RADIATA

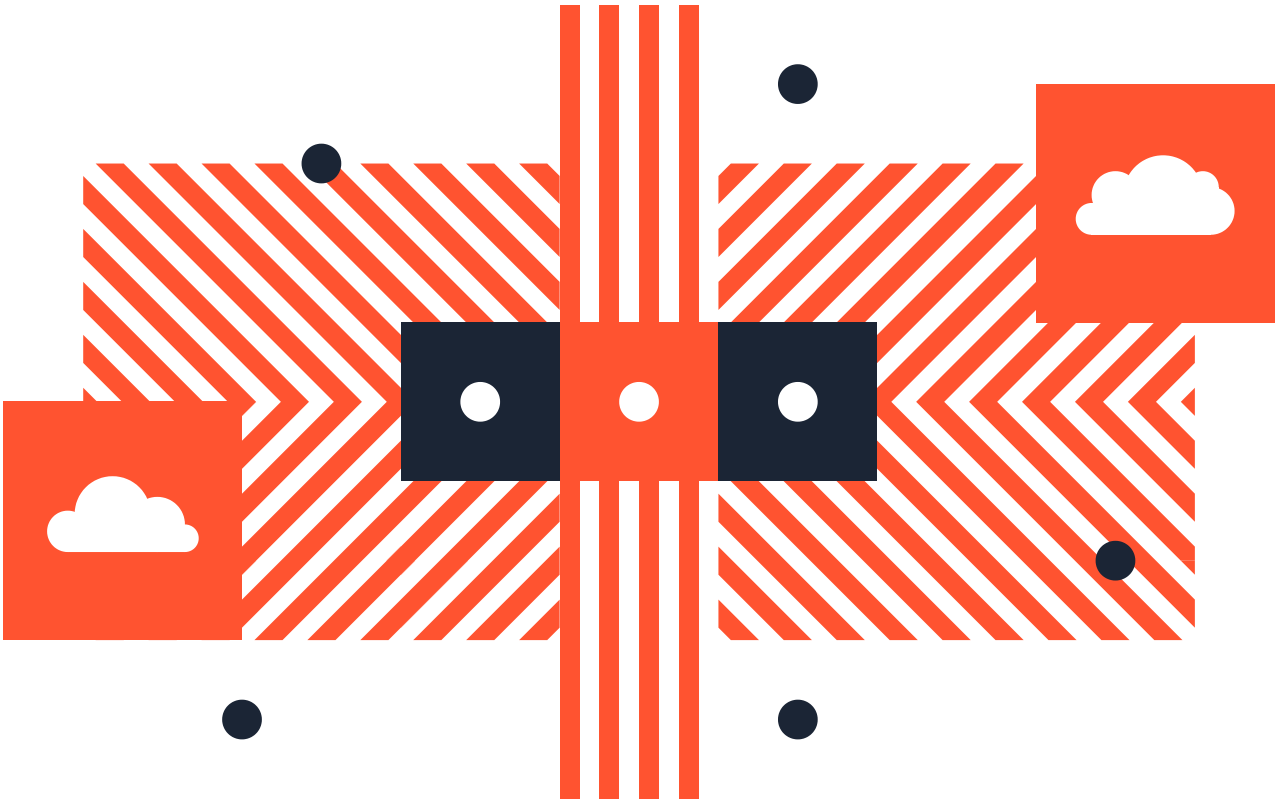
The Evolving Cyber Threat Landscape in 2025

Table of contents

Introduction

Cyberattacks are becoming more automated and widespread. According to Fortinet's 2025 Global Threat Landscape Report, there are now over 36,000 automated scans per second occurring globally. SentinelOne reports a 17% year-on-year increase in newly disclosed vulnerabilities, reflecting the expanding attack surface and growing software complexity.

This sharp rise in global cyberattacks - driven by AI, cloud computing, and IoT adoption - has fuelled a major increase in demand for cybersecurity solutions. According to Statista, the global cybersecurity market is expected to grow from US$185.7 billion in 2024 to US$271.9 billion by 2029, a compound annual growth rate (CAGR) of 7.92%.



Trends

Generative AI
Risk and Response
Generative AI (GenAI) introduces new threats as attackers use it to craft more sophisticated, evasive malware. At the same time, advances in AI and machine learning are dramatically improving detection and response, helping defenders keep pace with evolving threats.

Zero-Trust Architecture
With the rise of remote work and cloud-based operations since 2020, zero-trust architecture has gained widespread adoption. It removes implicit trust within networks, requiring continuous verification of all users and devices. Statista projects the zero-trust market will reach **US$133 billion by 2032.**

Growth of IoT
By 2028, over **20 billion IoT-connected devices** will be in use globally - each one a potential entry point for attackers. Remote working and smart infrastructure continue to drive this expansion, significantly widening the attack surface.

Cybersecurity Talent Shortage
A persistent shortage of skilled professionals continues to hamper cyber resilience. Statista notes that **57% of security leaders** see staffing gaps as a major threat to their organisation's safety.

Types of Attacks
While phishing remains the most common attack vector, the **fastest-growing threat** is investment fraud. Though it accounted for only **9.4% of attacks**, its growth rate has been staggering - **232% since 2016** (Statista). ere.

Industries

Healthcare

Healthcare experiences the highest average data breach costs globally—US$10.93 million per incident—and is projected to account for 12.7% of cybersecurity spending in 2024 (Statista). HealthTech Magazine reports that ransomware campaigns frequently exploit legacy infrastructure and misconfigured backups.

IT & Telecoms

Unsurprisingly, IT and telecoms companies have shown the strongest response, with a **4.6% annual growth rate in cybersecurity spending**, leading all other sectors (Statista).

Finance

The banking, financial services, and insurance (BFSI) sector leads all others in cybersecurity investment, accounting for just over one-third of global spending. However, this share has decreased by 7.1% since 2021 as other industries catch up (Statista).

- The average cost of a data breach in this sector was US$5.72 million in 2021 (IBM).
- Over 90% of successful cyberattacks begin with phishing (Infosec Institute).
- The Anti-Phishing Working Group (APWG) found that phishing was most prevalent in finance during Q1 2021.

E-commerce & Retail

Retail and wholesale industries have averaged just 8% of total cybersecurity spending between 2021 and 2024, despite increasing threats like credential stuffing, DDoS attacks, and payment fraud (Statista). As noted in Reuters, many businesses remain complacent despite rising risks.

SMEs vs Large Enterprises

Small and Medium Enterprises (SMEs)

- 46% of breaches impact businesses with fewer than 1,000 employees (**StrongDM**)
- Just 20% use multi-factor authentication
- 47% have no dedicated cybersecurity team

These organisations often lack the budget and in-house expertise needed to defend against evolving threats, making managed security services an ideal solution.

Large Enterprises

- Face more complex attack surfaces and greater regulatory scrutiny
- 43% report difficulty hiring cybersecurity professionals, particularly for cloud security and SOC roles (Statista)

Recommendations for Building Resilience in 2025

Implement Zero-Trust Architecture
Now a strategic imperative for organisations of all sizes, with global adoption steadily rising (Statista).

Deploy AI-Powered Security Tools
Techniques like deep learning for malware detection and natural language processing for phishing protection are leading innovations.

Secure IoT Devices
As the number of connected devices exceeds 20 billion, organisations must implement strong monitoring, segmentation, and patching.

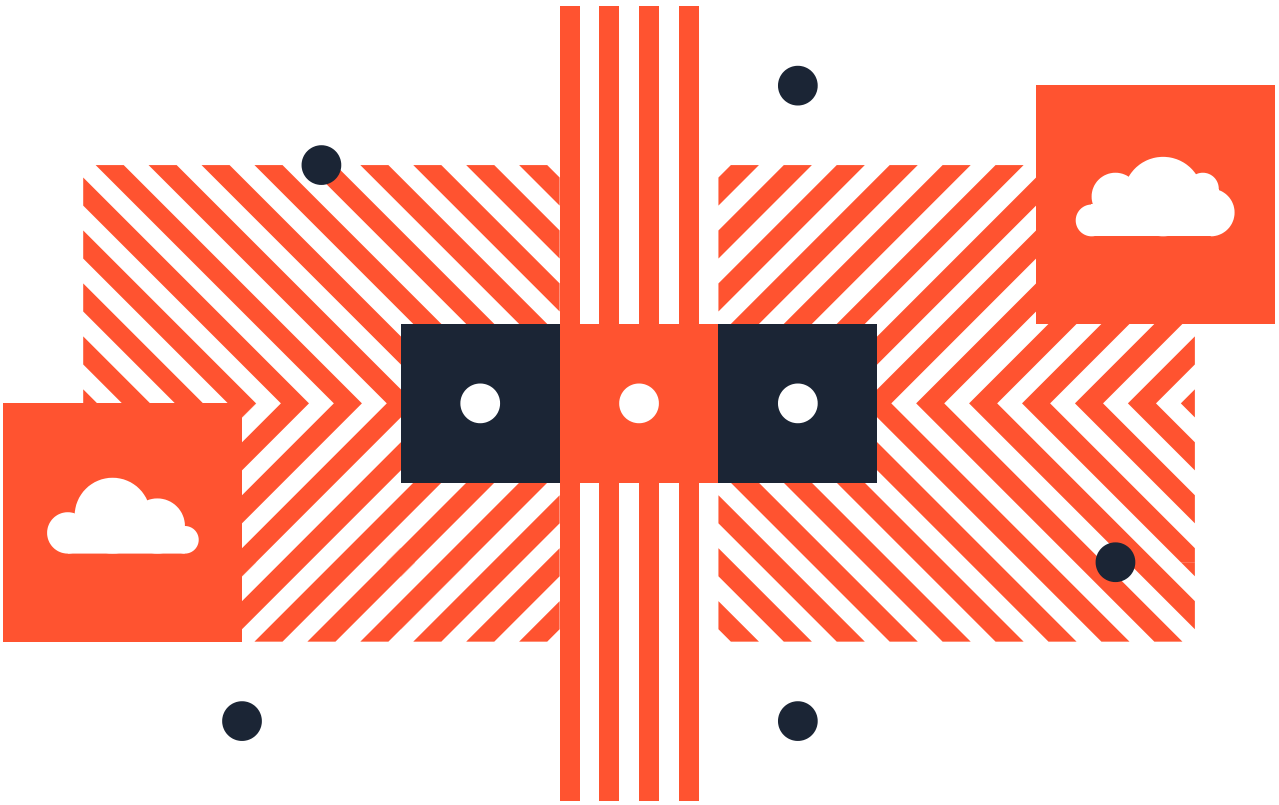
Close Talent Gaps Through Training and Partners
While 76% of boards recommend hiring more cyber staff, 60% of organisations struggle to recruit qualified candidates (Statista).

Adopt Managed Security Services
Providers such as SOC-as-a-Service help SMEs and enterprises reduce time to detection and contain threats effectively.

Invest in Cyber Insurance
Munich Re reports growing interest in insurance solutions as part of broader risk strategies.

Conclusion

Cybersecurity in 2025 is not just a technical issue—it's a board-level priority. As threats become more complex and persistent, businesses must respond with proactive strategies, modern tools, and trusted partners. Whether through zero-trust frameworks, AI-powered tools, or outsourced security services, resilience will define the winners in this evolving digital era.



RADIATA