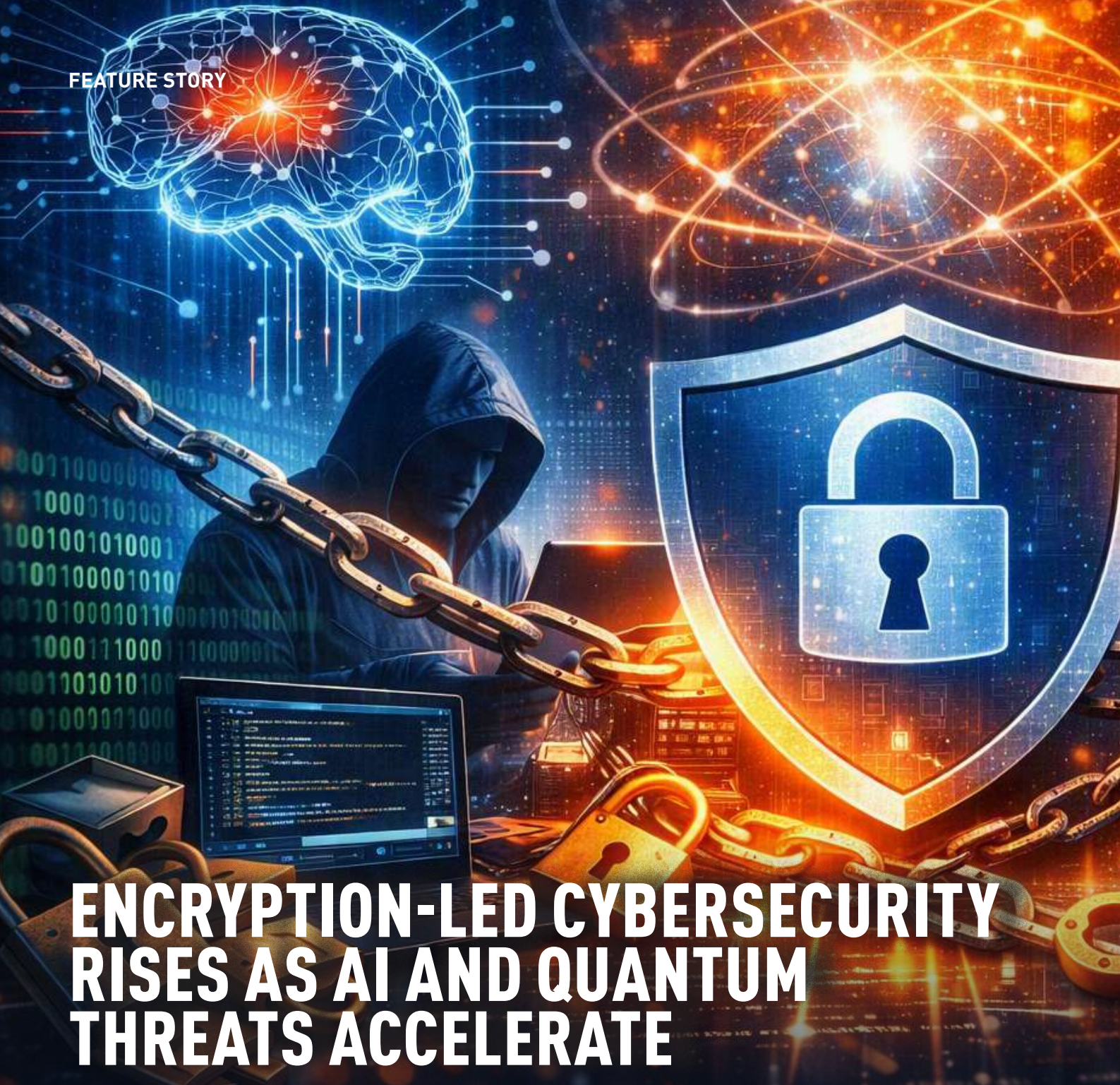




ENCRYPTION-LED CYBERSECURITY RISES AS AI AND QUANTUM THREATS ACCELERATE

As AI-driven automation, quantum disruption and cloud-scale complexity reshape the threat landscape, industry leaders warn that encryption must evolve into an adaptive, intelligence-led foundation for digital resilience. Vendors across the region outline how visibility, crypto-agility and quantum-safe models will define the next era of cybersecurity.

Encryption-led cybersecurity is entering a new era as AI, quantum computing and cloud-scale environments reshape the threat landscape across the Middle East. What was once a defensive control has now become a strategic foundation for national resilience, enterprise trust and digital continuity. As organisations accelerate digital transformation, encryption is no longer a static safeguard but a living, adaptive capability that must evolve at the speed of automation. Across the region, technol-

ogy leaders are rethinking how encryption is deployed, governed and modernised, especially as AI-driven attacks compress exploitation timelines and quantum computing threatens the long-term viability of classical cryptography. The shift is clear: encryption is becoming the backbone of cybersecurity, and the companies shaping this evolution are redefining how data, identities and systems remain secure in an increasingly hostile digital world.

AmiViz CEO Ramkumar B describes this shift

with striking clarity, noting that AI does not break encryption directly but “automates everything around it: stealing credentials, finding misconfigurations, social engineering at machine scale.” For him, the future of encryption-led cybersecurity lies in systems that renew themselves, adapt continuously and monitor their own integrity.

He explains that AmiViz is shaping its strategy across three layers. The first is automation that replaces keys and certificates so quickly that “stolen credentials die in minutes,” eliminating one



of the most common attack paths exploited by AI-driven adversaries. The second is the adoption of quantum-safe encryption running alongside today's algorithms, a hybrid approach designed to defeat "steal-now-decrypt-later attacks" that target long-lived sensitive data. The third is machine learning that detects when encryption is being weakened or tampered with before attackers exploit it.

Ramkumar argues that encryption must become self-aware and self-renewing, capable of anticipating threats rather than merely resisting them. He also highlights the obstacles enterprises face when modernising cryptography, describing cryptographic debt as "encryption hiding in old code, third-party products and industrial systems; like financial debt, the interest compounds quietly." He believes organisations must start with the data

that must remain secret the longest and embed encryption requirements into contracts today.

Looking ahead, he expects three models to define the future: quantum-safe encryption as a compliance requirement, protected computing that allows AI to run on sensitive data inside sealed environments, and key management treated as national infrastructure, where "location means nothing if someone else holds the keys."

Check Point Software Technologies, UAE's Channel Leader, Prashant Menon sees the same urgency but approaches it from a prevention-first perspective. He explains that AI-powered attacks have dramatically shortened the window between vulnerability disclosure and exploitation, making proactive protection essential. Encryption remains critical, but he argues that it must now be combined with AI-driven prevention, real-time



RAMKUMAR B
CEO OF AMIVIZ

threat intelligence and cryptographic agility to remain effective.

"As AI moves from assisting attacks to operating them," he says, "organisations need security controls that protect sensitive data and reduce risk continuously across increasingly complex environments." Menon highlights visibility as one of the biggest obstacles to modernising cryptography, noting that many organisations lack a complete inventory of where encryption is used, which algorithms protect critical data and how keys and certificates are managed.

Without this understanding, modernisation becomes complex and risky. Exposure management, he explains, helps identify cryptographic blind spots, prioritise high-risk assets and build the agility needed to transition securely without disrupting operations. He believes the future of encryption will be defined by cryptographic agility and post-quantum cryptography, with organisations adopting hybrid approaches that support both classical and quantum-safe algorithms.

He warns that the "harvest now, decrypt later" risk is real and growing, urging organisations to identify sensitive encrypted data and develop structured roadmaps toward quantum-safe cryptography. Ultimately, he sees encryption strategies evolving into adaptive systems that reduce risk continuously and integrate seamlessly with broader prevention-led architectures.

Ali AlJuneidi, Regional Sales and Business Development Manager at ESET Middle East frames encryption as part of a multilayered defence strategy rather than a standalone control. He explains that AI is enabling attackers to automate reconnaissance and accelerate cyberattacks, making strong encryption more important than ever.

At ESET, encryption is combined with advanced threat detection, behavioural analysis and continuous monitoring to protect sensitive data while strengthening resilience against both



PRASHANT MENON
CHANNEL LEADER, UAE, CHECK POINT
SOFTWARE TECHNOLOGIES



ALI ALJUNEIDI
REGIONAL SALES AND BUSINESS DEVELOPMENT
MANAGER AT ESET MIDDLE EAST



TONY ZABANEH
DIRECTOR, SYSTEMS ENGINEERING,
MIDDLE EAST SOUTH AT FORTINET

automated and sophisticated attacks.

AlJuneidi notes that many organisations still rely on legacy systems not designed for today's threat landscape, making modernisation challenging. Upgrading encryption requires careful planning to ensure compatibility, effective key management and minimal operational disruption. He advocates a phased approach supported by strong visibility and security management, enabling entities to strengthen protection while maintaining business continuity.

Looking ahead, AlJuneidi expects organisations to adopt cryptographic approaches designed for long-term resilience, including preparations for the post-quantum era. He emphasises that encryption must be integrated into broader security strategies that combine identity protection, endpoint security, continuous monitoring and threat intelligence to safeguard data across increasingly complex IT environments.

Fortinet's Director, Systems Engineering for Middle East South, Tony Zabaneh, views cryptographic agility as the foundation of long-term resilience. He explains that AI is accelerating the speed at

which attackers identify and exploit vulnerabilities, making it essential for encryption to evolve without disrupting business operations. Fortinet enables organisations to discover, manage and replace cryptographic components across networks, cloud, applications and OT environments, allowing them to adopt stronger algorithms and centralise key management as threats evolve.

Zabaneh highlights visibility as the biggest challenge, noting that many organisations lack insight into where cryptography is deployed across their environment. Legacy applications, hard-coded libraries and fragmented architectures make migration complex and resource-intensive. He argues that successful transitions begin with comprehensive cryptographic inventories followed by risk-based prioritisation and phased migration strategies that modernise encryption without disrupting critical operations.

Zabaneh expects post-quantum cryptography to play a critical role in the future but emphasises that adaptable, replaceable cryptography will define long-term resilience. Hybrid cryptographic models combining classical and post-quantum algorithms will ensure compatibility during migration, while technologies such as Quantum Key Distribution will support high-assurance use cases.

Hasanian Alkassab, Security Business Unit Director, GBM describes encryption-led cybersecurity as part of a broader resilience strategy that protects data at rest, in transit and increasingly in use. He explains that GBM strengthens cyber resilience by embedding advanced encryption, identity security, data protection and AI-driven threat detection across its GBM Shield portfolio. Encryption is combined with continuous monitoring, automated response and Zero Trust principles to reduce attack exposure and accelerate threat containment.

Alkassab notes that the biggest challenge is not replacing encryption but modernising it without

disrupting operations. Fragmented environments spanning legacy applications, hybrid infrastructure and multiple cloud platforms make visibility, key management and policy consistency difficult. He advocates phased, risk-based modernisation strategies with centralised governance to enable cryptographic agility and prepare organisations for evolving regulatory requirements.

Looking ahead, Alkassab expects the future of cybersecurity to be defined by post-quantum cryptography, confidential computing and privacy-enhancing technologies such as homomorphic encryption. He argues that organisations must adopt encryption that evolves without major infrastructure changes, relying on centrally managed, identity-aware encryption that protects data across hybrid environments throughout its lifecycle.

Proofpoint's Country Manager for Saudi Arabia, Abdulah Aljandal brings a people-centric perspective to encryption-led cybersecurity. He explains that as AI accelerates phishing, credential theft and exploit-driven attacks, encryption must work alongside intelligence-led security. Proofpoint combines data protection with real-world threat intelligence to identify actively exploited vulnerabilities and prioritise immediate protection across primary attack paths.

"By translating exploit intelligence into protection in minutes," he says, "organisations can significantly reduce exposure while securing people, data and AI-powered workflows." Aljandal highlights fragmented environments as a major obstacle, noting that sensitive data now spans email, cloud applications, collaboration platforms and AI systems, making consistent protection difficult. Proofpoint's research found that 98 percent of UAE organisations struggle with managing multiple security tools, making unified protection and faster investigation increasingly important.

He believes encryption will remain foundational, especially as organisations prepare for



HASANIAN ALKASSAB
SECURITY BUSINESS UNIT DIRECTOR,
GBM