

A futuristic digital landscape with a grid of glowing cubes and circuit patterns. The cubes are arranged in a 3D grid, some of which are illuminated with a warm orange glow, while others are dark. The background is a dark, hazy green with faint circuit lines and glowing particles. The overall aesthetic is high-tech and digital.

Leapfrogging to the future:

Securing an AI-native Middle East

The Middle East has emerged as a global proving ground for emerging technologies, driven by national agendas such as Saudi Vision 2030, the UAE National AI Strategy 2031 and the UAE Digital Government Strategy, Qatar National Vision 2030, and Kuwait Vision 2035. The region is leapfrogging traditional stages of technological development and positioning itself to build next-generation, AI-native national infrastructure, backed by significant capital commitments, including Saudi Arabia's US\$100 billion Project Transcendence initiative and Abu Dhabi's US\$100 billion MGX fund.¹

This ambition creates a unique "leapfrog paradox": the Middle East is advancing faster than many of its global peers, leaving less time to embed security into the foundation. Accelerated digitization, paired with unique geopolitical dynamics, makes the region a prime target for state-sponsored actors and cybercriminal enterprises targeting critical infrastructure. In fact, state-linked hostile operations increased by more than 700% during periods of geopolitical tension in late 2025.²

At the heart of this paradox lies a fundamental shift in how people live and work. 2025 was a watershed year for Artificial Intelligence (AI), as it proliferated in daily life and fundamentally redefined the relationship between personal habits and corporate security. The pace of adoption has been unprecedented, with Generative AI (GenAI) reaching hundreds of millions of users in a short period of time. AI is no longer a niche technical curiosity; it has become an "invisible engine" woven into the fabric of daily life.³

As consumers become accustomed to the speed and efficiency of AI at home, they are increasingly bringing these tools into the workplace, often to bypass slow or broken legacy processes.

This has fueled the rise of Shadow AI: the unauthorized deployment of AI tools by employees without corporate oversight. Recent research highlights that nearly 40% of workers share sensitive corporate data with AI tools without their employer's knowledge.⁴

The risk is evolving beyond simple chat prompts. Employees are now also connecting sophisticated autonomous agents to corporate systems to automate their workloads. These "shadow agents" can create uncontrolled pipelines for sensitive data, leading to significant leaks and compliance violations. On the business side, many functional departments are enabling AI features within existing platforms, such as Customer/Candidate Relationship Management (CRM) and Human Resources (HR) tools, without formal security reviews. This can create massive blind spots in the attack surface.

The Deloitte Tech Trends 2026 report notes that 38% of organizations are already piloting Agentic AI.⁵ This number will surge as organizations look to redesign entire processes for an AI-native environment rather than simply trying to automate legacy workflows. If organizations do not evolve at the same pace, Shadow AI could become an unmanageable systemic risk.

Merely blocking these tools is unlikely to be sufficient; employees may continue to seek faster and more effective ways of working when approved tools do not meet their needs. Organizations should build a security-conscious workforce that understands the risks of AI, while providing enterprise tools that match the speed of consumer applications. Moreover, instead of viewing AI as simply software, companies must start treating AI agents as a new class of digital workers that require the same oversight and accountability as any human hire.

Shadow AI could become an unmanageable systemic risk

In practice, AI is a double-edged sword; it is reducing the barriers to sophisticated attacks while serving as a force multiplier for defenders.

Frontier AI models are significantly accelerating the discovery and analysis of software vulnerabilities. Flaws that evaded manual review for decades are now being identified, validated, and chained into exploits at machine speed.

In this environment, Deloitte's Future of Cyber report found that 40% of organizations experienced between six and ten publicly disclosed breaches in the past year.⁶ In response, organizations are moving beyond basic posture management to deploy autonomous "red agents" and AI-driven patch synthesis to close exposure windows before they can be weaponized.

This acceleration of digital risk is most dangerous where the virtual world meets the physical. The convergence of Information Technology (IT) and Operational Technology (OT) has created concentrated infrastructure fragility whereby a single digital breach can spread across connected layers to cause real-world service outages. Currently, over 50% of cybersecurity incidents involve OT.⁷

In the Middle East, threats blocked from email clients on industrial computers are 1.8 times higher than the global average,⁸ highlighting the massive growth in "machine identities," the automated keys used by bots, sensors, and AI agents, which now outnumber human accounts by a ratio of 45 to 1, creating millions of poorly governed entry points for attackers.⁹

Looking beyond AI, organizations must confront the "new math" of quantum decryption, an unprecedented computational power capable of breaking the mathematical algorithms that currently secure the global digital economy. While full-scale quantum machines are not yet commercially available, as per Deloitte research, cryptographically relevant quantum computers (CRQCs) could break current encryption methods as soon as the 2030s. The transition to quantum-resistant systems could take a decade, creating a dangerous gap. Attackers are already engaging in a "Harvest Now, Decrypt Later" (HNDL) strategy, posing an immediate risk to data with long-term sensitivity.

Organizations should therefore begin creating a cryptographic inventory to transition toward Post-Quantum Cryptography (PQC). By establishing a "crypto-agile" operating model, companies can ensure the seamless interchange of algorithms as new threats emerge.

Encouragingly, regional regulators are moving from protecting only government assets to making cybersecurity a baseline requirement for the entire economy. In Saudi Arabia, the National Cybersecurity Authority's (NCA's) NCNICC-1:2025 regulations now mandate cybersecurity controls for private sector entities. As the private sector's contribution to gross domestic product (GDP) targets 65%, its digital resilience becomes a national priority. However, a governance gap remains; while the region leads in data sovereignty, 62% of organizations in Saudi Arabia still rely on manual processes for compliance evidence.

To survive this landscape, organizations must move away from a "patchwork" of disparate tools toward a unified data security platform. Zero Trust must become the architectural foundation, treating every user, sensor, and AI agent as a verified entity.

Ultimately, organizations must transition from seeing cybersecurity as a "cost center" to a strategic differentiator that enables business agility and builds customer trust. As per Deloitte's Global Future of Cyber report, 58% of global organizations now expect cybersecurity spending to be integrated directly into other departmental budgets.

Chief information security officers (CISOs) must also foster a culture of "AI Fluency," treating AI agents as "digital employees" that require formal onboarding, dynamic privilege management, and continuous auditing. Moreover, they should move toward "Policy-as-Code" and automated compliance monitoring to transform their infrastructure investments into a true governance advantage.

As autonomous discovery collapses the gap between vulnerability emergence and exploit generation, traditional periodic scanning is no longer sufficient. CISOs must transition to continuous, AI-driven runtime validation and reachability analysis, embedding automated remediation directly into deployment pipelines.

Accelerated digitization, paired with unique geopolitical dynamics, makes the region a prime target for state-sponsored actors and cybercriminal enterprises targeting critical infrastructure

The modern CISO must be a business executive that translates complex regulations into the "language of risk" for the board. The path forward is "cyber resilience-by-design"—a strategy that assumes a breach is always imminent, rooted in Zero Trust Architecture, and utilizes AI-powered autonomous defense to close the window of opportunity before it's too late. Organizations that thrive will be those that embed security into their operational DNA rather than retrofitting it as an afterthought. ●

By **Tariq Ajmal**, Partner, Cyber Leader, Deloitte Middle East

Endnotes

1. Deloitte, Technology Trends 2026: The Future of the Digital Landscape in MENA and Beyond; Strategic Resilience in a Fractured Digital Landscape: Middle Eastern Cyber Risk Projections and Sectoral Mitigation Strategies for 2025–2026; and [hai_ai_index_report_2025.pdf](#).
2. Cyfirma, Regional Stability on Shaky Ground: Cyber Threat Escalation in the Middle East; Strategic Resilience in a Fractured Digital Landscape: Middle Eastern Cyber Risk Projections and Sectoral Mitigation Strategies for 2025–2026 and Cobalt.io, The Unseen War: Cyber Warfare in the Shadow of Global Conflicts.
3. Deloitte, Tech Trends 2026; Deloitte Tech Trends 2025: A Life Sciences & Healthcare Perspective; and The New Math: Solving Cryptography in an Age of Quantum.
4. Deloitte, The AI Dilemma: Securing and Leveraging AI for Cyber Defense.
5. Deloitte, Tech Trends 2026. Strategic Analysis of Global Cyber Resilience and the Quantum Transition: Navigating the 2025–2030 Technological Horizon and Deloitte, GovTech Trends 2026.
6. Deloitte, Future of Cyber/Global Future of Cyber.
7. Fabritry, Internet of Things (IoT) Security: A Challenge for 2026, citing Deepstrike/IBM X-Force data.
8. Kaspersky ICS CERT, Threat Landscape for Industrial Automation Systems: Middle East, Q2 2025; Strategic Resilience in a Fractured Digital Landscape: Middle Eastern Cyber Risk Projections and Sectoral Mitigation Strategies for 2025–2026.
9. Future-Proofing IAM: Deloitte & CyberArk on Quantum-Safe Strategies; Strategic Analysis of Global Cyber Resilience and the Quantum Transition: Navigating the 2025–2030 Technological Horizon.