onsecurity

What are Security Leaders Prioritising in 2025?

Balancing innovation and risk: how security leaders are building cyber resilience while enabling digital transformation in an era of AI-enhanced threats

Current State of Affairs

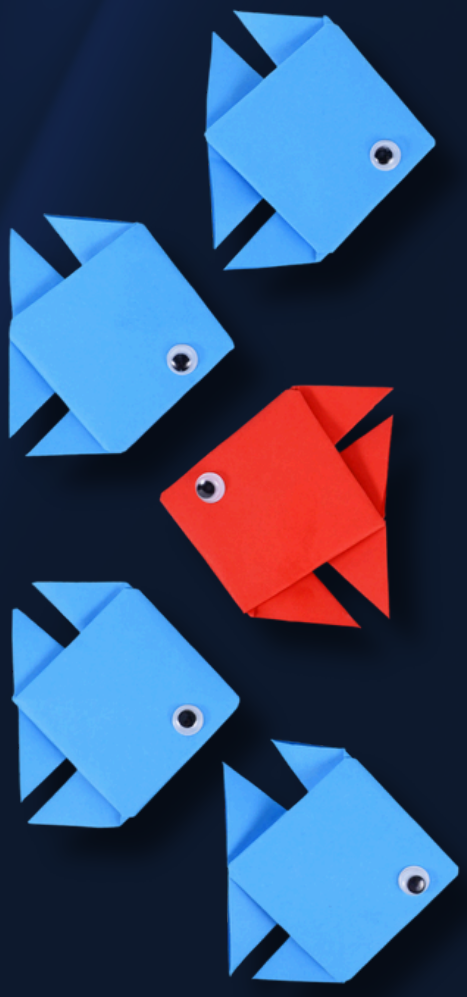
It's no secret that security leaders in 2025 are confronting **an unprecedented level of cybersecurity challenges across multiple fronts**, defined by their unprecedented complexity and pressure.

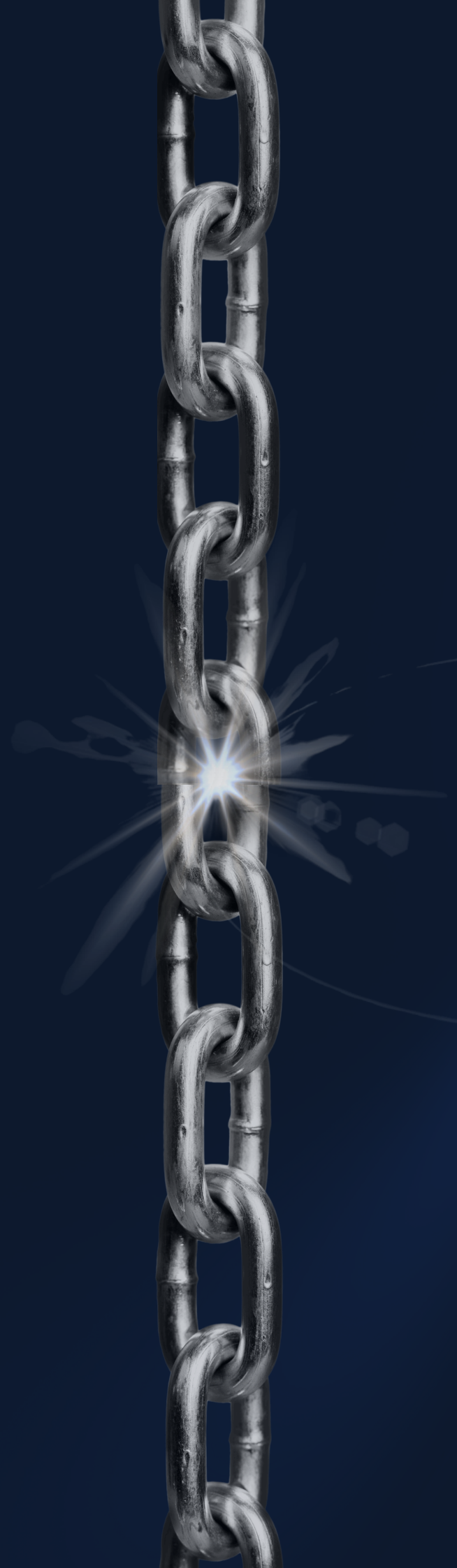
Whether it's striving to meet new and enforceable regulatory practices, working to fortify supply chain practices, or trying to get ahead of AI threats, **the cybersecurity world finds itself in a period of both immense pressure and, more excitingly, infinite potential.**

With security leaders at the beating heart of this exciting new chapter, they must **both defend against current threats whilst enabling digital transformation initiatives.**

They're under pressure to demonstrate measurable security outcomes, optimise programme performance, and build organisational resilience- **all within constrained budgets and regulatory frameworks** that continue to acceleratingly change.

This paper will outline **five of the most significant cybersecurity measures prioritised by leaders in 2025**, and how they have come to the forefront of proactive cybersecurity to **revolutionise existing approaches to threat defence.**





Supply Chain Resilience

Supply chain resilience has become **a critical focus for organisational leaders** in 2025 due to rising threats in interconnected digital environments.

54% Of enterprises cited **supply chain risks** as **the main barrier** to cyber resilience*

This figure underscores the significant risks that poor supply chain resilience poses to an organisation's security, with cybercriminals increasingly targeting third-party vendors.

Recent complex incidents highlight how a single compromised supplier can disrupt multiple organisations, reshaping the way IT security leaders approach risk management.

In response, regulatory pressures for stricter vendor assessments have intensified, while the rapid adoption of cloud services and AI have most prominently expanded the attack surface.

Proactive security leaders are investing in advanced visibility tools, zero-trust architectures, and robust vendor risk management frameworks to ensure survival in 2025.

**Global Cybersecurity Outlook 2025, World Economic Forum. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/*

onsecurity

Continuous Security Assurance

Continuous security assurance has emerged as an indisputable priority for organisational resilience, accelerated by the **escalating sophistication of cyber threats** and increasingly **complex digital risks in 2025.**

88% Of surveyed professionals were dissatisfied with their current tools for cyber risk oversight in 2024.*

Modern security frameworks demand **persistent monitoring, adaptive control validation, and immediate threat response capabilities** that evolve alongside emerging attack vectors.

The implementation of continuous security assurance enables organisations to maintain visibility across their entire attack surface whilst simultaneously addressing the challenge of securing **increasingly complex hybrid environments comprising cloud services, IoT devices, and interconnected third-party systems.**

This threat-conscious approach **transforms security from a reactive compliance exercise into a strategic business enabler**, ensuring that security controls remain effective against both known and zero-day threats whilst providing apt agility for businesses during this uncertain time.

Haynes, Why continuous controls monitoring should be a budget priority for 2025: Quod Orbis 2024

onsecurity

Automated Remediation Workflows and Integrations

Within testing, automation refers to the use of AI and automated solutions to streamline and speed up penetration testing activities.

Using scanners, **automated tools can identify low-hanging fruit findings that do not require human logic,** in turn speeding up reporting by allowing human testers to focus on more complex and business-logic-based findings.

Although manual testing remains the most reliable and comprehensive approach-thanks to human expertise and contextual intelligence- businesses can strengthen their security posture by complementing it with automated solutions. This combination **enhances speed, accuracy, and efficiency, enabling more continuous protection against evolving threats.**

To improve workflows and save valuable time in 2025, security leaders and DevSecOps teams are increasingly searching for **tooling that integrates seamlessly with their existing tech stack.**

onsecurity

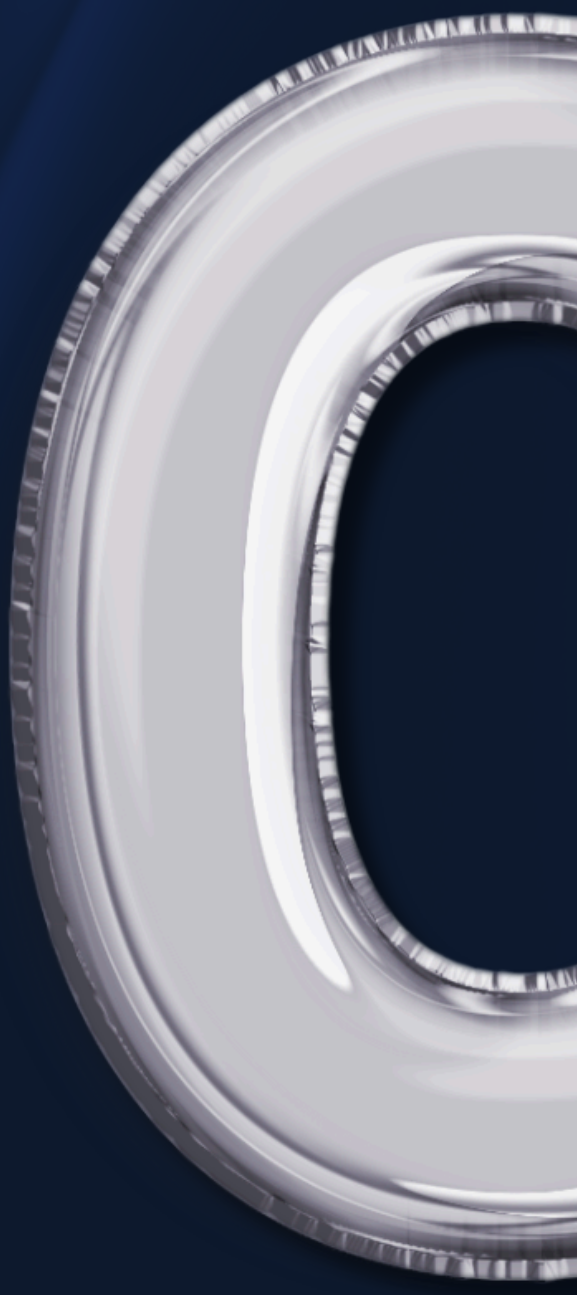
Zero-Trust Architecture Implementation

Grounded in the principle of 'never trust, always verify,' zero-trust architecture assumes no user or device is inherently trusted. Every access request must be continuously verified, wherever it originates, to reduce the attack surface and prevent lateral movement.

Remote-work policies continue to be used globally, with a large amount of data being shared via emails, Slack channels, and other communication routes daily. This has led hackers to become increasingly sophisticated with phishing techniques to deceive employees into thinking their messages are genuine.

Additionally, zero-trust protocols such as **least privilege access** enforce a level of control and manageability when confronted with a potential breach, **limiting lateral movement during security incidents** and reducing potential damage to critical systems and data.

Recent developments in regulatory requirements, particularly in financial services and healthcare, are **driving the adoption of zero-trust principles as a framework for demonstrating robust security controls and data protection measures**, proving it to be an overall largely beneficial security measure for leaders in 2025.



Cloud Security Posture Management

Multi-cloud complexity, DevSecOps integration, and cost optimisation have all emerged as driving factors of cloud security posture management being prioritised in 2025.

80% Of companies were affected by cloud security incidents in 2024, with more expected in 2025*.

What factors are driving this change? Several reasons contribute to this focus, most notably the **increasing reliance on cloud systems.** The complexities of multi-cloud environments present their own set of challenges: organisations using various cloud platforms often encounter inconsistent security configurations and find it hard to maintain uniform security postures across AWS, Azure, Google Cloud, and others. **Enhanced cloud security posture management (CSPM) provides a strong solution to these issues.**

Cloud environments are **highly dynamic, with frequent changes to infrastructure, applications, and permissions.** CSPM tools play a crucial role by continuously monitoring for misconfigurations that could lead to vulnerabilities or compliance gaps as these environments evolve.

Michalowski, M. (2025) 100+ cloud security statistics for 2025, Spacelift.

onsecurity


onsecurity