding idea behind Kerala Cyber Suraksha: bring the ecosystem under one roof – not only to discuss cyber threats, but to explore the opportunities created by AI, innovation and digital transformation while asking how we secure that future together.”

Much of the summit centred on how organisations define resilience as their dependence on digital systems grows. “For years, organisations asked, ‘How do we prevent an attack?’ Today, the more important questions are: Can we anticipate it? Can we detect and contain it? Can we continue operating through it? And how quickly can we recover?” explains Mohanachandran

He adds: “A cyber incident can stop operations, disrupt supply chains, compromise customer trust, create regulatory exposure and destroy enterprise value. Cyber risk has become business risk,” he says.

AI featured heavily across KCSS, both as an opportunity and a source of new risk. “AI makes this even more urgent because it accelerates both sides of the equation. Defenders have more powerful capabilities, but adversaries can also automate attacks, personalise social



engineering, manipulate identities and operate at unprecedented speed and scale,” says Mohanachandran.

Security culture was another recurring concern. “We can invest millions in cybersecurity technology, but one compromised identity, one convincing deepfake, one careless click or one moment of misplaced trust can still open the door,” Mohanachandran says. “Cybersecurity cannot be built only inside the SOC. It has to be built into organisational culture.”

Skills formed another part of the conversation, particularly as the range of cyber roles expands beyond traditional security functions. “We often describe cybersecurity as having a talent shortage. I see it slightly differently: India has a massive talent-conversion opportunity,” he says. “We have one of the world’s largest pools of young technology talent. The challenge is building stronger bridges between education, industry and the cybersecurity skills that organisations actually require.”

F9 has linked that priority to practical programmes, including free 24/7 SOC and cybersecurity services for 500 MSMEs and startups and the Kerala Cyber Resilience Foundation, through which cybersecurity training and certification are being made available free of cost to educational institutions across Kerala. “If

“Our job as technology and cybersecurity leaders is not simply to protect technology. It is to protect the trust that allows society to use technology with confidence”

we want to solve tomorrow’s cybersecurity challenge, we have to start building tomorrow’s cyber defenders today,” says Mohanachandran.

KCSS also placed collaboration high on the agenda. “Cybersecurity is a team sport - and nobody can defend the digital economy alone. Attackers do not recognise corporate boundaries, industries, states or national borders. Our defences cannot afford to remain fragmented by them,” explains Mohanachandran.

The summit also brought Indian and Middle Eastern perspectives together through its “AI Security Beyond Borders” discussion. “At Kerala Cyber Suraksha, ‘AI Security Beyond Borders’ brought Indian and Middle Eastern perspectives

together around AI security, cross-border risk, regulation, enterprise resilience and trust,” he says. “It reinforced something I have believed for a long time: the next phase of collaboration needs to move beyond the traditional customer-and-service-provider relationship.”

“The most powerful takeaway from Kerala Cyber Suraksha 2026 was that cybersecurity is no longer one conversation. It is the thread connecting almost every major conversation about our digital future,” says Mohanachandran. “You cannot discuss AI without discussing trust. You cannot discuss digital transformation without discussing resilience. You cannot discuss data without discussing privacy and accountability.”

KCSS is intended to continue beyond the annual summit itself. “Our ambition is to build KCSS into a year-round platform connecting awareness, leadership, skills, innovation, policy, social impact and international collaboration,” he says. “Our approach has always been that the conversations on the KCSS stage should eventually translate into action outside the conference hall.”

As Mohanachandran puts it: “Our job as technology and cybersecurity leaders is not simply to protect technology. It is to protect the trust that allows society to use technology with confidence.” 

THE RESPONSE IMPERATIVE

Eljo JP, Chief Business Officer, and Pradeep Krishnan, VP-IT Security at Finesse, discuss the growing role of AI and automation in security operations and why cyber resilience increasingly depends on response, recovery and continuity

Which capabilities should organisations be investing in now to strengthen resilience by 2030?

ELJO JP (EJP): Organisations should invest in Zero Trust, AI-powered security and strong cyber recovery capabilities to stay ahead of evolving threats. Building a resilient, security-aware workforce will further strengthen business continuity and long-term cyber resilience.

A Zero Trust approach can strengthen identity and access management by continuously verifying users, devices and applications to reduce cyber risk. Organisations should also invest in AI-powered threat detection and automated incident response to identify and contain threats faster.

Operational resilience will also be critical. This means strengthening cyber recovery, securing cloud

environments and fostering a security-aware workforce through regular training and testing.

These investments will help organisations strengthen cyber resilience and ensure business continuity in an increasingly complex threat environment.

Where is the biggest disconnect between the cyber risks boards worry about and what security teams are actually dealing with?

Pradeep Krishnan (PK): Boards often focus on major cyber incidents, financial impact and reputational risk, while security teams are dealing with a much broader range of everyday threats, vulnerabilities and security alerts.

The rapid adoption of AI, cloud technologies and third-party platforms is also creating new risks that may not always be visible at board level. Security teams need to translate technical challenges into clear business risks and measurable outcomes. At the same time, boards need better visibility into the organisation's overall security posture and ability to respond to incidents.

Regular risk reviews, clear reporting and realistic cyber simulations can help bridge this gap. Ultimately, cybersecurity should be viewed as a shared business responsibility and a key component of long-term resilience.

“Building a resilient, security-aware workforce will further strengthen business continuity and long-term cyber resilience”

Eljo JP



“At Finesse, we believe true cyber resilience is built around advising, enabling and securing organisations for the evolving threat environment”

Pradeep Krishnan

What role are AI and automation playing in modern SOC operations?

EJP: AI and automation are integral to Finesse's Cognitive Security Operations Center (CSOC), transforming cybersecurity into a proactive and adaptive function. These technologies enhance detection by analysing vast data volumes in real time, reducing Mean Time to Detect (MTTD) by 50 percent and identifying insider threats through User and Entity Behavior Analytics (UEBA).

Automated response mechanisms, powered by Security Orchestration, Automation, and Response (SOAR), initiate immediate actions such as isolating devices or blocking malicious IPs, minimising the impact of an attack.

This integration of AI-driven analytics, automation and behavioural analysis strengthens cyber resilience by shifting operations from reactive to proactive, anticipating threats and building an adaptive defence against sophisticated attacks.

How is Finesse applying AI across its Cyberhub SOC and security services?

PK: Finesse's Cyberhub SOC offers a suite of AI-powered cybersecurity solutions designed for modern



threat environments. Our 24/7 Cognitive Security Operations Centers in Dubai and Bangalore leverage advanced AI analytics and machine learning algorithms to continuously monitor the entire digital ecosystem, from endpoints to networks and cloud environments.

This AI-driven approach enables real-time anomaly detection, identification of unusual activity patterns and proactive threat neutralisation before damage occurs. Our AI systems also automate critical security workflows, reducing response times from hours to minutes, minimising human intervention and helping ensure business continuity during active threats.

As organisations adopt generative AI technologies, Finesse also provides a Gen AI Governance Framework to support responsible implementation and compliance. Our Gen AI Broker/LLM Gateway serves as a secure intermediary between users and AI systems, providing content filtering, protection against prompt injection attacks and automatic data sanitisation.

AI is also being applied across Zero Trust, cloud security, digital identity and brand protection, data protection and privacy, as well as AI and cybersecurity assessments.

What is the industry still getting wrong about resilience when prevention can no longer be the only measure of success?

PK: The industry still tends to measure cybersecurity success by how well organisations prevent attacks, rather than how effectively they can respond, recover and continue operations when an incident occurs.

At Finesse, we believe true cyber resilience is built around advising, enabling and securing organisations for the evolving threat environment. This means preparing for the reality that breaches can happen by strengthening detection, response, recovery and business continuity.

Regular testing, clear response plans, strong recovery processes and continuous improvement are therefore just as important as prevention in building lasting cyber resilience. 

SECURING WHAT COMES NEXT

Alain Penel, Regional Vice President – Middle East, Fortinet, explores why stronger cyber resilience depends on reducing complexity and building security into business decisions from the outset

As security architectures evolve, which capabilities are becoming essential, and which are losing relevance?

Three capabilities are becoming indispensable: unified visibility, automation, and AI-driven security operations.

Security teams now manage environments spanning on-premises infrastructure, multiple clouds, SaaS applications, operational technology, and remote users. Point solutions operating in isolation can create blind spots and increase operational complexity.

Organisations therefore need integrated security platforms that provide consistent visibility, coordinated protection, and automated response across the attack surface.

By contrast, fragmented architectures are becoming less effective. Continuously adding standalone tools can increase complexity without necessarily improving security outcomes. The direction is towards greater consolidation and interoperability, with less operational overhead and stronger security efficacy.

Where do you see the biggest disconnect between the cybersecurity risks boards worry about and those security teams are actually dealing with?

Boards are increasingly focused on



“Organisations need to evaluate new initiatives through the lens of cyber risk and resilience from day one”

business risks such as operational disruption, regulatory exposure, reputational damage, and the financial consequences of major cyber incidents. Security teams, meanwhile, spend much of their time dealing with alert overload, tool complexity, skills shortages,

and increasingly sophisticated threats.

At the same time, accountability for cybersecurity is moving further into the executive suite. Fortinet's 2026 State of Operational Technology and Cybersecurity Report found that 52 percent of organisations now place responsibility for OT cybersecurity with the CISO or CSO, up from 16 percent in 2022, while 95 percent report cybersecurity responsibility at the C-suite level.

As CISOs assume greater responsibility for resilience, regulatory compliance, and operational continuity, their role increasingly involves bridging these two perspectives, translating technical risk into business outcomes, and aligning cybersecurity with strategic priorities.

Where can Fortinet have the greatest impact on the cyber challenges organisations are facing in 2026?

The greatest opportunity lies in helping organisations simplify cybersecurity while strengthening protection across increasingly complex and interconnected environments.

As enterprises adopt AI, expand their use of cloud, modernise networks, and connect more critical infrastructure, complexity itself is becoming a security risk. Our role is to help customers reduce that complexity through integrated security platforms, AI-driven security operations, and the convergence of networking and security.

There is also a broader responsibility to address the cybersecurity skills gap. Through the Fortinet Training Institute and partnerships with educational institutions, governments, and industry stakeholders, we are working to expand access to cybersecurity education and help develop the workforce needed to secure an increasingly digital economy. 

Breach Ready. Board Ready. AI-Powered.

Unified Defense SIEM with Agentic AI. Sam, the AI SOC Analyst, executes Tier 1 and Tier 2 work across triage, investigation, and response, with governance and human control built in.



Breach Ready.

Less noise.
Faster action.

- Unified detection, investigation, and response
- Sam executes Tier 1 and Tier 2 SOC workflows
- Behavioral analytics and threat intelligence surface high-confidence threats
- Up to 50% less manual SOC workload



Board Ready.

Measured outcomes.
Proven execution.

- Measure AI by analyst work completed and time returned
- Up to 50% reduction in manual SOC workload
- Up to 60% faster time to respond
- Quantifiable outcomes for board-level reporting



AI-Powered.

Execution at Scale.
Control by Design.

- Sam executes frontline SOC work
- Agentic Mesh coordinates specialized AI agents
- Agentic Guardrails keep actions explainable and auditable
- Human supervision keeps analysts in control

Securonix is transforming security operations with the industry's first Unified Defense SIEM with Agentic AI, built to decide and act across the threat lifecycle with a human-in-the-loop philosophy. Its cloud-native platform unifies detection, investigation, and response, while enabling Sam, the AI SOC Analyst, and a productivity-based AI operating model for the SOC, so organizations can measure and govern AI by the analyst work it delivers. Helping enterprises become Breach Ready and Board Ready, Securonix delivers accountable, outcome-driven security operations at scale. Recognized as a Leader in the Gartner® Magic Quadrant™ for SIEM and a Customers' Choice by Gartner Peer Insights™, Securonix delivers trusted security operations for global enterprises. Learn more at www.securonix.com

securonix.com

securonix

Book a Demo



THE NEW PERIMETER

Sujoy Banerjee, Regional Business Director, ManageEngine, discusses why security now demands visibility across identities, cloud and connected assets

How is digital transformation changing the security priorities of organisations across the Middle East?

As companies across the Middle East accelerate digital transformation, the definition of enterprise security is becoming significantly broader. Security is no longer limited to protecting networks, systems and data from cyberattacks. Organisations must also consider the security of devices, applications, physical infrastructure, connected assets and the operational processes that keep the business running.

This shift is particularly important in the Middle East, where the rapid adoption of cloud, AI, IoT and smart infrastructure is creating increasingly interconnected technology environments. A vulnerability or disruption in one area can have consequences across multiple systems, affecting business continuity, customers and critical services.

Enterprises therefore need to approach cybersecurity as a connected business strategy that brings together technology, people, processes and assets. This requires greater visibility across the environment, including understanding what assets exist, who or what has access to them, how they are interconnected and where potential risks lie.

By connecting security insights across identities, endpoints, applications, infrastructure and operations, organisations can identify risks earlier, prioritise investments more effectively and build stronger resilience across the business.

As environments continue to converge, breaking down visibility and operational silos will be essential to building a more effective and resilient security strategy.

With identity emerging as a primary attack vector, what should organisations prioritise to strengthen identity and privileged access security?

Digital identity has become a primary security perimeter. As organisations operate across hybrid and multi-cloud environments, they must protect not only human users but also privileged, machine and application identities that extend beyond traditional directory boundaries.

The first step is gaining comprehensive visibility into identities and their access privileges, wherever they reside. Organisations should apply least-privilege principles and regularly review permissions to ensure users, applications and machines have only the access they need.

Privileged accounts require particular attention, with continuous monitoring to detect unusual or risky behaviour. As identities span cloud platforms, unmanaged devices and non-domain environments, directory-independent visibility and control are becoming increasingly important.

Identity security should ultimately move beyond administration and compliance to become a core component of enterprise risk management.



“Digital identity has become a primary security perimeter”

Where are organisations most exposed as cloud environments become more distributed and complex?

One of the biggest challenges is maintaining visibility across increasingly distributed cloud environments. As organisations spread workloads across multiple providers and hybrid infrastructure, fragmented monitoring can lead to inconsistent security controls, misconfigurations and undetected vulnerabilities.

Cloud identities add another layer of complexity, with accounts, service identities and privileged access multiplying rapidly across environments. This makes centralised governance and understanding who has access to critical resources increasingly difficult.

Organisations should prioritise a unified view of their cloud and on-premises environments rather than relying solely on provider-specific tools. This enables security teams to identify risks in context, apply consistent controls and understand the relationships between identities, workloads and infrastructure. 

THE SKILLS IMPERATIVE

Ned Baltagi, Managing Director – Middle East, Turkey and Africa, SANS Institute, explores how AI and emerging technologies are changing the skills, governance and capabilities cybersecurity teams need



Where are the biggest gaps in cyber resilience today?

Two areas continue to stand out: end-to-end visibility and the ability to demonstrate resilience through real-world testing rather than relying on documented plans.

Many organisations still lack a clear view of how an attacker could move through their environment, from the initial point of entry through to operational impact. Remote access and system-to-system connectivity remain particularly important, with external access linked to roughly half of confirmed incidents, while more advanced

“As technologies and threats evolve, cybersecurity skills cannot remain static”

controls capable of identifying these threats are still not widely implemented.

There is also a need to rethink how detection and incident response programmes are designed. Too often, they focus on identifying anything unusual rather than building detection around realistic threat scenarios. A more effective approach is to identify attack scenarios that have occurred within the industry, alongside a worst-case operational scenario, and use these to shape monitoring, detection and response.

For network monitoring, this means focusing on adversary behaviours and tactics so that alerts point to something specific and actionable rather than simply adding to the volume of anomalies security teams must investigate.

The visibility challenge is also evolving as AI becomes more embedded in operational environments, including predictive

maintenance, flow optimisation and production forecasting. As automated systems make more decisions at greater speed and with less direct human review, security programmes need consistent guardrails and oversight for any system, whether human-operated or automated, that can influence how a plant or grid functions.

Resilience must also go beyond having backups and failover capabilities in place. Organisations need to test whether they can recover under realistic conditions, understand system dependencies, and determine what must be restored first and in what sequence.

At SANS Institute, the focus is on helping organisations translate these principles into practice through scenario-driven detection, tested resilience, the Five Critical Controls, industry research that tracks maturity gaps, and practical training. This gives organisations a clearer, evidence-based understanding of where they stand and where improvements should be prioritised.

As cybersecurity becomes more complex, which skills are becoming most critical?

Some of the most important capability gaps are emerging where traditionally separate disciplines now overlap. Organisations need practitioners who can work across cybersecurity and AI, IT and OT, cloud and automation, as well as offensive and defensive security.

The workforce challenge is therefore no longer simply about increasing the number of cybersecurity professionals. It is about developing the specialised and cross-functional expertise required to secure increasingly complex environments.

This requires organisations to treat workforce development as an ongoing process rather than a periodic training exercise. A more effective approach starts by defining the capabilities required for critical cybersecurity roles and

“Many organisations are moving beyond reactive approaches and early-stage policies towards a more structured, risk-informed model for securing AI”

assessing existing teams against those requirements. This allows organisations to identify specific gaps and focus development efforts where they will have the greatest impact.

Practitioners also need regular opportunities to build, apply and validate their skills through hands-on labs and exercises that reflect real-world scenarios. As technologies and threats evolve, cybersecurity skills cannot remain static.

Organisations need to continuously develop and validate workforce capabilities so their people are prepared for the environments and threats they are responsible for protecting.

What separates organisations with a mature approach to AI security from those still at an earlier stage?

Many organisations are moving beyond reactive approaches and early-stage policies towards a more structured, risk-informed model for securing AI. What sets more mature organisations apart is their ability to demonstrate that security and governance measures are working in practice rather than relying on policies alone.

This starts with a clear understanding of the AI systems and agents operating across the organisation. More mature

organisations know what these systems are, the data they can access, and who is accountable for them. They also have greater clarity around how identities and permissions are managed and whether the security controls surrounding AI are being effectively tested.

Governance plays a particularly important role in this progression. Within the SANS AI Security Maturity Model, governance effectively sets the ceiling for an organisation's overall level of AI security maturity.

As AI adoption grows, organisations therefore need to move beyond simply establishing policies and build the visibility, ownership, access controls and testing needed to demonstrate that those policies are being applied in practice.

What cybersecurity priorities is SANS bringing to GISEC 2026?

At GISEC 2026, SANS is focusing on equipping cybersecurity professionals with the skills needed to address the technologies and risks changing how organisations operate and defend their environments.

AI is a key part of this focus, with the Gulf Edition of the AI Security Maturity Model, the AI Cybersecurity Career Guide, and new GIAC certifications covering areas including offensive AI, red team automation, model integrity and AI operations.

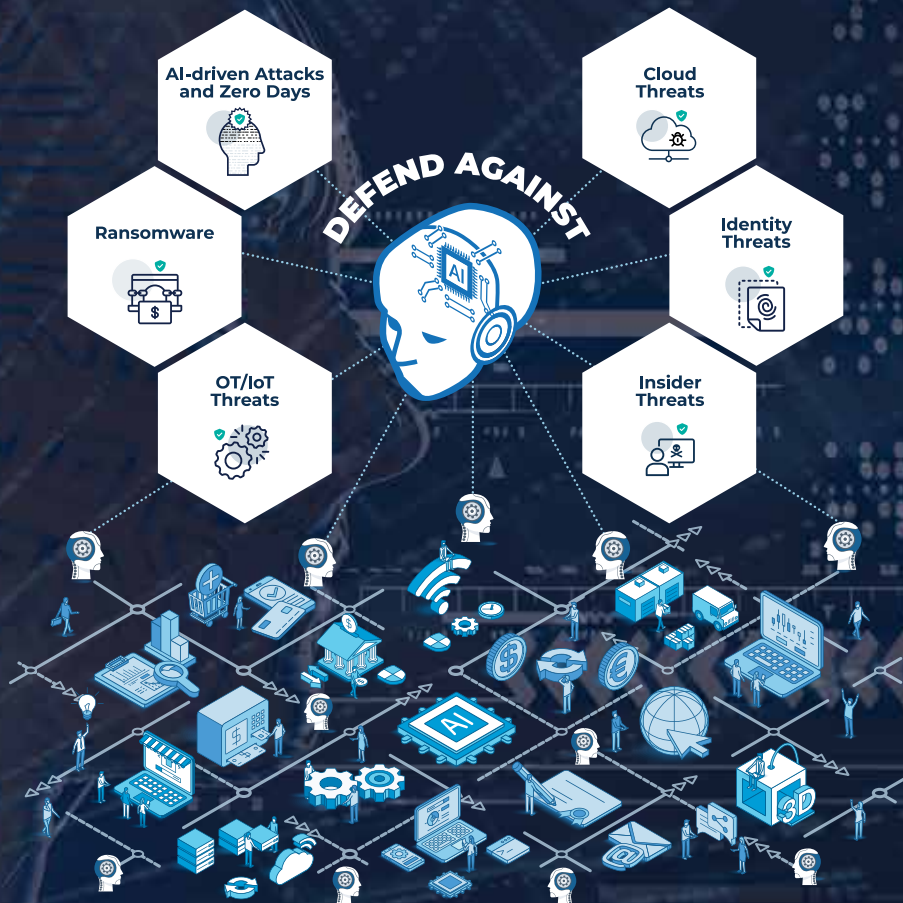
SANS is also addressing quantum readiness through executive briefings examining the implications for encryption, alongside practical workshops focused on quantum-resistant algorithms and asset inventory.

The programme extends to ICS and OT defence, cloud and container security, and third-party and industrial risk. Together, these areas reflect the breadth of cybersecurity capabilities organisations across the region need to develop as technologies and threats continue to evolve. 



Deception Guardrails for Agentic AI

Recognized as the company to beat
in the Gartner AI Vendor Race



Gartner, AI Vendor Race: Acalvio Is the Company to Beat in AI-powered Advanced Cyber Deception, December 8th, 2025

Acalvio is an AI-powered preemptive cybersecurity company focused on countering AI-driven identity and infrastructure intrusion. Its 360 Deception platform combines Dynamic Deception, evolving HoneyPaths, and cloaking of production assets within deception fabric to disrupt automated reconnaissance, credential abuse, and lateral movement across identity systems, endpoints, cloud, network, and cyber-physical environments. By altering what attackers can perceive and trust, Acalvio shifts detection from post-compromise analysis to pre-impact exposure, enabling organizations to detect, delay, disrupt, and deny malicious activity at machine speed. The company serves enterprise and government organizations determined to break automated intrusion at its source. www.acalvio.com/

TENABLE

CLOSING THE EXPOSURE GAP

Walid Natour, Director – Security Engineering, Tenable, examines how AI and expanding attack surfaces are changing cyber risk and the need for continuous exposure management



What cyber-attack and information-security trends have emerged in the UAE in 2026, and are they likely to continue through the rest of the year?

Since early 2026, cyber-attacks against UAE organisations have surged alongside regional geopolitical tensions. The UAE Cyber Security Council has reported a significant rise in daily attack attempts, with AI amplifying both the volume and sophistication of these campaigns.

At the same time, the window between vulnerability discovery and active exploitation has collapsed from months to minutes. Attackers are using automated tools to rapidly identify low-resistance entry points, chaining

together minor software flaws, cloud misconfigurations, and excessive identity permissions to create complete attack paths.

We expect this heightened pace to continue through the rest of the year. Organisations therefore need an AI-powered exposure management approach that continuously maps their attack surface and helps them stay ahead of threats rather than simply reacting to them.

As attack surfaces become increasingly complex, how can organisations identify and prioritise the vulnerabilities that pose the greatest risk?

As attack surfaces expand across cloud, identity, OT, and AI

“By applying machine learning and threat intelligence to assess real-world exploitability alongside business context, organisations can cut through the noise”

infrastructure, traditional scoring systems become less effective because they can flag too many issues as critical. The answer is to move beyond basic vulnerability discovery towards exposure management.

Organisations need a complete view of their digital footprint to understand how vulnerabilities, identity permissions, and misconfigurations connect. Rather than treating every flaw equally, security teams need to evaluate attack paths and identify which weaknesses could actually lead to core business assets.

By applying machine learning and threat intelligence to assess real-world exploitability alongside business context, organisations can cut through the noise. This allows teams to focus on the relatively small proportion of exposures that present material business risk instead of becoming overwhelmed by a backlog of theoretical threats.

What is Tenable’s key theme for GISEC GLOBAL 2026, and what security challenges will you be highlighting at the event?

At GISEC GLOBAL 2026, Tenable will demonstrate how organisations can bridge the gap between exposure discovery and automated remediation as rapid AI adoption and expanding attack surfaces create connected risks across cloud, identity, industrial systems and AI workloads.

The Tenable One Exposure Management Platform continuously maps relationships across the enterprise, helping security teams cut through alert noise, identify critical attack paths and prioritise the chokepoints that need to be addressed first.

From booth B130 in Hall 7, Tenable will also showcase Tenable Hexa AI and AI Exposure, demonstrating how agentic AI can analyse complex attack paths, prioritise material risk and automate remediation workflows before attackers can exploit them. 

TEKSALAH

NEW RULES OF RESILIENCE

Murali Konasan, CEO, Teksalah, discusses why cyber resilience is moving beyond prevention, and what organisations need to change to prepare, respond and recover as risk evolves

What does putting cyber first actually demand from business and technology leaders?

For too long, cybersecurity has been an afterthought. Businesses tend to focus first on speed, innovation and growth, while security is brought in later to manage the risk. That will not work in today's environment.

If cyber is truly to come first, the executive who approves a product, transformation or technology decision must also own its risk. Security and resilience need to be considered before something is built, not after.

Cyber First is not about buying more security tools. It is about refusing to build products, businesses and ecosystems without first understanding what can go wrong, what matters most and how the risk will be managed. Organisations that genuinely put cyber first must be prepared to accept slower initial progress or higher upfront costs in exchange

“Static controls are no longer sufficient in an AI-driven threat environment”



for lower systemic risk, greater resilience and the ability to operate with confidence.

It must become part of how we design and run the business. Events such as GISEC also play an important role in taking that message forward and reinforcing the need to prioritise foundational security.

What is the industry still getting wrong about cyber resilience?

We still tend to confuse resilience with prevention. We measure how well we can stop an attack, when the real question is what happens when prevention fails.

Resilience is about limiting impact, not pretending breaches will never happen.

As security architectures evolve, which capabilities are becoming indispensable and which approaches are losing relevance?

The capabilities becoming increasingly important are deep visibility, strong identity, continuous exposure management, data protection and fast response.

They also need to work as one integrated system rather than as isolated controls. What is losing relevance is the belief that a single unified perimeter, or a collection of advanced security products, can protect the enterprise.

Static controls are no longer sufficient in an AI-driven threat environment. The future is not about assembling a bigger security stack that also has AI. It is about fewer disconnected tools, stronger intelligence, greater automation and the ability to continuously see, contextualise and respond across the enterprise.

Where can Teksalah have the greatest impact on the cyber challenges organisations are facing in 2026?

At Teksalah, we believe our greatest impact is in helping enterprises move from buying security tools to building genuine cyber resilience.

As a long-standing systems integrator and security partner, we sit at the intersection of technology innovation, people and business, helping customers focus on what matters most and act on it.

The challenge today is not a lack of security technologies. It is connecting them effectively, continuously reducing exposure and responding faster as threats evolve, including AI-driven attacks.

Our role is to make this practical by helping organisations continuously assess, detect earlier, respond faster, recover better and keep improving. That is where a trusted security partner can create lasting value. 



OPINION

VOICE OF DECEPTION

By Javvad Malik, Lead CISO Advisor, KnowBe4



For decades, the human voice was a cornerstone of trusted and reliable authentication, providing a layer of certainty that digital systems often lacked. While email filters, secure web gateways, and multi-factor authentication (MFA) protected digital perimeters, a quick phone call served as the final trusted check for organisational decision-making. Hearing a familiar voice or an authoritative executive on the line was usually enough to provide the green light to move forward.

But with the evolution of voice phishing, or 'vishing', that call can no longer be trusted.

What was once a niche vector operated by low-grade phone scammers reading scripts from call centres, has transformed into a high-precision, scalable enterprise threat. Driven by breakthroughs in AI voice cloning and social engineering, vishing is now a primary method for breach, extortion, and ransomware deployment across major global organisations.

The AI catalyst

According to Mandiant's M-Trends 2026 report, interactive vishing attacks have climbed to become the second most commonly observed initial infection vector, jumping ahead of email phishing.

The catalyst behind this rise is the availability of AI voice cloning. Threat actors no longer need hours of pristine studio recordings to replicate a target's voice. Modern AI models require as little as 30 seconds of clear audio — easily harvested from public webinars,

podcasts, earnings calls, or video keynotes — to create an ultra-realistic synthetic clone.

When combined with real-time text-to-speech engines and natural language processing, attackers can easily execute dynamic, two-way telephone conversations. Unlike email, where employees have time to inspect headers or hover over links, live phone calls create a sense of urgency where decision-making error rates can increase under pressure. Furthermore, mobile network compression and occasional background noise naturally mask minor AI imperfections, making synthetic voices more likely to sound authentic over the phone.

From helpdesks to the C-suite

Recent high-profile breaches demonstrate that vishing attacks target two distinct pressure points within the enterprise: frontline support desks and executives.

1. Exploiting the helpdesk:

Frontline IT support staff are hired to solve problems quickly, making them ideal targets for manipulative social engineering. In the high-profile MGM Resorts ransomware outbreak, attackers from the ALPHV/BlackCat ransomware group reportedly gathered information from LinkedIn, impersonated an MGM employee, and called the internal IT helpdesk. By tricking support personnel into issuing new credentials and resetting MFA devices, the attackers took down hotel management and casino systems for days, incurring millions in operational losses.

2. Executive deepfakes: When attackers elevate their targets to senior leadership or high-value organisations, the potential payouts increase exponentially. In early 2026, the ShinyHunters group used a targeted vishing campaign against Charter Communications, culminating in the unauthorised access of nearly 42 million customer records. In another instance, fraudsters

“Defending against modern voice attacks requires an evolution in processes, operational culture, and technical guardrails”

generated a voice clone of Italian Defence Minister Guido Crosetto to execute high-urgency calls to prominent business figures, including former Inter Milan owner Massimo Moratti. Claiming emergency funds were needed to release kidnapped journalists in the Middle East, the scam successfully coaxed over €1 million from victims before law enforcement intervened.

Building a vishing-resilient organisation

Traditional endpoint security, antivirus software, and email security gateways are unable to protect organisations from vishing. Defending against modern voice attacks requires an evolution in processes, operational culture, and technical guardrails.

- **Enforce strict verification:**

Under no circumstances should credential resets, MFA re-enrollment, or financial transfers be authorised solely on an inbound phone call. Organisations must implement mandatory callbacks using pre-verified phone numbers listed in an official corporate directory. Additionally, two-person authorisation controls should be enforced for high-risk operations, such as bank transfers or privileged account changes.

- **Harden the service desk:** IT helpdesks must be treated as a critical security risk point. Teams need to transition away from

information-based authentication such as employee ID numbers or birthdates that can easily be scraped online. Mandating video verification with active employee managers or push-notification identity checks via secure enterprise portals prior to resetting access provides a crucial additional layer of protection.

- **Deploy zero-trust technical controls:** By assuming a worst-case scenario is inevitable, technical controls can limit the blast radius of a successful vishing call. Application allowlisting and ringfencing ensure that even if a user is coerced into downloading remote access software, unapproved executables are blocked by default. Furthermore, organisations should replace voice- or SMS-based MFA codes with hardware security keys.
- **Modernise security awareness training:** Most training programmes still focus largely on identifying phishing emails, leaving a major gap in phone-based defence. Organisations must update their training to conduct realistic, vishing simulations that build employee defensive awareness. Crucially, leadership must establish a corporate culture where questioning authority or delaying an urgent request to perform mandatory identity checks is praised rather than penalised.

As generative voice tools become cheaper, faster, and more accessible, AI-driven vishing will continue to escalate in frequency and sophistication. To protect critical infrastructure, sensitive data, and financial assets, security leaders must accept that the human voice can no longer be trusted.

Operational resilience requires pairing zero-trust technical measures with unyielding human verification processes, so your organisation is ready to pause and verify whenever a suspicious request arrives. 🛡️

HOLDING THE LINE

Ajith Surendran, Regional Business Manager – META, Tiger Technology, on moving beyond traditional backup and building continuous protection into the way enterprise data is stored and managed



The theme of this year's GISEC GLOBAL is "Cyber First: The New Digital Order". What does putting cyber first actually demand from business and technology leaders?

It means deciding how much data loss and downtime a system can withstand before choosing the technology, rather than after something breaks. Too often, resilience is added to infrastructure that was designed around cost or speed first.

Cyber-first thinking starts with a straightforward question: if this system went down right now, what would it cost the business financially, legally, or in terms of trust? That answer should determine how quickly data needs to be recoverable and how much interruption is tolerable. The storage and backup architecture should then be built around those requirements, rather than the other way around.

As the security stack continues to evolve, which capabilities are becoming indispensable, and which are losing relevance?

Continuous protection is becoming a baseline rather than an upgrade. Systems that capture every change as it happens, while maintaining a full version history, allow organisations to roll back a bad change or encryption event to the point immediately before it occurred, rather than simply restoring last night's copy.

Automated detection is also becoming essential. The ability to recognise patterns associated with an attack, such as a sudden spike in file changes, and pause replication before the damage spreads can significantly reduce exposure.

What is losing relevance is the idea that periodic, scheduled

“Cyber-first thinking starts with a straightforward question: if this system went down right now, what would it cost the business financially, legally, or in terms of trust?”

backup alone is sufficient protection for data the business genuinely cannot afford to lose.

What role can Tiger Technology play in addressing the cyber challenges emerging in 2026?

At Tiger Technology, we see our greatest impact in helping organisations build stronger data resilience through hybrid cloud. It is not about forcing a choice between on-premises infrastructure and the cloud, but giving organisations the flexibility to place each file where it makes the most sense while managing everything as one system.

As pressure grows from data sovereignty requirements, rapid AI adoption, and large-scale digitisation, that flexibility becomes increasingly important. It allows organisations to keep data protected and recoverable without locking themselves into a single environment.

Helping enterprises gain that unified view and place data selectively, without disrupting what is already running, is where we believe we can make the biggest difference.

What should organisations be investing in now if they want to be resilient by 2030?

Investment should reflect the organisation's risk tolerance. Start by asking what it would cost the business to lose an hour of data or a day of availability, then build the protection model around that answer.

To protect against data loss and corruption, organisations should invest in continuously replicated, versioned copies of their files, allowing them to roll back to the point before an incident occurred.

To recover from a site or system failure, they need a current file-level replica elsewhere, so recovery time reflects what was actually lost rather than the size of the entire dataset.

And where any interruption is unacceptable, high availability becomes critical, with a second system kept live and ready to take over immediately. 



AI delivers enhanced threat protection and increased operational efficiency while securing your AI journey.

Fortinet
Global AI-Driven Cybersecurity Leader.

> Visit our booth in Hall 9

The Fortinet Security Fabric is the industry's most integrated AI-Driven cybersecurity platform, encompassing Secure Networking, Security Operations and Unified SASE solutions that leverage AI for increased threat detection and response and securing the AI journey. The Security Fabric is supported by real-time FortiGuard threat intelligence and an extensive ecosystem of over 3,000 integrations across more than 400 technology partners.

Learn more at fortinet.com

BEYOND THE PERIMETER

Hussam Abu-Rida, Technical Director, MEA, TXOne Networks, examines why OT security must be designed around operational continuity as digital and physical environments become increasingly connected



“As IT, OT, cloud, and connected technologies converge, the architecture must adapt in lockstep”

The theme of this year’s GISEC GLOBAL is “Cyber First: The New Digital Order”. What does putting cyber first actually demand from business and technology leaders?

Cyber comes first when security decisions are made alongside technology and operational decisions, not after systems have already been deployed. In OT, that starts with understanding the environment: what assets you have, how they communicate, which systems are critical, and where the risks sit.

As IT, OT, cloud, and connected technologies converge, the architecture must adapt in lockstep. New connections should be designed around Zero Trust principles, including segmentation and least-privilege access, rather

than assuming anything within the operational network can be trusted.

Procurement must also account for the full asset lifecycle. Many OT environments run legacy systems that cannot easily be patched, replaced, or taken offline, so security must protect them without disrupting production.

Most importantly, OT security cannot be separated from safety, availability, and continuity. The goal is not to prevent every attack, which is unrealistic, but to ensure that a threat that gets through can be contained before it reaches critical operations.

What is making digital trust harder to establish as enterprises become more connected and autonomous?

Trust is becoming harder to maintain because the boundaries between IT, OT, cloud, and physical infrastructure are disappearing. Industrial assets that were historically siloed are

increasingly being connected to wider networks and cloud services.

Nothing can be trusted simply because it authenticated once or because it has always been part of the environment. Verification needs to be continuous and based on the asset, its role, its expected communications, and its behaviour.

AI adds another layer as we move towards more autonomous machine-to-machine decisions. The question is no longer only, “Who are you?” It is also, “What are you allowed to do, on which asset, and under what conditions?”

In OT, Zero Trust must be implemented without compromising worker safety or site productivity. That means combining asset visibility, segmentation, least-privilege access, and continuous verification with a deep understanding of the industrial environment. Trust then becomes contextual and verifiable rather than assumed.

From TXOne Networks’ position in the ecosystem, what role can you play in helping customers respond to the next phase of cyber risk?

Our greatest impact will come from protecting environments where cyber risk can translate directly into operational and physical consequences.

AI is making attacks more scalable and sophisticated, while organisations continue to connect industrial assets, remote operations, IoT devices, and legacy systems to modern IT and cloud environments. The result is an increasingly complex attack surface across OT and critical infrastructure.

We work at the intersection of cybersecurity and operational continuity, giving teams visibility across their assets, identifying abnormal or unauthorised activity, controlling how devices communicate, and enabling rapid containment without interfering with the processes those systems are responsible for. 



Bringing Visibility and Control to GCC Energy Operators

Insights from industrial leaders on securing critical infrastructure through digital transformation



▲ Learn more



AmiViz Returns to GISEC Global with Architecture-First Security for the AI Era

"We are demonstrating architectures and technologies built for the AI era — solutions that help organisations stay ahead of threats that evolve faster than legacy defences."

Ramkumar Balakrishnan,
Chief Executive Officer, AmiViz



VISIT AMIVIZ AT GISEC · HALL 5, B110 · 16-18 SEPT 2026

Meet our technology vendors featured on our stand

Kiteworks

sysdig

PhishRod.
Addressing Human Risk

Abnormal

QuilrAI

CEQUENCE

ACALVIO
AI-POWERED DECEPTION

A10

algosec

ZEROFOX

evertrust

NEOX
NETWORKS