# Organisations ramp up generative AI security spending amid rising data threats



Thales recently released its 2025 Data Threat Report, illuminating a critical concern for modern organisations: the rapid advancement of artificial intelligence, particularly generative AI. According to the survey conducted by S&P Global Market Intelligence 451 Research, nearly 70% of IT and security professionals from over 3,000 organisations worldwide described this technological evolution as their foremost security worry. This insight underscores a growing awareness of how swiftly AI's integration into business processes can create a precarious security landscape.

The report delineates three primary concerns regarding AI: the speed of development, which was identified as the leading risk by almost seventy percent of participants; issues surrounding AI's integrity (64%); and its trustworthiness (57%). This trepidation reflects the dual nature of AI as both a transformative tool for innovation and a potential vector for threats. While organisations are keen to harness AI's capabilities, they are also becoming increasingly aware of the inherent risks associated with its deployment.

In response to these concerns, investment in security measures tailored specifically for generative AI has surged. Approximately 73% of respondents reported that their organisations are now allocating funds towards AI-specific security tools, marking a significant shift in prioritising security in tandem with technological adoption. Notably, generative AI security has become the second highest spending priority, overtaken only by cloud security—a reflection of the shifting focus within cybersecurity budgets towards emerging technologies.

As organisations struggle to keep pace with the growing AI landscape, Eric Hanselman, Chief Analyst at S&P Global Market Intelligence 451 Research, highlighted the pressures they face. "The fast-evolving GenAI landscape is pressuring enterprises to move quickly, sometimes at the cost of caution," he stated. This sentiment resonates within organisations that are often deploying AI solutions before fully grasping the complexities of their application architectures, which can lead to unintentional vulnerabilities and risks.

In addressing AI-related security challenges, organisations are adopting a multi-faceted approach. Over two-thirds indicated they are procuring security tools directly from their cloud providers, while about three in five are relying on established security vendors. Additionally, nearly half are exploring partnerships with start-ups specialising in this area, demonstrating a willingness to innovate in safeguarding data.

As generative AI continues to reshape operational frameworks, its integration is already well underway. A third of respondents reported that generative AI is either enhancing or transforming their operations. As agentic AI applications—those capable of autonomous decision-making— emerge, ensuring data quality and security is more critical than ever.

However, the threat landscape remains complex and multi-dimensional. Malware has firmly established itself as the most persistent attack vector since 2021, and this year, phishing has surged to become the second most prevalent form of attack, shifting ransomware to the third position. While the overall rates of reported data breaches have modestly decreased from 56% in 2021 to 45% in 2025, the ongoing evolution of cyber threats indicates a persistent need for vigilance.

The nature of cyber threat actors is also shifting, with external sources such as hacktivists and nation-state actors now perceived as the most significant threats. Human error, which previously ranked higher, is now viewed as the third largest contributor to breaches, reflecting a changing awareness of the sources of risk.

Emerging technologies, such as quantum computing, are amplifying security concerns regarding encrypted data. Among surveyed organisations, 63% fear that quantum technologies could one day disrupt current encryption methods, exposing sensitive information. Other concerns include vulnerabilities in encryption key distribution and the "harvest now, decrypt later" risk, where attackers collect encrypted data today for future decryption once quantum computing capabilities advance. In response, half of the organisations are reassessing their encryption strategies, and 60% are either prototyping or evaluating post-quantum cryptography solutions.

Todd Moore, Global Vice President of Data Security Products at Thales, commented on the urgent need for action: "The clock is ticking on post-quantum readiness… even with clear timelines, the pace of encryption change has been slower than expected due to a mix of legacy systems and the complexity of balancing innovation with security." This suggests a critical juncture for organisations: the necessity to proactively refine their security infrastructures against emerging threats while navigating the complexities of integrating new technologies.

The insights from the 2025 Data Threat Report indicate substantial improvements in organisations' overall security postures; however, the pathway ahead demands ongoing adaptation to face the operational challenges posed by emerging technologies like generative AI and quantum computing. As the cyber threat landscape continues to evolve at an unprecedented pace, companies are left with the imperative to balance innovation with robust security measures to protect their systems and sensitive data from an ever-expanding array of risks.

### Reference Map

1. [[1]](https://channellife.co.nz/story/organisations-boost-ai-security-as-data-threats-risks-evolve)
2. [[2]](https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/artificial-intelligence-fuels-rise-hard-detect-bots)
3. [[3]](https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/press_release/thales-unveils-its-cyber-trends-2025-report)
4. [[4]](https://cds.thalesgroup.com/index.php/en/hot-topics/ai-appsec-and-offensive-security-penetration-testing-trends-2025)
5. [[5]](https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/magazine/whats-happening-cybersecurity-here-are-25-facts)
6. [[6]](https://www.thalesgroup.com/en/countries-europe/spain/news/thales-s21sec-reveals-key-trends-will-transform-cybersecurity-2025)
7. [[7]](https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/2024-thales-data-threat-report-reveals-rise-ransomware)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://channellife.co.nz/story/organisations-boost-ai-security-as-data-threats-risks-evolve> - Please view link - unable to able to access data
2. <https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/artificial-intelligence-fuels-rise-hard-detect-bots> - Thales' 2025 Imperva Bad Bot Report reveals that AI-driven bots now constitute over half of global internet traffic, with automated traffic surpassing human activity for the first time in a decade. The report highlights the role of accessible AI tools in enabling cyber attackers to create and deploy malicious bots at scale, leading to a 37% increase in bad bot activity compared to the previous year. The travel sector is notably impacted, accounting for 27% of all bot attacks in 2024. The report emphasizes the need for organizations to adopt adaptive and proactive security measures to counteract the evolving threat landscape.
3. <https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/press_release/thales-unveils-its-cyber-trends-2025-report> - Thales' Cyber Trends 2025 Report identifies key cybersecurity challenges, including targeted ransomware, supply chain vulnerabilities, and the exploitation of connected devices (IoT). The report underscores the dual role of artificial intelligence as both a tool for cyber attackers and defenders, highlighting the necessity for appropriate countermeasures. It also points out the persistent threat of software vulnerabilities and the exploitation of open-source software. The report advocates for an adaptive, multi-layered approach to cybersecurity, emphasizing continuous monitoring and collaboration between public and private sectors to safeguard IT systems.
4. <https://cds.thalesgroup.com/index.php/en/hot-topics/ai-appsec-and-offensive-security-penetration-testing-trends-2025> - Thales' analysis of penetration testing trends for 2025 highlights the integration of artificial intelligence in offensive security. The report discusses the emergence of Purple Teaming, which combines offensive and defensive security efforts to enhance threat detection and response capabilities. It also explores the use of AI in red teaming tactics, including AI-driven phishing attacks and advanced evasion techniques. Additionally, the report addresses the importance of securing AI models against adversarial attacks and the need for organizations to proactively identify vulnerabilities to strengthen defenses against evolving threats.
5. <https://www.thalesgroup.com/en/worldwide/digital-identity-and-security/magazine/whats-happening-cybersecurity-here-are-25-facts> - Thales' 'What's Happening in Cybersecurity? Here Are 25 Facts for 2025' provides insights into the evolving cyber threat landscape. The report reveals a 72% increase in cyber risks, with cybercriminals earning over $1 trillion in 2024. It highlights the rise of AI as a significant threat, with 66% of organizations expecting AI to have the most substantial impact on cybersecurity. The report also notes a 223% rise in the trade of deepfake-related tools on the dark web between Q1 2023 and Q1 2024, emphasizing the growing sophistication of cyber threats.
6. <https://www.thalesgroup.com/en/countries-europe/spain/news/thales-s21sec-reveals-key-trends-will-transform-cybersecurity-2025> - Thales S21sec's analysis of cybersecurity trends for 2025 highlights the intensification of geopolitical conflicts, the deployment of AI, and the growing digital reliance as primary challenges. The report notes the evolution of cybercrime into a 'crime as a service' model, enabling individuals with minimal technical knowledge to conduct cybercrimes. It also emphasizes the exploitation of supply chain vulnerabilities and the rise of cyber espionage operations, particularly targeting NATO members and influencing electoral processes in Latin America.
7. <https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/2024-thales-data-threat-report-reveals-rise-ransomware> - Thales' 2024 Data Threat Report reveals a 27% increase in companies falling victim to ransomware attacks, with 8% paying the ransom. The report highlights that 43% of enterprises failed a compliance audit, with those companies being ten times more likely to suffer a data breach. Human error is identified as the top cause of data breaches for the second consecutive year. The report also explores the impact of emerging technologies, noting that 57% of IT professionals view artificial intelligence as a significant source of concern in cybersecurity.