The Cyber-Resilience Playbook:
Securing the Future of Business and Innovation

Sponsored by

HELP AG
an e& enterprise company

The Security Powerhouse of **e& enterprise**

July 2025

Table of Contents

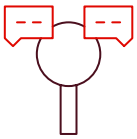
Author:
Shilpi Handa– Associate Research Director, IDC, META

Executive Summary

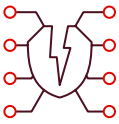
In an era defined by AI-driven attacks, regulatory pressure, and increasing digital complexity, cyber resilience has become a strategic mandate for every organisation. This playbook delivers a clear road map for building future-proof cybersecurity – one that goes beyond defence to enable growth, innovation, and trust.

Drawing on insights from IDC and the real-world experience of e& enterprise and Help AG, this guide explores:

The evolving Middle East threat landscape



Practical steps to fortify detection, response, and governance



Key technologies and trends reshaping cyber defence (AI, identity security, Cloud-Native Application Protection Platform, zero trust, quantum readiness)

The critical role of strategic partnerships in achieving cyber maturity

Whether you are modernising your Security Operations Center, mitigating new AI-driven risks, or aligning with national cybersecurity strategies, this playbook empowers you to act decisively – and lead with confidence.

Introduction

This playbook explores how cybersecurity is transforming from a defensive function into a driver of innovation, trust, and sustainable growth. It outlines the key forces shaping today's threat landscape, the critical capabilities needed to respond, and the frameworks that help organisations align security with business resilience.

The content is structured as follows:

1 Understanding the Cyber Threat Landscape

As digital transformation accelerates, so does the threat landscape. From ransomware-as-a-service to AI-driven phishing, modern attacks are faster, smarter, and more targeted. Understanding the anatomy of these threats is the first step toward building proactive, intelligence-led cyber resilience.

2 Recent Threats and Regulatory Impact

Heightened regulatory enforcement, combined with the growing complexity of threats, is reshaping cybersecurity strategy. Organisations must now align with evolving frameworks — from national cyber mandates to industry-specific compliance — while maintaining agility and resilience across their operations.

3 Building a Robust Cyber Defence

True cyber defense is no longer static — it must be adaptive, integrated, and intelligence-driven. This section explores how advanced detection capabilities, threat-informed operations, Zero Trust architectures, and AI-powered tools come together to create dynamic security environments that can anticipate, endure, and outmaneuver today's evolving threats.

4 About Help AG

Discover how Help AG (the region's leading cybersecurity provider) combines deep local insight, global innovation, and cutting-edge security operations to empower governments and enterprises with real-time resilience.

Understanding the Threat Landscape
Cyber Resilience Is Imperative

The New Face of Cyber Threats

Cyberattacks are no longer opportunistic — they are precision-engineered. From ransomware as a service to deepfake-powered phishing, today's adversaries leverage automation, AI, and advanced social engineering to bypass traditional defences and deliver maximum impact with minimal effort.

Threats like cryptojacking, supply chain intrusions, Distributed Denial of Service (DDoS) campaigns, and insider compromise now operate in parallel, targeting not just infrastructure, but trust, continuity, and control. The convergence of these risks demands more than just detection — it requires anticipatory defence built on intelligence and adaptability.

The Middle East continues to be a high-value target, with the UAE ranked among the top 25 most attacked countries globally — reinforcing the urgent need for regionally aligned, intelligence-led cyber strategies.

Resilience Is the New Cyber Strategy

Cyber resilience is the capacity to operate securely and recover quickly — not just in spite of attacks, but through them. It shifts the focus from protecting static assets to ensuring dynamic, continuous operations — even under duress.

While traditional cybersecurity emphasised perimeter defence and system integrity, resilience expands the scope to availability, recovery, and agility. As technologies like AI and cloud scale across enterprises, resilience ensures that your security posture evolves with the threat — not after it.

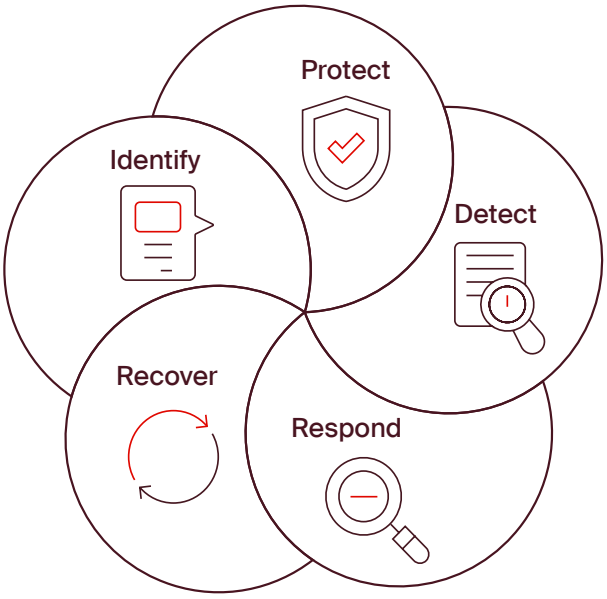
At its core, cyber resilience is not just a framework — it's a business enabler that ensures trust, continuity, and competitiveness in a world where disruption is the norm.

Strategic Transition

Cyber resilience is not achieved through technology alone — it requires a structured, adaptable framework that aligns security priorities with business outcomes. Among the most widely adopted models, the National Institute of Standards and Technology Cybersecurity Framework 2.0 offers a clear, functional structure to help organisations build, evaluate, and evolve their cyber strategies.

While the five core pillars — Identify, Protect, Detect, Respond, and Recover — remain foundational, the way they are applied must reflect today's dynamic threat landscape, increasing regulatory demands, and the shift toward proactive defence. Frameworks are only as valuable as the intelligence, agility, and execution layered into them.

The NIST Cybersecurity Framework 2.0



Source: NIST

There Emergence of GenAI Has Caused an Alarming Spike in the Threat Landscape

> The UAE public sector alone endures around 50,000 cyberattack attempts daily.
> – Mohammed Al Kuwaiti, Head of Cybersecurity for the UAE Government, at the GPRC Summit in Dubai

> Cryptominers allegedly made $100,00 from mining at an Airbnb for three week – guests ran up a $1,500 electricity bill.

> Company worker in Hong Kong pays out £20m in deepfake video call scam.

> Pwn2Own 2024: Tesla Hacks, Dozens of Zero-Days in Electrical Vehicles.

> Anonymous Arabia, a notorious ransomware group, allegedly targeted a website belonging to one of the UAE's official public services and an authority that manages water and electricity supply in Abu Dhabi.

> A Saudi Arabian water corporation was targeted by a DDoS attack in April 2024. Furthermore, one of the country's top government ministries reportedly suffered a massive data breach, exposing the personal information of more than 1.4 million employees affiliated with the ministry.

> Help AG's latest state-of-the-market report highlights a significant rise in DDoS activity across the UAE in 2024, with 373,429 incidents recorded, an 862% increase compared to 2019. Some attacks persisted for over 35 days, reflecting not only the scale but also the increasing complexity and endurance of threats facing the region's digital infrastructure.

Source: Various media sources

From Enterprise to Nation: Securing What Matters Most

Across the Middle East, cybersecurity has become a national priority — embedded into economic policy, digital transformation road maps, and regulatory reform. Governments are taking decisive action: launching cyber strategies, regulating digital infrastructure, and investing in sovereign capabilities to protect both institutions and citizens.

But national resilience cannot be achieved by policy alone. It requires deep collaboration between public and private sectors — where enterprises align not just to compliance, but to the shared vision of a secure, thriving digital society.

Cybersecurity, in this context, is not only a risk response; it's an engine for confidence, innovation, and continuity — from the boardroom to the country level.

Regional Momentum in Action

The UAE has introduced national frameworks like the UAE Cybersecurity Strategy and Digital Government Regulations, focusing on cloud security, data protection, and sectoral resilience.

Saudi Arabia continues to elevate its National Cybersecurity Authority (NCA), with clear compliance mandates and proactive oversight — accelerating resilience across sectors including finance, energy, and healthcare.

Both nations are investing in cyber capacity building, localised regulations, and public-private threat intelligence exchange to strengthen readiness and response.

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

- National Cyber Security Strategy
- New policies around cybersecurity and AI to be issued by mid-2025

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

- Dubai Cyber Security Strategy
- PKI Policy, ICS Standard, IoT Security Standard, ISR Audit, CSP Security Standard, Dubai AI Security Policy
- Dubai Cyber Innovation Park
- Cyber Security Competency Framework (Qudraat)
- DESC Cyber Force Framework

These efforts have been recognised globally, with the UAE achieving a top ranking in the International Telecommunication Union's 2024 Global Cybersecurity Index.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

- Essential Cybersecurity Controls (ECC)
- Critical Systems Cybersecurity Controls (CSCC)
- MSOC Licensing

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

- Saudi Data Privacy Law
- AI Ethics (draft)

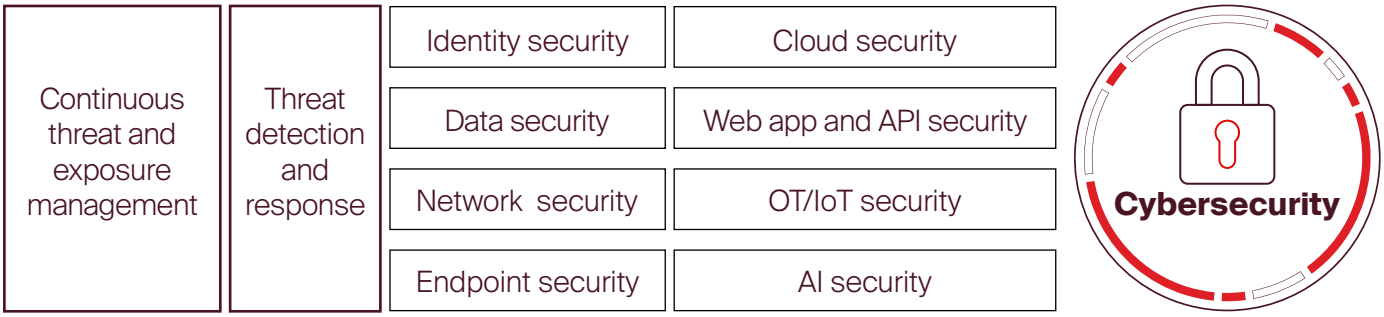
Saudi Arabia has earned the second-ranking globally in the Global Cybersecurity Index (GCI) by the International Telecommunications Union (ITU)

Source: Various government websites

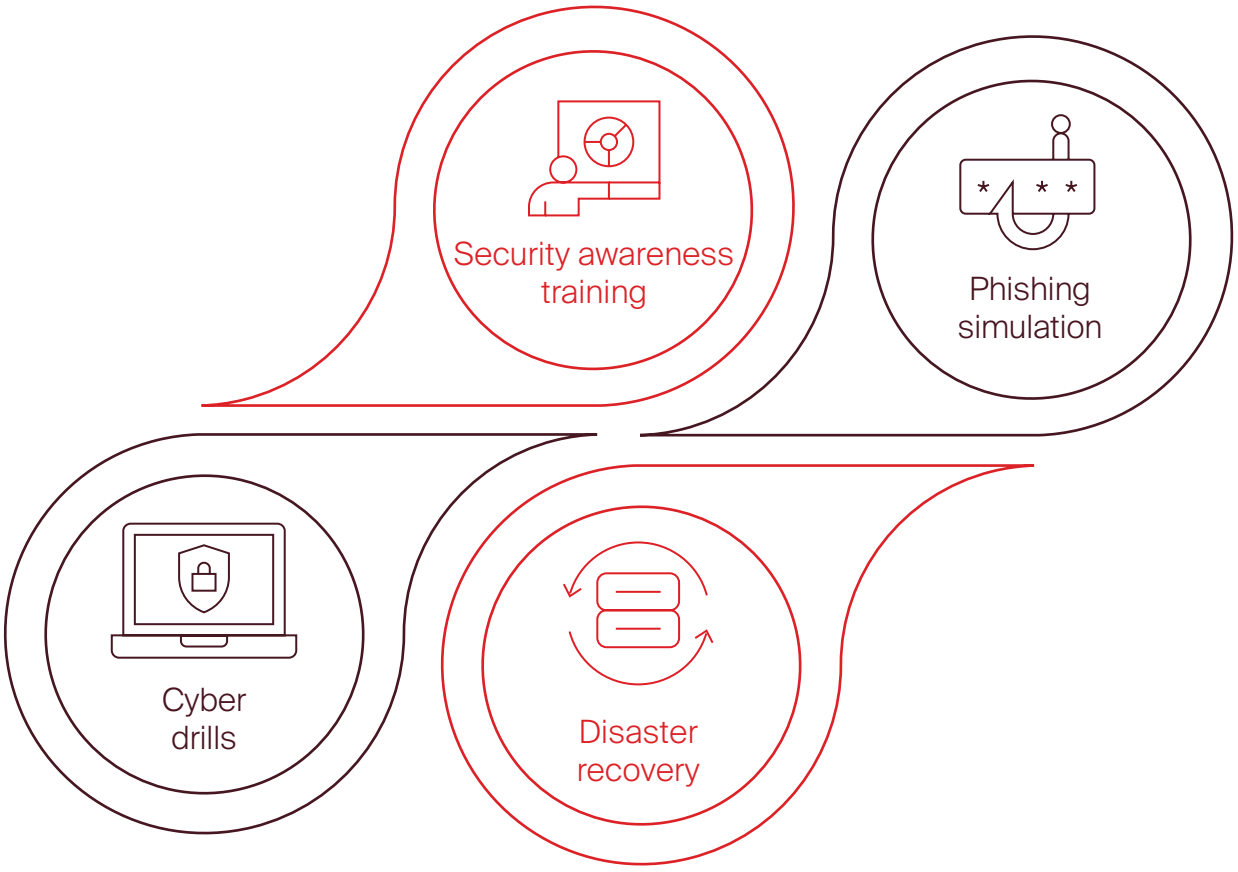
Building a Robust Cyber-Defence Strategy

Cybersecurity: A Continuous Journey

Beyond regulatory compliance, technology leaders, board members, and senior executives in the Middle East now recognise the critical importance of cybersecurity and are actively involved in shaping their organisations' cyber strategies. This increased involvement reflects a broader understanding that cybersecurity is not just a compliance issue but a fundamental aspect of protecting the organisation's assets, reputation, and overall business continuity.



While detection tools are essential, proactive security training remains one of the most effective ways to prevent cyberattacks. Regular training programs equip employees to recognise and respond appropriately to threats such as phishing and social engineering.



Strategic Partnerships: Elevating Cyber Defence

Organisations that partner with experienced security service providers achieve better detection and response rates.

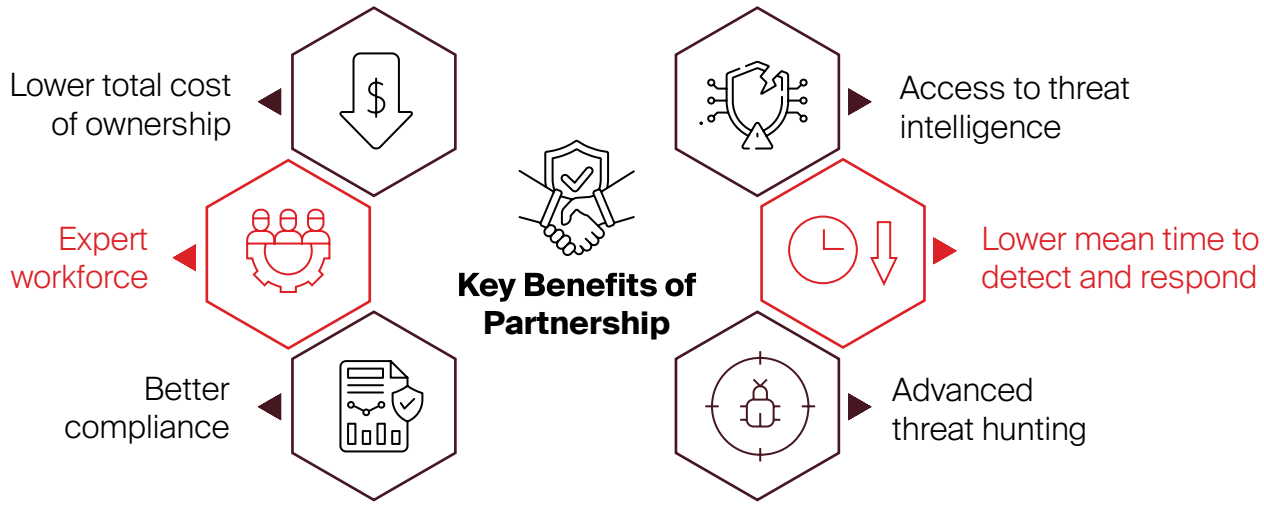
In today's hyperconnected threat environment, cybersecurity is no longer a support function — it's a strategic enabler of trust, innovation, and resilience. Choosing the right cybersecurity partner is not just critical for protection — it defines an organisation's ability to grow, adapt, and lead securely in a digital-first economy.

The right partner brings more than technologies; they deliver continuous innovation, predictive threat intelligence, agile incident response, and the strategic foresight needed to stay ahead of adversaries This allows enterprises to fully focus on their business priorities with clarity and confidence.

Strategic Value and Why It Matters

- **Agile Threat Intelligence:** Access to real-time, predictive threat insights, globally and regionally.
- **Proactive Detection and Response:** Lower mean time to detect (MTTD) and mean time to respond (MTTR) — minimising impact.
- **Resilience by Design:** Architect systems and processes for continuity — not just defence.
- **Risk-Aligned Compliance:** Navigate global and national regulations without slowing innovation.
- **Operational Scalability:** Expand securely across geographies, platforms, and hybrid environments.
- **Cost and Resource Optimisation:** Drive better ROI by integrating expertise, automation, and threat-informed services.

Choosing the right cybersecurity partner is no longer just an operational decision — it's a strategic imperative. In today's threat landscape, where speed, sophistication, and automation define cyberattacks, only a partner with proven expertise, regional depth, and scalable innovation can ensure true resilience. The right choice empowers your organisation to not just defend, but to predict, prevent, and thrive — securing your critical assets while accelerating your digital future.



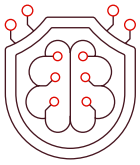
Securing AI, Data, and Identities Across the Digital Ecosystem

Leverage AI and Identity Security to Stay Ahead of the Curve

Artificial intelligence(AI) is now embedded across applications, systems, and workflows — used by humans, machines, and autonomous agents. But with AI comes new layers of cyber risk: unauthorised access, data leakage, decision manipulation, and operational disruption.

To build digital trust in an AI-powered world, organisations must move beyond securing traditional infrastructure — and instead secure the entire AI lifecycle: the data fuelling AI, the models making decisions, the apps and Application Programming Interfaces (APIs) delivering AI services, and the human and machine identities interacting with them.

The Key Pillars of Securing AI and Digital Trust

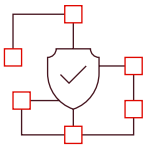


Data Protection Across the AI Lifecycle

- Secure the training data feeding AI models.
- Protect input/output flows to prevent manipulation or leakage.
- Deploy data loss prevention (DLP) and encryption at every layer.

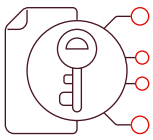
Application and API Security

- Secure apps embedding AI capabilities against vulnerabilities.
- Harden APIs — the backbone of AI integration — to prevent injection and abuse attacks.
- Implement continuous API security testing and anomaly monitoring.



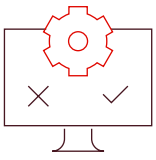
AI Infrastructure and Model Security

- Safeguard AI models from model extraction, poisoning attacks, and adversarial inputs.
- Deploy runtime protection for AI workloads across cloud, hybrid, and edge.



Identity and Access Governance

- Enforce strong identity management for users, services, and machines interacting with AI systems.
- Adopt zero trust architectures to validate every access request dynamically.



Continuous Monitoring and Assessment

- Monitor AI-driven environments for anomalies in behaviour, access, and decision outputs.
- Conduct regular risk assessments to identify emerging vulnerabilities across the AI stack.

Governance, Ethics, and Policy Alignment

- Implement robust AI governance frameworks to ensure transparency, fairness, and compliance.
- Continuously update policies to address evolving AI threats and regulations.

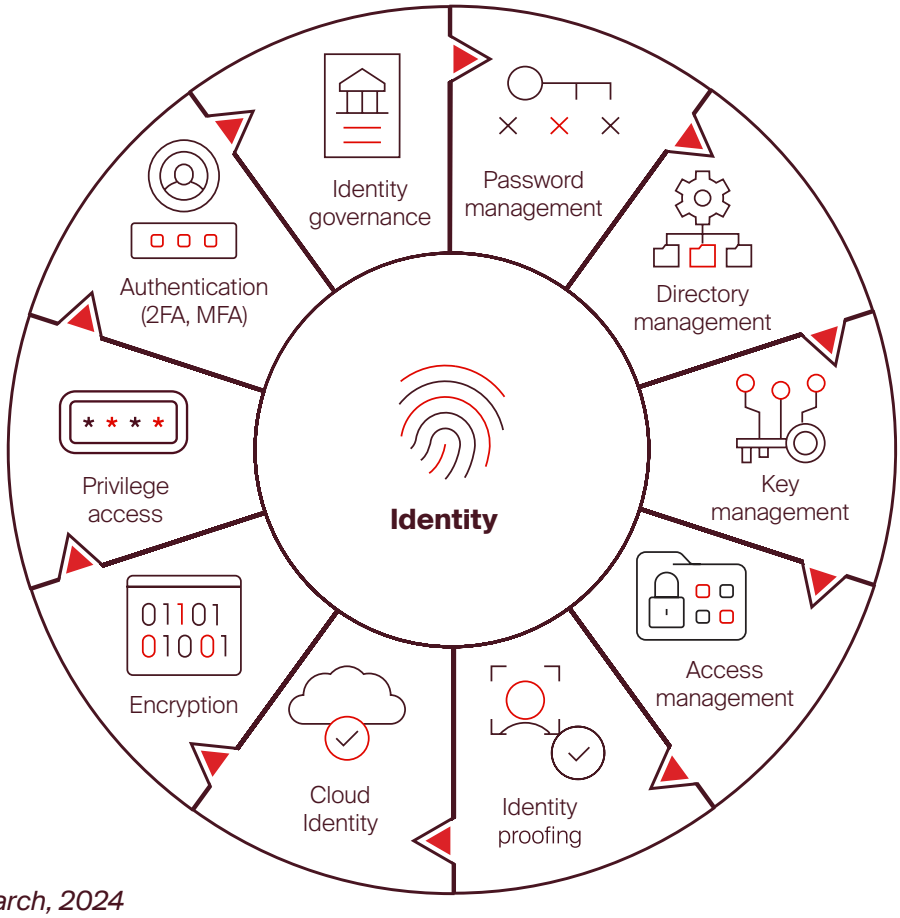
Securing AI is not about protecting a tool — it's about safeguarding the future of decision-making, trust, and digital business. Organisations that embed security across the full AI and data lifecycle will not only defend against new threats — they will lead with resilience, innovation, and sustainable growth.

Securing the New Digital Perimeter: Identity and Cloud Security

As enterprises accelerate their cloud adoption and hybrid operations, the traditional network perimeter has dissolved. In this new digital reality, identity and cloud infrastructure have become the primary security perimeters.

Protecting user identities, machine credentials, cloud configurations, and application access points is now essential to ensuring trust, continuity, and compliance across modern digital ecosystems.

Identity Security as the New Frontline



Source: IDC research, 2024

Key Focus Areas

- **Identity Governance:** Define, control, and audit who has access to what.
- **Authentication and Privileged Access Management (PAM):** Strengthen authentication beyond passwords; restrict privilege escalation.
- **Encryption and Identity Proofing:** Safeguard sensitive data at rest and in motion.
- **Directory Management and Key Management:** Protect core identity services and cryptographic keys across hybrid environments.

A comprehensive identity fabric approach ensures that user, device, and machine identities are continuously verified and protected across diverse cloud and on-premises ecosystems.

Addressing Cloud Security Complexity

Key Focus Areas

- **Misconfigurations and Unauthorised Access:** The top causes of cloud breaches.
- **Identity and Access Management (IAM) and AI-Powered Detection:** Prevent unauthorised access and monitor for anomalous behaviours.
- **Cloud-Native Application Protection Platforms (CNAPPs):** Deliver unified, automated protection — integrating workload security, configuration management, threat detection, and compliance across multicloud environments.

Cloud security is no longer just about perimeter defence — it's about embedding security into every layer of the application, identity, and infrastructure stack.

As identities and cloud platforms become the new critical control points, securing them holistically is not optional — it's the foundation of resilience.

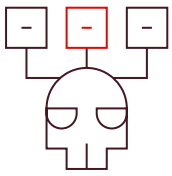
Organisations that treat identity and cloud security as integrated, continuous capabilities — not siloed projects — will be better positioned to manage risk, achieve compliance, and unlock secure innovation at scale.

Future-Proof Your Cyber-Defence Strategy

Stay Proactive, Stay Secure

As cyber risks evolve — from AI-manipulated threats to quantum decryption capabilities — organisations must move beyond reactive security.

Future-proofing cybersecurity means anticipating tomorrow's risks today, embedding resilience at every layer of operations, and evolving faster than adversaries can innovate.

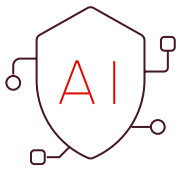


Deepfake Threats

AI-powered content manipulation is escalating. Organisations must deploy deepfake detection tools, train high-risk decision-makers, and integrate verification mechanisms into critical communications and media workflows.

Quantum Threats

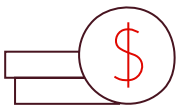
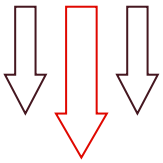
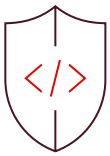
Quantum computing will eventually render today's encryption obsolete. Organisations must proactively inventory cryptographic assets, prioritise post-quantum migration for critical systems, and partner with quantum-resilient technology providers.



AI Security

Securing AI means safeguarding models, data, and decision-making pipelines. Robust governance frameworks — combining regular audits, real-time monitoring, AI-specific controls, and data integrity checks — are critical to sustain trust in AI-driven ecosystems.

A long-term cybersecurity plan should focus on:

 Optimising Security Operations	 Investing in Intelligent Security Tools	 Removing Innovation Barriers	 Developing Resilient Security Architectures	 Partnering for Predictive Cyber Defence
Automate, streamline, and threat-align internal workflows.	Prioritise AI-driven, adaptive technologies.	Align security to enable — not obstruct — digital transformation.	Embed resilience into cloud, application, and identity ecosystems.	Work with strategic partners that enable foresight, not just protection.

Action Plan: Advancing Your Cyber-Resilience Journey

In a rapidly evolving cyber landscape, resilience is non-negotiable. Building a defence that adapts to tomorrow's threats will empower organisations to innovate fearlessly.

Don't wait — start building your cyber resilience today.

1

Prioritise Comprehensive Risk Assessments:
Continuously map critical assets, vulnerabilities, and evolving threat exposures.

2

Establish a Proactive Incident Response Strategy:
Prepare for the inevitable — define clear, rapid response protocols to minimise damage.

3

Invest in Advanced Security Technologies:
Deploy Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Identity and Access Management (IAM) solutions to strengthen threat detection and response capabilities.

4

Foster a Culture of Security Awareness:
Turn every employee into a line of defence with continuous awareness and behaviour change.

5

Strengthen Strategic Partnerships:
Align with cybersecurity experts who drive agility, innovation, and intelligence at scale.

6

Adapt, Learn, and Evolve Relentlessly:
Integrate threat intelligence, risk insights, and regulatory changes into daily operations.

Source: IDC research, 2024

"The biggest mistake organisations can make is thinking quantum security is just another software update."

Nicolai Solling
Cyber Advisor at Help AG, an e& enterprise company

Cybersphere Nexus from Help AG

Our Flagship Initiative aimed at revolutionizing cybersecurity focusing on securing AI and Post Quantum Cyber.

End-to-end Zero Trust Solutions

- Intelligent SOC Automation
- Identity Fabric Immunity
- Securing Cloud & Modern Apps
- Secure Access Service Edge (SASE)
- OT & IoT Security
- Data Security & Privacy

Cybersecurity Solutions

- Managed Security Services
- DDoS Protection & Assurance Services
- Offensive Cybersecurity
- Digital Forensics & Incident Response
- Cyber Trust Advisory & Consulting
- Continuous Threat Exposure Management (CTEM)

About Help AG an e& enterprise company

Help AG, an e& enterprise company, is a recognised leader in next-generation cybersecurity technology and innovation. It combines strategic consulting with bespoke information security solutions and services to empower governments and enterprises across the Middle East and Africa to secure their digital transformation journey while maintaining a competitive edge.

Leveraging e&'s robust technology portfolio, vast market reach, and deep expertise, Help AG enables organisations in the region with the tools and capabilities needed to confidently navigate the ever-changing cybersecurity landscape. Help AG's advanced security offerings, coupled with a commitment to cybersecurity innovation and compliance, ensure that its customers benefit from unparalleled resilience and agility in an increasingly digital world.

As a trusted partner to both governments and enterprises, Help AG is dedicated to fostering a secure and compliant digital environment, helping its clients thrive in their digital endeavours.

To learn more about Help AG, please visit www.helpag.com.

About e& enterprise

e& enterprise is a digital transformation leader supporting governments and large-scale organisations in building and scaling their digital core.

Through optimising operations, enhancing customer engagement, and data-driven decision-making, we enable seamless, sustainable, and secure transitions into the evolving digital world.

Currently operating in the UAE, KSA, Egypt, Turkey and Oman, e& enterprise brings cutting-edge digital scalable solutions designed to deliver tangible business value and address the unique challenges faced by organisations and executives across industries.

With a proven track record as a trusted digital transformation partner, technical expertise, and the ability to deploy and manage complex solutions, e& enterprise provides collaborative tailored solutions that empower customers to navigate their end-to-end digital transformation journey.

To learn more about e& enterprise, visit our site or reach out:

enterprise@eand.com e& enterprise www.eandenterprise.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.