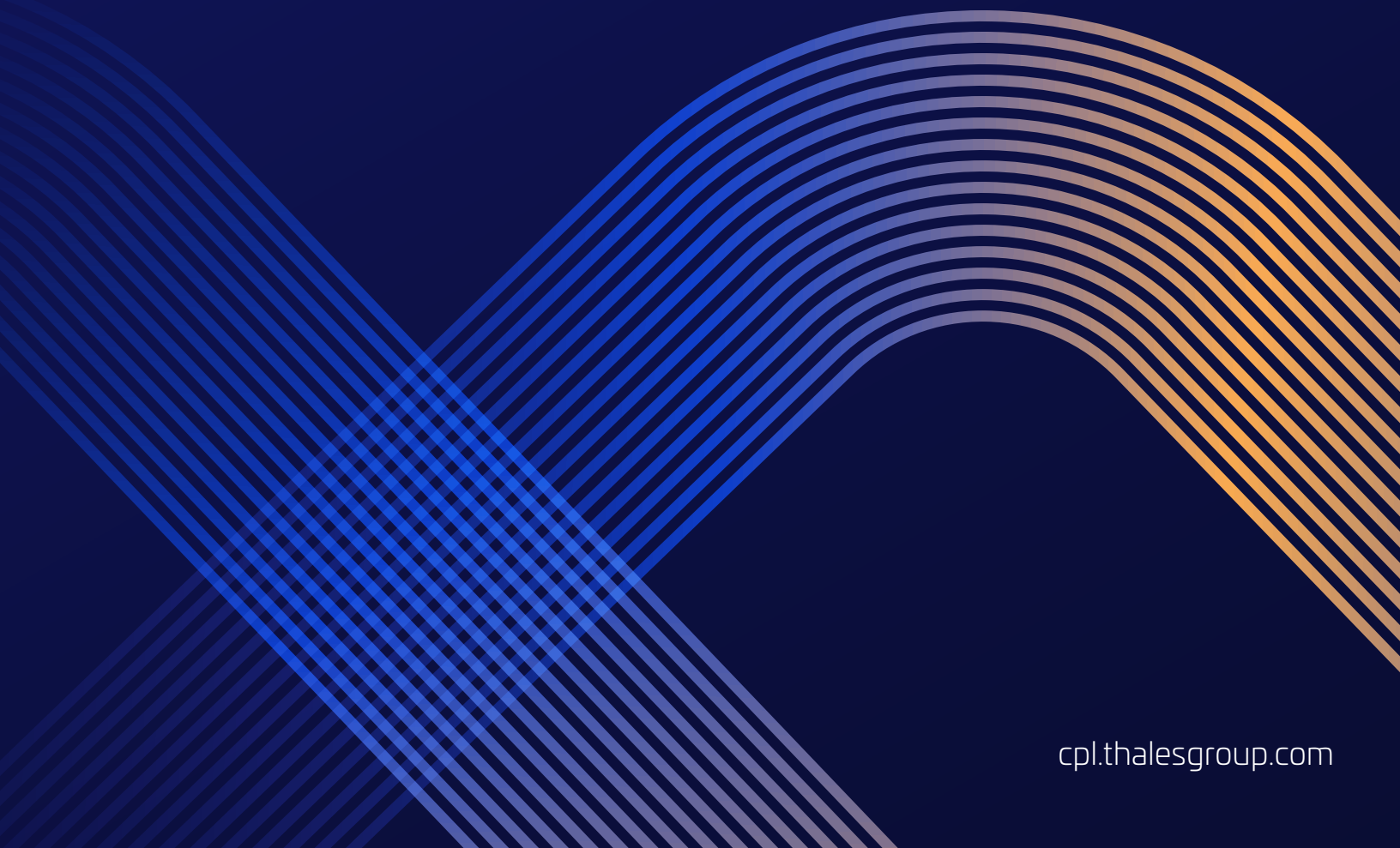
THALES
Building a future we can all trust

#2025DataThreatReport

2025

DATA THREAT REPORT

AI, Quantum and the Evolving Data Threatscape



cpl.thalesgroup.com

Table of Contents

Introduction

For five consecutive years, the **Thales Data Threat Report** has analyzed worldwide trends in data security, cloud adoption, compliance and security strategies. The 2025 report continues to examine internal vulnerabilities, external threats and their impacts on enterprise assets. The Data Threat Report also evaluates new and evolving technologies affecting risk management and data security. The report revisits core data security principles in light of evolving technology, industry, regulatory and risk landscapes, with additional focus this year on application security. As always, the Data Threat Report encourages and equips security leaders to build stronger alliances spanning their own organizations and partner ecosystems to achieve broader enterprise goals.

S&P Global
Market Intelligence

Source: 2025 Data Threat Report custom survey from
S&P Global Market Intelligence 451 Research, commissioned by Thales.

Sponsored by

Arrow Five Years Out

EXCLUSIVE NETWORKS

CLIMB

TD SYNNEX

Executive Summary

The 2025 Data Threat Report is based on survey data from nearly 3,200 IT and security professionals across 20 countries and 15 industries, including financial services, public sector, critical infrastructure and technology verticals. Participants included executives, managers and practitioners in data science, security, development and policy-making. The report studies current attitudes and actions to better understand enterprise priorities in a changing global threat landscape.

AI, and generative AI (GenAI) in particular, has been a major focus of technology investment and operational change. Dramatic technological changes related to AI have much to do with the technology's critical dependence on data. Reliable, high-quality data is essential for training, inference, augmentation and content generation. With the emergence of agentic AI, data quality will be equally critical for enabling AI agents to make sound decisions and take relevant actions. Much of the data used for these purposes is both sensitive and indispensable to the organizations that rely on it. This means that the success of today's technological disruption hinges on assuring the confidentiality, integrity and availability of vital data resources.

Enterprises of all sizes are embracing GenAI. This year, a third of respondents said they are integrating GenAI into their organizations or the technology is already transforming their operations. GenAI's impact may further influence evolving data and privacy regulations, emphasizing the importance of maintaining confidentiality, trustworthiness and safety. However, the rapidly changing GenAI ecosystem*, characterized by new infrastructures, SaaS services and increasingly autonomous agents, poses significant risks. Notably, 69% of respondents cited this fast-changing ecosystem as the most concerning security risk for GenAI adoption.

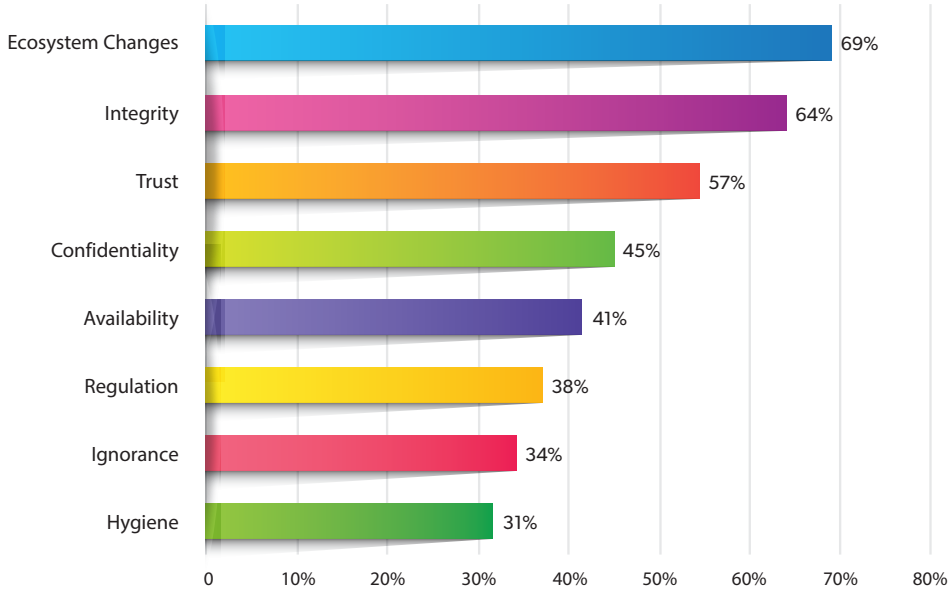
While GenAI is intensifying the focus on data security, hasty implementations raise the risk of data breaches. The vulnerabilities in DeepSeek reported shortly after its V3 release serve as a cautionary tale for security teams. Because GenAI architectures are new for most security teams, prioritizing data security efforts is crucial.

Structural and geopolitical changes in 2025 will likely prompt enterprises to rethink their security strategies. The Data Threat Report results suggest that organizations would be wise to focus on their most valuable asset: the data they collect, process, store and steward for stakeholders and customers. This report examines various data security concerns and identifies practical ways to mitigate risks.

Among these concerns is the growing complexity of application architectures, which necessitates improved application security. More than a third of businesses (34%) reported having over 500 application programming interfaces (APIs) in use. This proliferation raises broad concerns about vulnerabilities in code (59%) and in the software supply chain (48%). While shift-left security controls are the top-cited priority for application protections, respondents also emphasized foundational production controls such as dynamic application security testing (DAST) and web application firewall (WAF).

** For the purposes of the Data Threat Report survey, GenAI ecosystem encompasses the full set of vendors and technologies in GenAI.*

Most concerning risks related to GenAI security



Other application security concerns on the architecture side include secrets management, which leads among DevOps security concerns. However, only 16% identified secrets management as important for data protection, despite the high risk associated with secrets management failures, which can expose authentication data such as API keys. This concern is amplified given the high reported number of APIs in use.

Understanding data is critical to securing it effectively, and there are encouraging results in data classification: 87% reported that they can classify at least half of their data, a notable increase from previous years. However, nearly two-thirds (61%) use five or more tools for data discovery and classification, which can lead to misalignment and conflicting protection policies. There is better alignment regarding post-quantum cryptography risks, with three out of five respondents prototyping new ciphers. Deployment timelines are crucial, but early signs of this transition are promising. Regulatory focus on cryptographic protections is also notable. When asked about data sovereignty concerns, two in five said they believe encryption could provide sufficient protections to meet sovereignty mandates. For this strategy to be viable, regulators will also need to accept this mitigation; developments such as Singapore's Data Embassy initiative could signal progress in this regard.

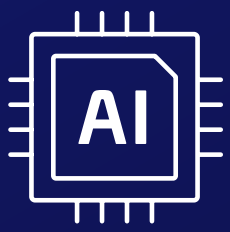
The 2025 Data Threat Report results show progress in key areas of data security, but much work remains as organizations mature their data security controls. Efforts must intensify to securely empower the surge in GenAI activity. New and unfamiliar risks must be addressed, and the tools and technology to mitigate them are available, but they must be used effectively and expeditiously.

Note: All charts displayed in this document are from S&P Global Market Intelligence 451 Research's 2021-2025 Data Threat custom surveys.

Key Findings

Tracking AI Development

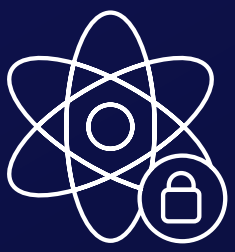
69% regard fast-moving ecosystem as most concerning GenAI security risk, followed by lack of integrity (64%) and trustworthiness (57%).



73% of respondents are investing in GenAI-specific tools, with 20% using newly allocated budget.

11% considering their AI implementations as transformational.

Right on 'Q'



Organizations identified these major quantum computing security threats:

63% future encryption compromise

61% key distribution

58% future decryption of today's data, including harvest now, decrypt later

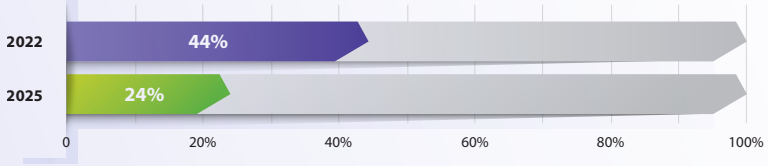
Data Security Fuels Digital Sovereignty

55% were driven to pursue digital sovereignty by specific customer, regional or global privacy mandates.

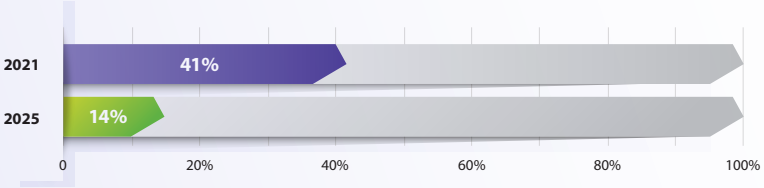
42% said that encryption and key management provide sufficient protection.

Trends in Data Security

24% have little or no confidence in identifying where their data is stored.

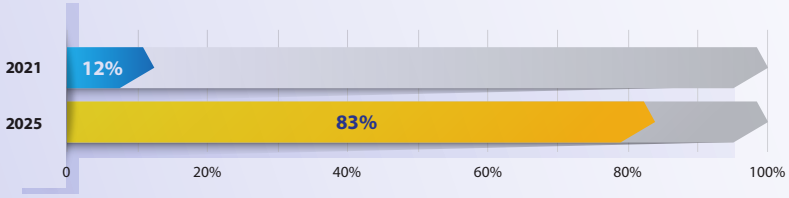


14% reported experiencing a recent data breach.



The Threat Landscape, Inside and Out

83% said that strong MFA is used more than 40% of the time.



From Cloud DevOps to Platform Engineering

55% said Secrets management is the leading DevOps security challenge.

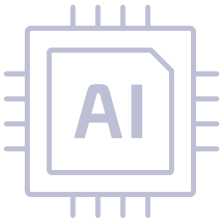
16% identified secrets management as most effective in protecting data, despite the devastating impact of compromised secrets.

Application Security: Essential for Data Protection

34%

of enterprises use more than 500 APIs; that proportion rises to 50% among Manufacturing respondents.

59% of respondents said code vulnerabilities are a major concern for application security, placing it as the top response.



In the Era of AI, Data Takes Center Stage

GenAI's promise to transform enterprises is enticing, and the resulting enthusiasm is significantly impacting data security along with other areas of enterprise IT. Functions such as report writing, customer service, marketing, sales and legal all stand to benefit from GenAI. For example, chatbot interfaces in customer service can intelligently preempt or resolve issues at scale, while marketing teams may generate content dynamically for each customer interaction. GenAI enables knowledge workers to augment their work at unprecedented scale, marking a potential leap in productivity.

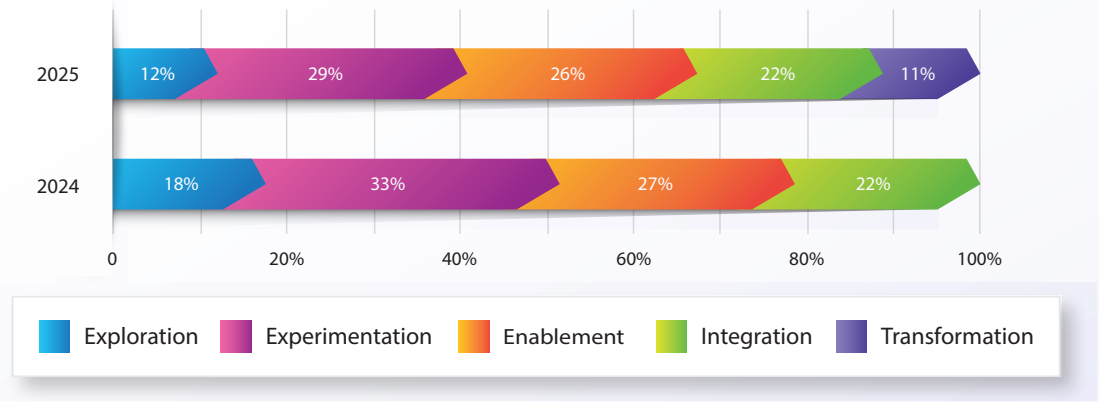
Technology leaders must draw parallels between GenAI and other major technological shifts. As applications become more distributed in the cloud, with presentation, logic and data tiers spread across multiple cloud regions or sourced from various third-party APIs or SaaS offerings, enterprises must also consider the protections that safeguard those diverse systems. Risks must be translated across various model tiers and architectures. If not properly addressed, this complexity can result in ambiguous security or compliance enforcement. For example, verifying a data subject access request may be difficult if a public large language model (LLM) already includes that user's personally identifiable information. Thus, training data provenance has become an important part of data security.

> *The pace of adoption has shifted significantly in just one year, with one-third of enterprises now saying they are in the 'integration' or 'transformation' phases of their GenAI journey.*

These issues notwithstanding, organizations are under immense pressure to deliver GenAI capabilities. The pace of adoption has shifted significantly in just one year, with one-third of enterprises now saying they are in the "integration" or "transformation" phases of their GenAI journey.

This year's Data Threat Report compares the security practices of organizations in the integration and transformation phases with those in the exploration, experimentation and enablement phases. Interestingly, those in the latter phases do not exhibit discernably different security behaviors than those in earlier phases. Statistical testing across breach occurrence, compliance failures, MFA adoption rates, data classification rates and data encryption rates reveals little evidence of changes in security beliefs or practices among those in latter phases of the AI journey. Similarly, we found no correlation in technology choices.

Where are you in your AI Journey?



It is also reasonable to expect little meaningful correlation between security outcomes and technology adoption rates. Complex enterprises with multiple clouds, hundreds of SaaS services or thousands of API endpoints do not necessarily have more compliance failures or data breaches. And while simpler environments may reduce the complexity of security control verification, they are not inherently more secure than complex environments.

This suggests that respondents in the latter phases of AI adoption are simply not waiting to get their security or technology houses in order before departing on their journey. The urgency to move into transformation supersedes improvements to organizational readiness. In this way, respondents may be creating their own greatest security risk: The fast-moving GenAI ecosystem may be luring enterprises into taking excessive risks in fear of falling behind the AI adoption curve.

Data Threat Report respondents have long wrestled with complexity and uncertainty, including multicloud IaaS, numerous SaaS applications and thousands of API endpoints. The potential number of AI agents, their capabilities and the depth of integration or interoperation remain unknown. This rapidly increasing complexity is top of mind for survey respondents: 69% cited the fast-moving GenAI ecosystem as their greatest security concern.

However, security for GenAI also raises data security principles that have not been as widely considered. While many security leaders have historically focused on data availability and data confidentiality, they have often directed less effort toward data integrity and trustworthiness. Yet data integrity and trustworthiness are now the second- and third-greatest security concerns with GenAI, respectively. In ranked choice voting, 64% of respondents said data integrity attacks — where adversaries could inflict bias or poison models with incorrect data — are a significant concern. While industries such as retail and financial services with large volumes of financial transactions have invested in fraud-detection tools to identify and remediate false ledger entries, unstructured data integrity and trustworthiness may be more difficult to enforce than either availability or confidentiality.

Some organizations are simply not waiting to get their security or technology houses in order before departing on their AI journey as the urgency to move into transformation supersedes improvements to organizational readiness.

GenAI Model Risks

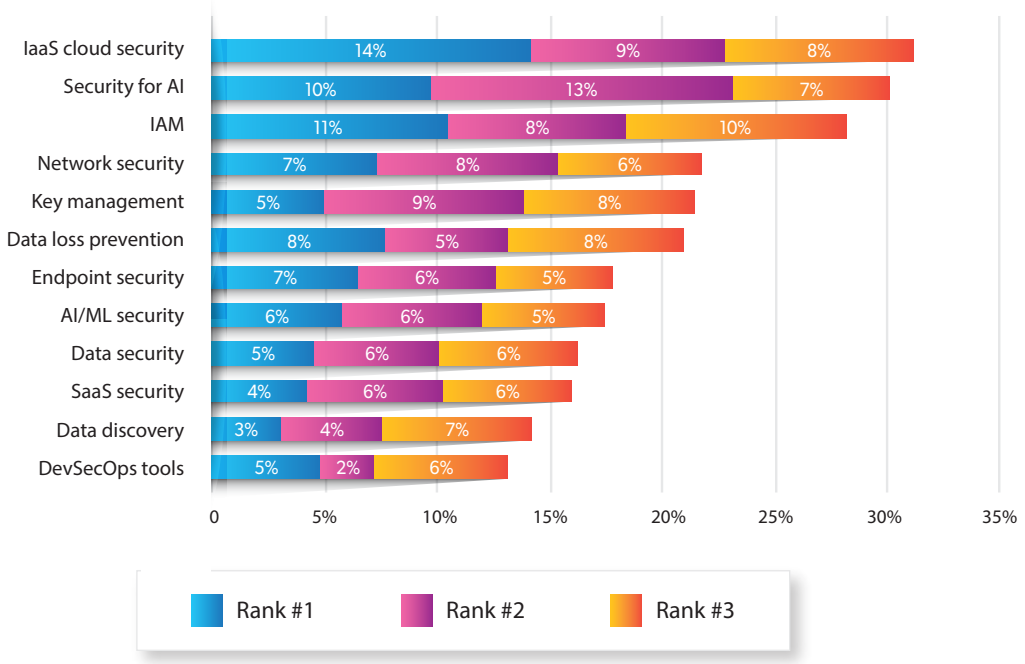
GenAI language models entail systemic risks, including:

- **Bias and fairness** — models can learn bias, which can negatively affect the quality of output.
- **Model theft** — underlying architecture, content, embedding layers, weights and measures may be maliciously obtained or extracted.
- **Adversarial input** — input data can manipulate or deceive the model to release incorrect or confidential output.
- **Output manipulation** — Deepfakes and other fraudulent contents can be created to cause harm.

Model risks have implications for data confidentiality, trustworthiness and integrity.

In response, 73% of respondents said they are investing in AI-specific security tools with either new or existing budgets. Those investing in AI-specific security tools tend to pursue multiple avenues: More than two-thirds have obtained tools from their cloud provider, three in five have used an established security vendor and about half have used new or startup vendors. As a spending priority, security for GenAI debuted at No. 2, just behind cloud security in ranked choice voting.

Top security technologies by spending level



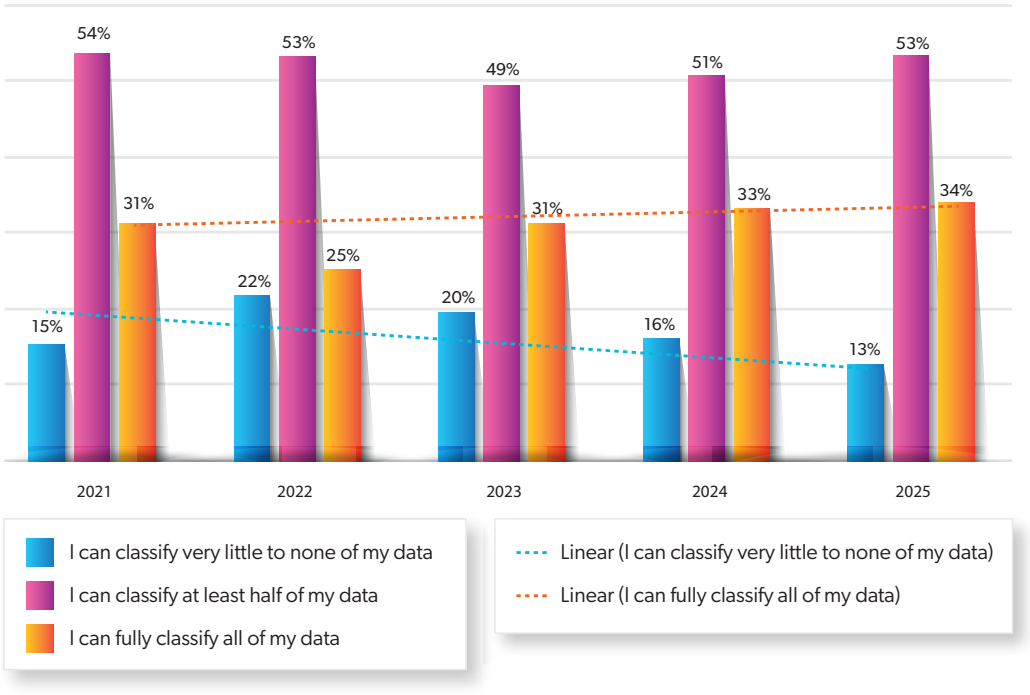
Enterprises may not fully understand their GenAI application architectures, and the popularity and proliferation of enterprise SaaS applications with GenAI capabilities adds further complexity. Nevertheless, enterprises must take stock of their data, which remains a durable, critical and valuable asset. GenAI applications will increasingly rely on enterprise data to support agentic interfaces and interactions. GenAI represents a logical progression of digital transformation for enterprises, and organizations that combine it with improved automation are likely to achieve better outcomes. The pathway to GenAI parallels enterprise movement to the cloud; flexibility and readiness are essential for navigating a changing landscape of opportunities and threats.

Trends in Data Security

Over the years, the Data Threat Report has tracked enterprise respondents' data security strategies and results, revealing a shift in industry understanding of risks as enterprises transform internally and face new external market realities. The era of "set and forget" audits and controls is over; the dynamism of technology requires enterprises to be more responsive than ever. GenAI represents the latest leap for enterprises, but it is part of a larger picture. As the data security discipline evolves across various data-driven lines of business, and as external privacy and compliance expectations grow, this year's survey results reflect progress in addressing data security risks.

Enterprises are gradually improving their security measures. Despite ever-growing data volumes, confidence in data location has risen. In 2021, 36% of respondents said they were somewhat or not at all confident in locating their data. In 2025, this figure dropped to 24%. However, confidence in data classification has remained quite flat, with 80%-85% of respondents consistently saying they can classify at least half of their data.

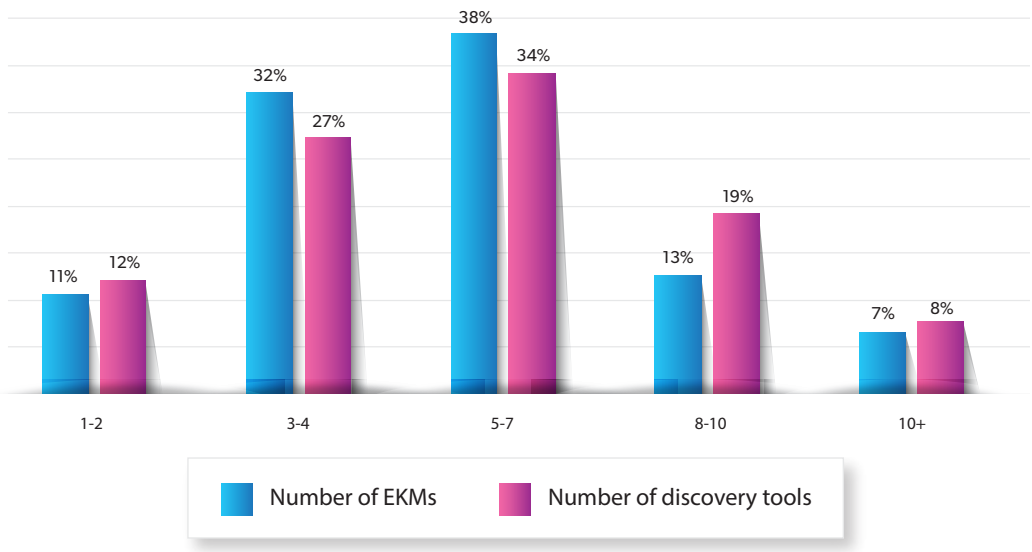
Ability to classify organizational data



Notably, enterprises report implementing stronger controls, particularly for cloud data. In 2021, only 46% of respondents said that 40% or more of their sensitive cloud data was encrypted. By 2025, this proportion rose to 68%, marking encouraging progress.

Technology improvements have enhanced the application of controls. Today, more than 99% of browser and mobile app traffic is encrypted via HTTPS, embodying secure-by-design and secure-by-default principles. However, data location, classification and control enforcement in enterprises remains fragmented. Nearly two-thirds of respondents (61%) use five or more tools for data discovery, monitoring or classification. Similarly, 57% of respondents use five or more enterprise key managers (EKMs) for encryption.

Number of data discovery tools and EKMs in use



Effective classification and encryption capabilities are critical to manage the risk associated with AI integration.

Multiple rule sets across various tools can lead to duplicative methods of identifying or classifying data. Moreover, the variety of systems can result in inconsistent controls applied to sensitive data. Fragmented or unknown data locations, duplicate classification rules and inconsistent protections create silos and security coverage gaps over time, and the complexity of these fragmented systems raises the risk of breaches caused by human error.

Enterprises seeking to leverage AI must ensure that it does not compromise their security. Effective classification and encryption capabilities are critical to manage this risk. Proprietary or confidential information must not be included in the training of publicly available LLMs. Furthermore, retrieval-augmented generation processes may add specific information and fetch content without adhering to existing classification or usage rules. Unmonitored or ungated GenAI use poses significant risk, including the potential for adversarial misuse that could drive the spread of misinformation and engender brand distrust. Therefore, controls to locate, classify and protect data are critical to enable GenAI integration and transformation.

Right on 'Q'

As noted in 451 Research's 2024 report The Next phase of the Quantum Future, quantum computing capability jumped in 2024, with current quantum processors surging to more than 5,000 physical qubits. In addition, GenAI and specific transformer models are used to simulate and test quantum circuits with applications in both logic validation and noise management. In 2024, researchers successfully used a 5,000-qubit quantum computer to attack 50-bit RSA keys, demonstrating a real-world implementation of Shor's algorithm. While classical computing can quickly decrypt 50-bit RSA keys, the study brings a theoretical attack a step closer to "Q-day," when quantum computing will be able to decrypt classical encryption algorithms.

PQC Primer

Quantum computing holds the potential to solve mathematical problems that are difficult or impossible with conventional or classical computing methods.

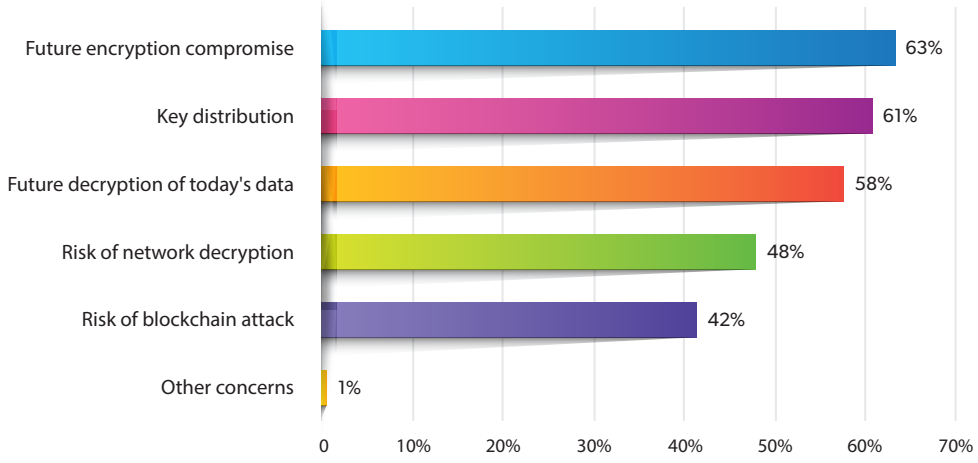
Much of what makes data encryption effective is the extensive time it would take for classical computers to perform decryption. Classical encryption algorithms such as RSA (Rivest, Shamir, Adleman) are based on the multiplication of two large prime numbers; these numbers are difficult to factor for classical computers.

In 2010, researchers factored a 768-bit key with 2,000 hours of computing time; a similar effort for today's RSA 3,072-bit or 4,096-bit keys would take thousands of years. However, Shor's algorithm, proposed by mathematician Peter Shor in 1994, suggests that sufficient quantum computing resources could decrypt classical encryption much more quickly.

In response, efforts to develop, evaluate and implement new, stronger encryption algorithms have given rise to the discipline of post-quantum cryptography (PQC).

When asked about post-quantum cryptography (PQC) challenges, respondents cited future encryption compromise, secure key distribution and future decryption of today's data as their top security concerns, with about 60% identifying each of these issues in ranked choice voting.

Top quantum computing security threats



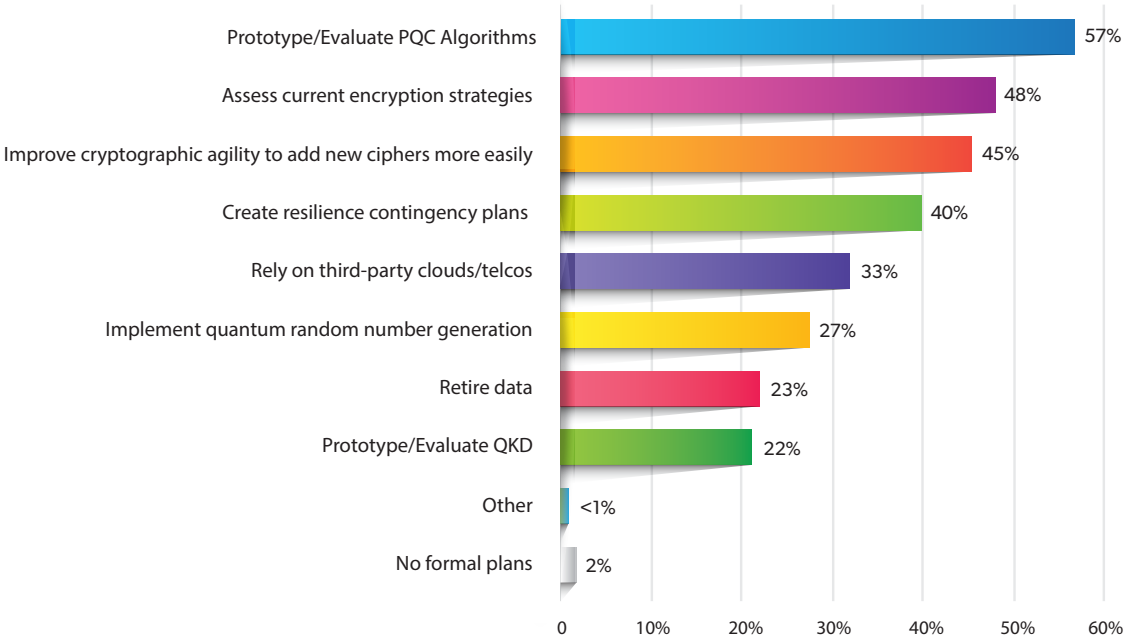
Both enterprises and industry governing bodies have made progress. The National Institute of Standards and Technology (NIST) released its suite of algorithms, the Commercial National Security Algorithm (CNSA 2.0), in September 2022, followed by its PQC transition guide in November 2024. The NIST guide advocates deprecating public-key cryptography algorithms such as RSA and ECC by 2030 and disallowing their use by 2035, leaving only a decade to prepare for a quantum-enabled future.

Encouragingly, many organizations are proactively addressing these challenges. In ranked choice voting, respondents emphasized evaluating PQC algorithms, assessing encryption strategies and improving cryptographic agility as the leading measures to satisfy quantum computing security concerns. While large cloud service providers have also implemented PQC within their offerings, only about one-third of respondents said they would rely on third-party cloud and telco service providers.

> *Only around a third of organizations said they would rely on third-party cloud and telco service providers to address PQC concerns.*

Despite the timelines specified for transitioning to PQC algorithms, encryption has been slow to change for various reasons. While standards such as RSA have stood the mathematical test of time and remain relevant for classical cryptography, cryptography disciplines have not quickly adapted to changing technology. Encryption and security are frequently applied to systems long after their initial design. For example, TCP/IP was created in 1983, while SSL, the predecessor to TLS, did not achieve significant adoption until 1996. Much classical encryption applied via public key infrastructure (PKI) has not evolved to accommodate rapid changes in trust. The developer experience necessary to implement security has also lagged, creating risks in managing classical encryption.

Top responses to quantum threats



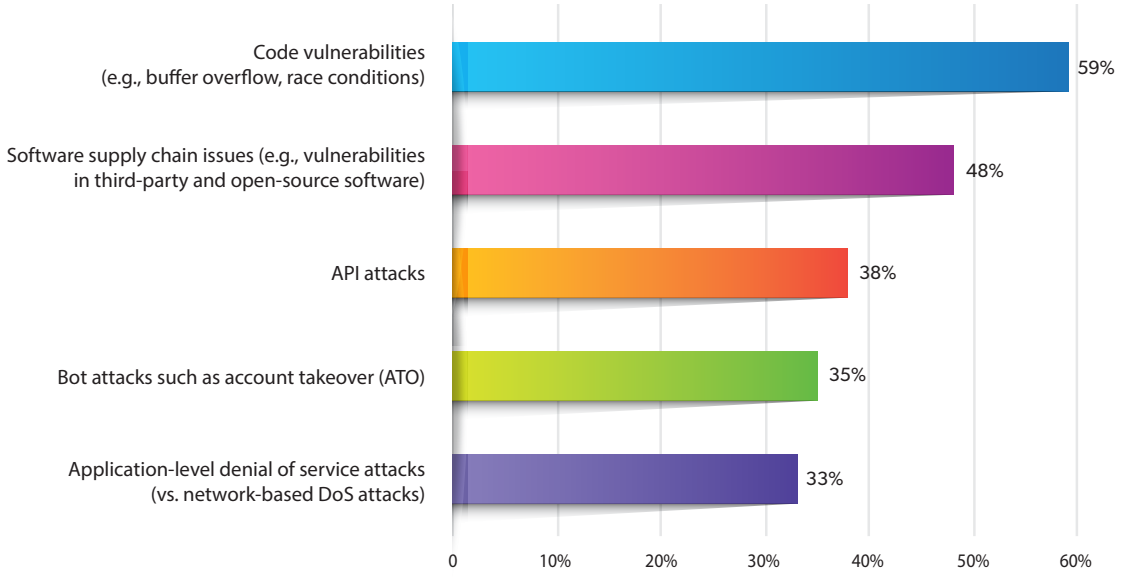
Given the integration of encryption and authentication capabilities in software, enterprises often struggle to update their classically encrypted systems. Implementing algorithm improvements from RSA to lattice-based PQC algorithms such as ML-KEM requires extensive changes in protocols, programming libraries, cryptographic hardware such as hardware security modules and trusted platform modules. Brittle networks that cannot support newer protocols such as TLS 1.3 or accommodate the longer key lengths of PQC algorithms impede crypto-agility and make it difficult to retire technical debt.

Infrastructure such as PKI and certificate authorities may require organizations to implement significant operational changes while carefully maintaining backward compatibility throughout a potentially lengthy transition period. Enterprises should assess all their assets to understand which updates to apply.

There is No Data Security Without Application Security

Application security threats and mitigating measures have evolved rapidly, led by progress in application development technologies — another area where security controls are chasing changes in infrastructure. As organizations have adopted methods such as DevOps and CI/CD to accelerate software development and deployment, security teams face pressure to avoid hindering that pace. At the same time, the consumption of software functionality is changing. The use of APIs is driving integration of software systems, and this represents another area where security controls must catch up. Many enterprise applications deployed as serverless architectures are exposed solely through APIs. The software supply chain has expanded beyond third-party code built into applications to include functionality delivered through APIs. The survey results indicate challenges organizations face in balancing application functionality and security needs.

Top concerns about application security



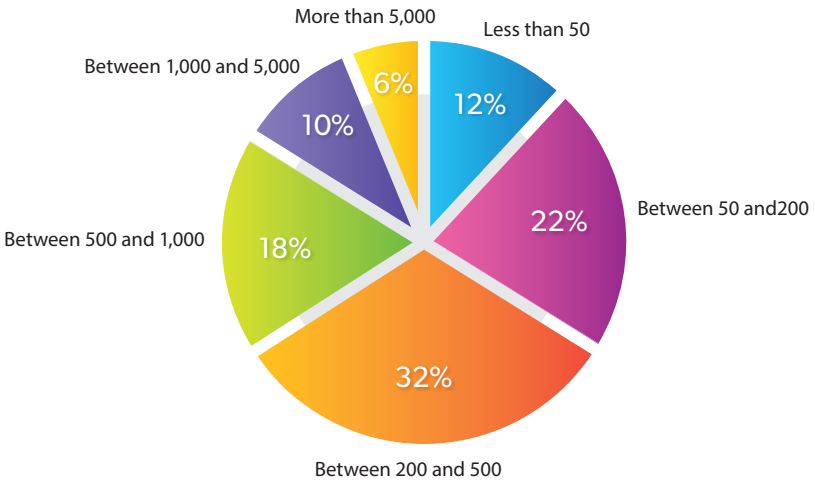
Code vulnerabilities lead among the application security concerns reported. It is an age-old problem, and this concern is also reflected in respondents' prioritization of application security methods: Static application security testing and dynamic application security testing lead the list of AppSec tactics in use or in plan.

The use of APIs varies considerably across industries. Survey-wide, 34% of respondents reported using more than 500 APIs, but that proportion rises to 50% among manufacturing respondents.

Retail and financial services follow, with 41% of respondents in each of these verticals using more than 500 APIs. Education is at the bottom, with only 15%. Interestingly, the relative prevalence of API use in a given industry does not correlate with the expressed level of concern about API attacks. For instance, pharmaceutical industry respondents notably rated API attacks high on their list of concerns, but only 30% have more than 500 APIs in use, below the survey-wide result. However, that concern is not necessarily translating into implementation priorities: Pharmaceuticals respondents ranked API security behind DAST and SAST in terms of current or planned security implementation.

One strategy to improve security in software development is "shift left," which aims to incorporate security controls as early as possible in the development process. While this concept is important, it can be challenging to implement. SAST, a technique that could be considered a shift-left method, leads the list of priorities, but it is followed closely by DAST and WAF, both of which could be described as "shift right" because they test applications in production. Challenges in deploying shift-left approaches may continue to drive investment in shift-right protections. Production application protections support shift-left efforts by, for example, catching unknown threats and zero-day vulnerabilities that have not yet been discovered in the code.

Number of APIs in use



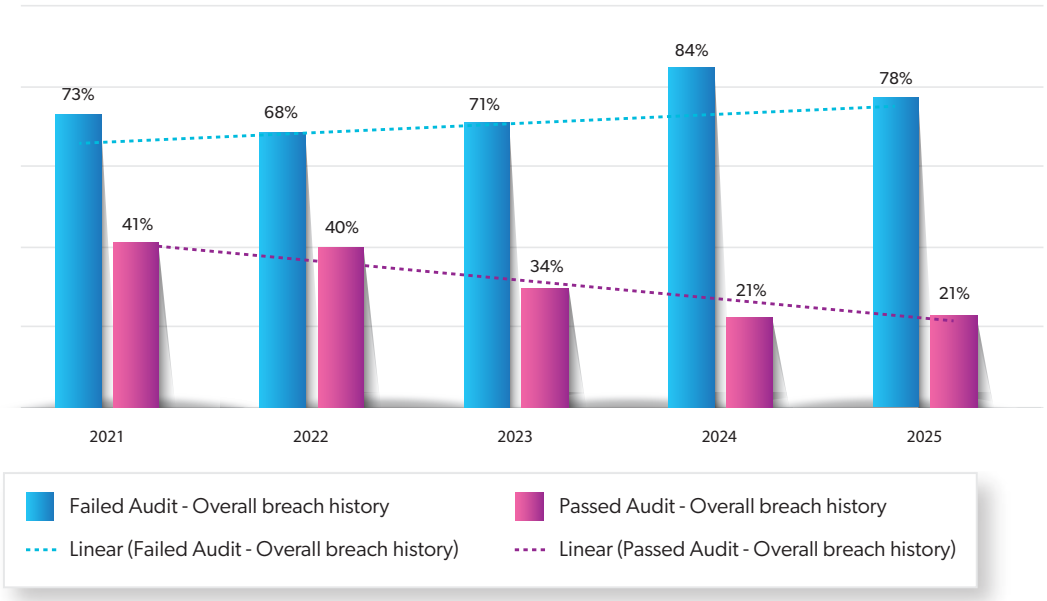
Production application protections support shift-left efforts by, for example, catching unknown threats and zero-day vulnerabilities that have not yet been discovered in the code.

Some Progress in Reducing Data Breaches

Enterprises report improved outcomes from enhanced security measures in data discovery, classification and protection. Although breach occurrences remain high, they have declined slightly over the past few years. In 2021, 56% of respondent enterprises had experienced a data breach, compared to 45% in 2025. The percentage of respondents reporting a breach in the last 12 months decreased from 23% in 2021 to just 14% in 2025.

While breaches will persist, security teams must strive to prevent or mitigate them. A notable trend is the correlation between compliance achievement and breach occurrence. In 2021, 73% of enterprises that had failed a recent compliance audit had a history of one or more data breaches. In contrast, among those that had passed all recent audits, only 41% had a breach history. In 2025, this gap widened: 78% of enterprises that failed audits had a breach history, versus just 21% of those that passed compliance. Put simply, in the last five years of the Data Threat Report study, the likelihood of experiencing a breach decreased by half among enterprises that passed all their compliance audits.

Correlation of compliance results and data breach history



The tendency to dismiss compliance audits as ineffective "checkbox" exercises reflects a failure to understand their purpose: to verify, at a given time, that controls are in place to prevent or minimize damage from data breaches. Achieving compliance is a critical step toward a risk-managed security program. However, compliance failure rates remain high, with 45% of 2025 respondents reporting a recent failed compliance audit, down slightly from 48% in 2021.

Organizations need to improve compliance performance. While compliance automation has gained traction among digital-native organizations such as SaaS providers that need SOC2 Type2 or ISO27K compliance, it has lagged in larger, established enterprises where audit processes remain manual. Automation efforts are hampered by hybrid enterprise infrastructure. With data repositories spread across cloud and on-premises locations, there is an urgent need for capabilities that enable unified risk identification and policy enforcement. Separate tooling for different environments is unscalable and can create hidden policy gaps that lead to data exposure and compliance failures.

Data on ransomware response planning provides a useful example of the need for improvement. Despite record costs associated with ransomware incidents in 2024, just 28% of respondents said they have a formal ransomware response plan. Even among those with a ransomware plan, few regularly practice its execution.

> *In the last five years of the Data Threat Report study, the likelihood of experiencing a breach decreased by half among enterprises that passed all their compliance audits.*

The Threat Landscape, Inside and Out

This year's report continues to encourage security, technology and commercial leaders to focus on factors within their control. While most enterprises cannot directly neutralize external adversaries, they can manage other risk factors.

Among attack types on the rise, malware maintains the top spot as it has since 2021, while phishing moved up to second from third on the list, and ransomware dropped from second to third. Regarding the most concerning threat actors, the top two are external attackers: Hacktivists remain at No. 1, followed by nation-state actors. Human error is third, down one spot from a year ago.

From an attack-chain perspective, all three top actors often initiate threats via phishing mechanisms that trick users into revealing credentials, allowing initial entry into the victim's network. However, external attackers are responsible for the actual damage, using various tactics, techniques and procedures including malware and ransomware to infiltrate and traverse networks and compromise data and systems.

Increasing Attack Types

	2021	2022	2023	2024	2025
#1 Attack Type	Malware	Malware	Malware	Malware	**Malware**
#2 Attack Type	Ransomware	Ransomware	Ransomware	Ransomware	**Phishing**
#3 Attack Type	Phishing	Phishing	Phishing	Phishing	**Ransomware**

Top Threat Actors

	2021	2022	2023	2024	2025
#1 Threat Actor	Malicious insiders	Human error	Human error	External attackers — hacktivists	**External attackers — hacktivists**
#2 Threat Actor	Human error	External attackers — hacktivists	External attackers — hacktivists	Human error	**External attackers — nation-state actors**
#3 Threat Actor	External attackers	External attackers — nation-state actors	External attackers — nation-state actors	External attackers — nation-state actors	**Human error**

Information security risk encompasses not just outside threats but also internal factors such as asset vulnerabilities and misconfigurations, user errors and the enterprise's level of ability to mitigate internal risks. Controls may reduce vulnerabilities. For example, transport encryption via TLS protects private data over public networks, user education can reduce insider risk, and data classification and access controls can mitigate the impact of lost or unavailable sensitive data. As previously noted, there is no shortage of discovery and enforcement tooling for enterprise data. However, adversaries and malicious insiders often pit assets against one another to further penetrate, exfiltrate or damage target enterprises.

Phishing-resistant MFA using passkeys appears to be taking hold. In 2023, about 40% of respondents reported using biometrics or passwordless authentication. In 2025, nearly 60% of respondents reported using biometrics, and 47% use passwordless authentication. Passkeys could eliminate certain attack types, such as credential stuffing or account takeovers using stolen credentials, because passkeys are cryptographically signed to each device.

MFA, Passkeys Defined

Strong multi-factor authentication requires a combination of something you know, such as a password, and something you have, such as a generated token. Time-based one-time password (TOTP) tokens securely generated via an authenticator application form the second factor in addition to a primary password.

Passkeys leverage private keys that are uniquely and securely associated with and stored on the user's specific computing device. Passkeys are phishing-resistant because they do not require the exchange of a password or other credential from the user.

While applications accessed via common PC or smartphone operating systems may be able to use passkeys, not all cloud resources or applications can do so. However, strong MFA adoption rates are improving — with "strong" MFA defined as a system where the second factor is a cryptographically based time-based one-time password (TOTP) or dynamically generated token driven by a challenge/response mechanism. In 2021, fewer than 16% of respondents used strong MFA for cloud application access more than half of the time. This has improved to 57% in 2025. Still, work remains. Failure to use MFA for privileged users was identified as the root cause for 13% of respondents' data breaches.

While adversaries may initially pursue insiders, enterprise data is the ultimate target. In ranked choice voting, respondents prioritized cloud storage, SaaS apps and cloud management infrastructure as the biggest targets for attack.

Digital Sovereignty as a Product of Data Security

Digital sovereignty has emerged as a principle for cloud adoption, allowing enterprises to manage sensitive and confidential information under specific controls in particular settings. It has arisen largely in response to the proliferation of data protection and privacy laws across various jurisdictions. Digital sovereignty enables enterprises to maintain control over their data security and privacy independent of external organizations, governments or service providers. Several levels of digital sovereignty exist, depending on legal, security or risk management requirements.

The rapid evolution of GenAI is further prompting enterprises to incorporate sovereignty considerations into the digital transformation journey. As applications become more AI-driven, enterprises must balance expediency and flexibility as digital sovereignty requirements influence decisions regarding GenAI development and implementation.

Sovereignty Levels

Under the broader umbrella of digital sovereignty, one of three levels is often applied to a workload depending on security or risk management requirements:

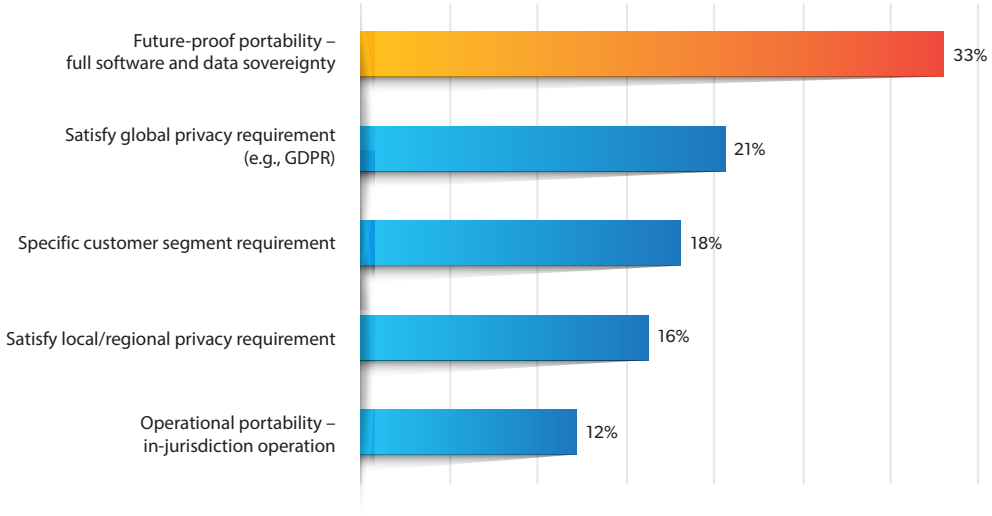
Level 1 – Data sovereignty: Enterprises control their own data in the jurisdiction. Via strong data encryption or designated data residency, data sovereignty ensures that enterprises can fully control and repudiate challenges to their data.

Level 2 – Operational sovereignty: In addition to data sovereignty, enterprises have the discretion to specify the national location or other requirements of personnel operating cloud infrastructure.

Level 3 – Software sovereignty: In addition to operational sovereignty, software sovereignty enables an enterprise to take its data from one IaaS or PaaS platform and work with it in the same way via open-source or alternative equivalents.

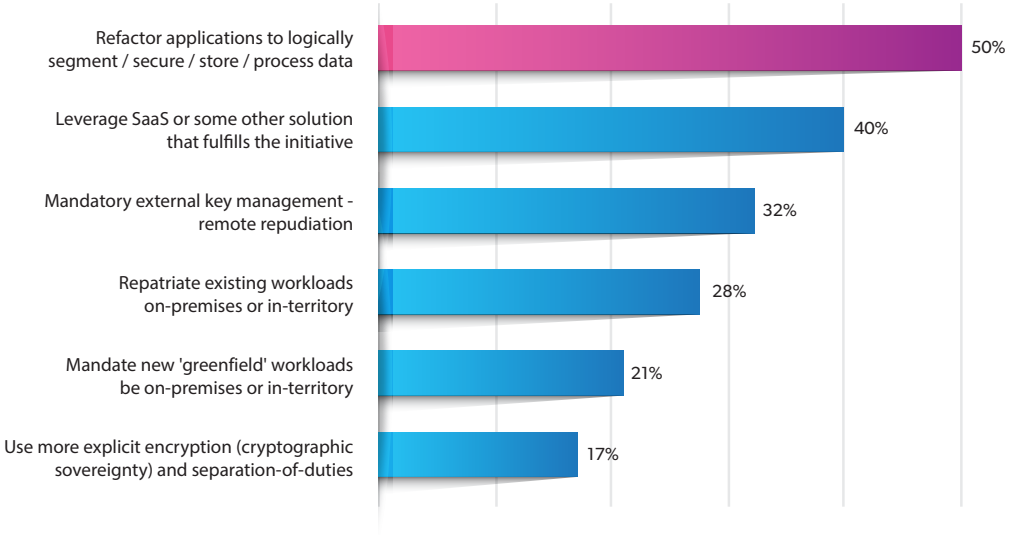
Overall, respondents showed preference for flexibility and a willingness to change. Nearly one-third of respondents said future-proof portability and software sovereignty was the top driver for digital sovereignty initiatives.

Primary drivers of sovereignty initiatives



Enterprises also expressed a willingness to refactor their applications to achieve sovereignty. Half of all respondents said that application refactoring was the primary method for achieving sovereignty.

Methods for accomplishing sovereignty initiatives



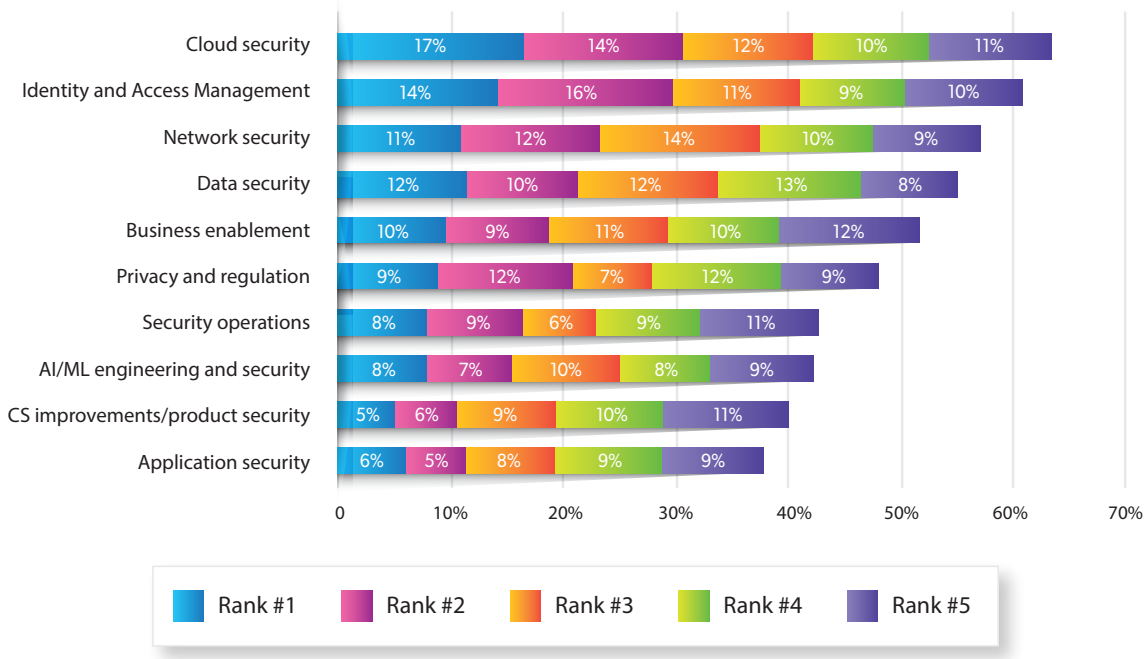
The shifting regulatory landscape may create apprehension, as overlapping cybersecurity regulations can arise from various jurisdictions at the industry, provincial and national levels. For example, major global financial services firms operating in New York must comply with national regulators such as the US Securities and Exchange Commission and Federal Trade Commission, as well as local regulators such as the New York State Department of Financial Services. The same multinational organizations must comply with regulations such as the Network and Information Security Directive 2 and the Digital Operational Resilience Act for their EU operations. Geopolitical concerns are also increasingly influencing digital sovereignty considerations.

> *As applications become more AI-driven, enterprises must balance expediency and flexibility as digital sovereignty requirements influence decisions regarding GenAI development and implementation.*

Cloud Devops Evolves to Platform Engineering

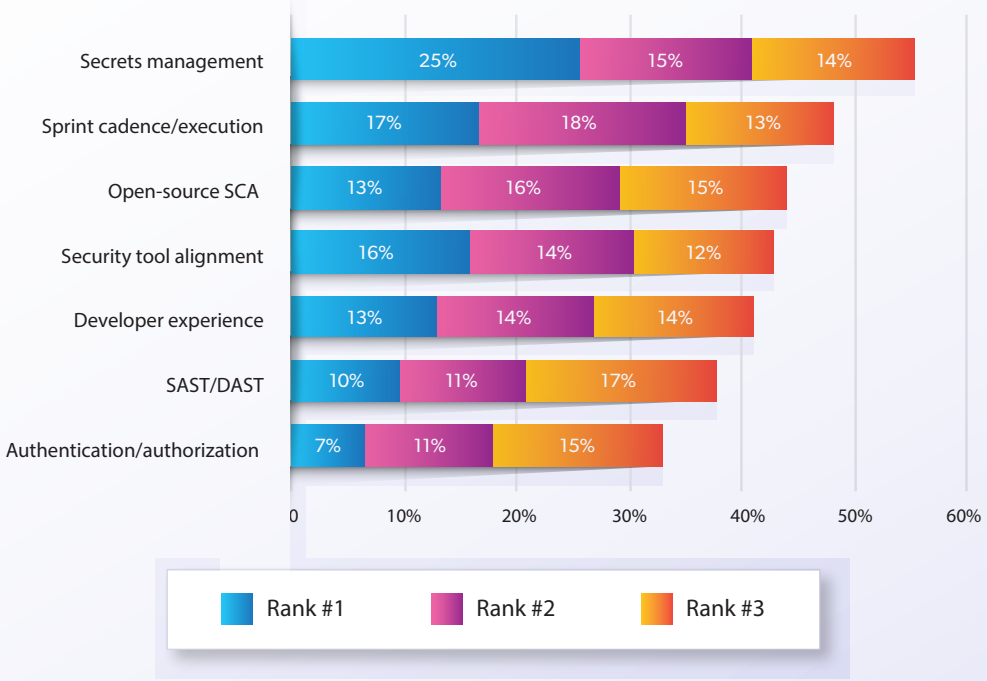
In this year's Data Threat Report, enterprises named cloud security as their top concern, with 64% of respondents citing it as their most pressing security discipline in ranked choice voting. This is understandable since both SaaS data and cloud storage remain top attack targets. In ranked choice voting, 29% of respondents also prioritized cloud management infrastructure. Platform engineers and operators play a crucial role in managing and deploying data assets via development pipelines.

Most pressing security disciplines



Among platform engineering teams, secrets management emerged as the top DevOps challenge. Secrets are often "bearer tokens" — anyone who has them can access the given resource. Secrets can include various assets — signing keys, passwords, tokens and certificates — and their loss or compromise can lead to severe damage. For example, an adversary with a stolen signing key may create or falsely authenticate malicious code, bypassing many detection and response mechanisms.

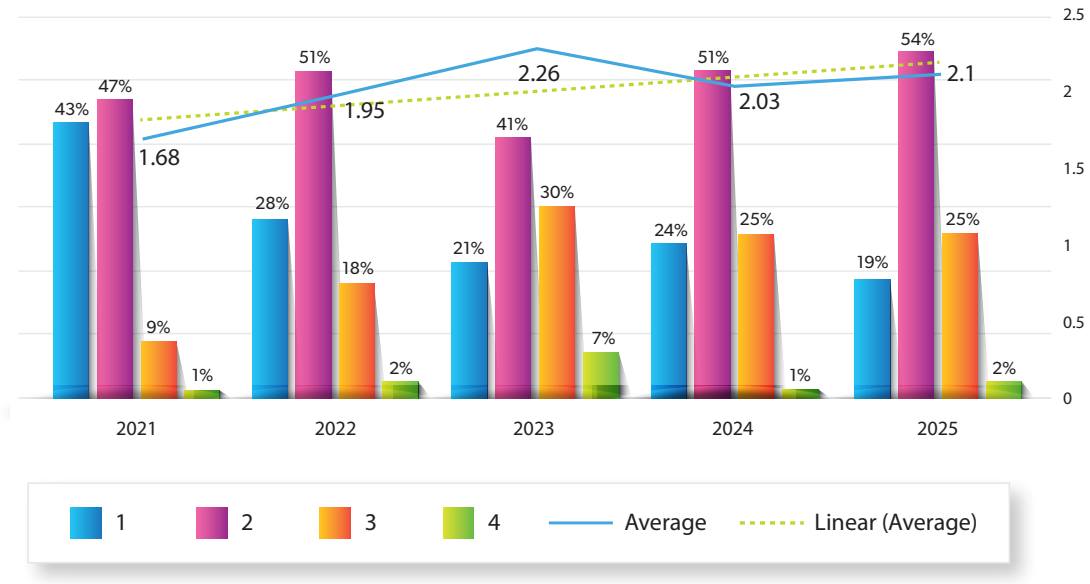
Top DevSecOps challenges



Secrets can include various assets — signing keys, passwords, tokens and certificates — and their loss or compromise can lead to severe damage.

The complexity of cloud environments compounds the challenge. This year's Data Threat Report shows continued multicloud adoption, with 76% of respondents using two or more clouds. Differences between various cloud products — even those from a single provider — further exacerbate the problem. The 451 Research Cloud Price Index, which tracks pricing for a variety of cloud services, tabulates more than 100,000 SKUs for a single public cloud provider. While cloud providers may offer similar features in computing, database, networking and security, implementations vary considerably; expertise in one provider does not guarantee proficiency in another.

Number of IaaS cloud providers in use

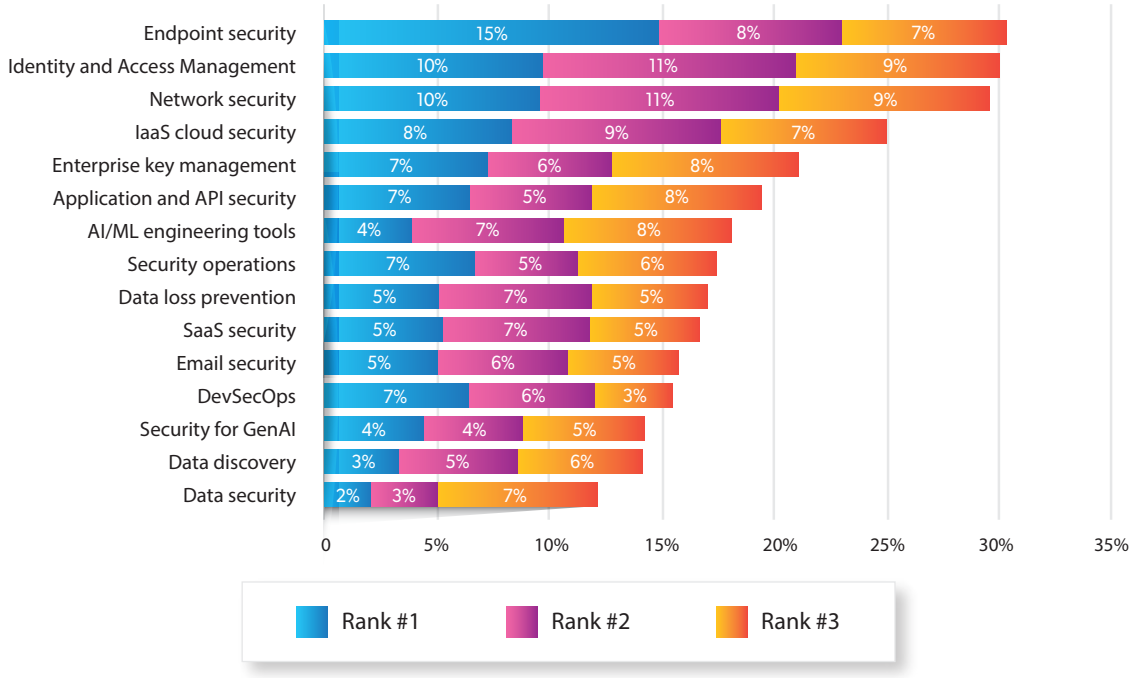


Enterprises are on an evolving cloud journey. Many organizations have embraced SaaS, with 64% of enterprises in 2025 reporting 26 or more SaaS vendors. Virtually every enterprise SaaS vendor now incorporates GenAI capabilities and integrates with other major SaaS tools. The pathways for sensitive enterprise data through SaaS environments are numerous, complex and difficult to trace. Meanwhile, the evolution from DevOps to platform engineering further separates developers from site reliability engineers and infrastructure owners, driving increased focus on core competencies. Many enterprises may not have realized the benefits of bringing developers and operators together. As cloud architectures increasingly become serverless or API-driven, cloud security must align with application security principles.

Threat Reality Versus Investment Priorities, and the Need for Alignment

Given the pace of organizational and technological change, technology and security leaders must proactively modernize and secure their businesses. Alignment is crucial for understanding needs, rationalizing investments and measuring effectiveness. In ranked choice voting, 64% of enterprises identified cloud security as the most pressing security discipline, followed by identity and access management (IAM) with 61% and network security with 57%.

Security technologies deemed most effective in protecting sensitive data from cyberattacks



As a spending priority, security for GenAI debuted at No. 2, just behind IaaS cloud security in ranked choice voting.

However, a significant disconnect exists regarding the perceived effectiveness of security tools in the context of enterprise practices and risks. Some discrepancy is to be expected; security for GenAI is a relatively new category, and attacks compromising integrity or trustworthiness may not cause the same immediate harm as breaches in confidentiality or ransomware attacks that compromise availability. Even with ranked choice voting and multiple selections, just 14% identified security for GenAI as effective, while network security, IAM and endpoint security hovered around 30%.

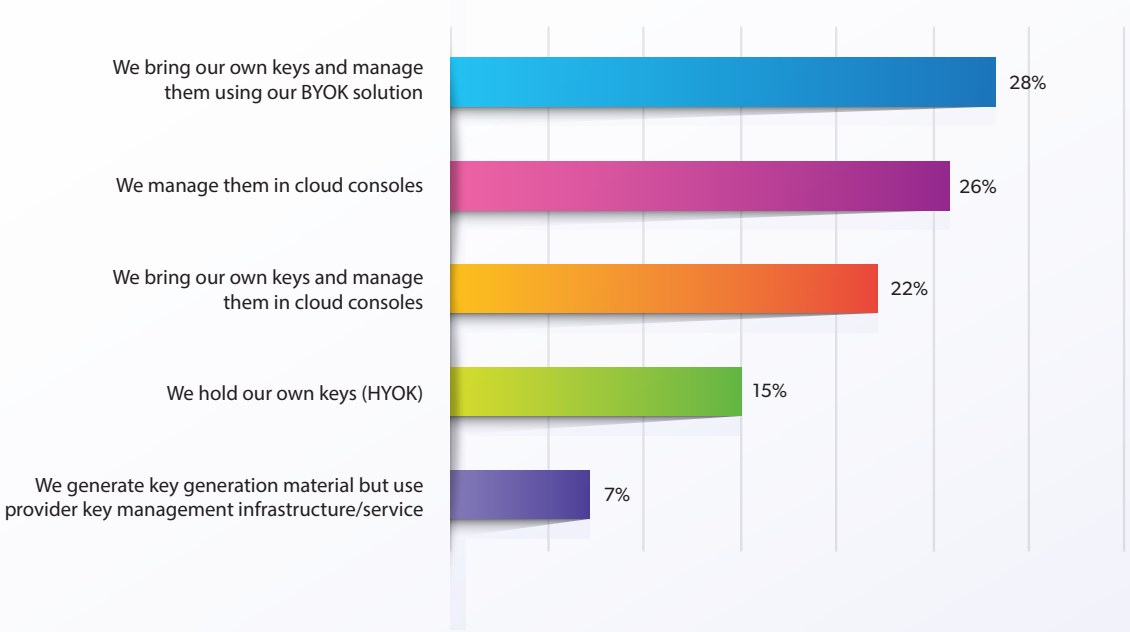
Other disconnects may stem from shifting ownership. Secrets management is a top issue for DevOps and platform engineering, yet just 16% of respondents said that their DevSecOps tooling was effective. Since secrets management is integral to platform engineering and development teams, security teams may lack the visibility to verify secrets management effectiveness.

Organizations use layered security approaches, leading attackers to use a blend of tactics, techniques and procedures, such as phishing preceding a malware payload. It is natural to use security tools and controls that match each step of an attack, with network and endpoint security tools historically applied at perimeters to detect and prevent the first steps of an attack.

While network and endpoint controls are essential, improvements are needed, particularly in data security and discovery. Some of the difficulty stems from complexity and duplication: As previously noted, most enterprises have five or more tools for data discovery and five or more enterprise key managers. Even within tools, complexity is prevalent. For example, organizations must choose between various methods for managing encryption keys. Most commonly, they bring their own keys that are managed in private or cloud environments. However, 48% use cloud consoles. In multicloud environments, controls such as data encryption can also become fragmented and siloed.

A significant disconnect exists regarding the perceived effectiveness of security tools in the context of enterprise practices and risks.

Methods for controlling encryption keys



For enterprises, efficacy depends not only on tool design but also on adoption and implementation processes. In fast-moving technology environments, controls must provide the flexibility required to meet business needs.

Conclusion

The Data Threat Report survey results should encourage organizations to improve their security posture. The emergence of GenAI reinforces the importance of data security as a foundation for enterprise value. Organizations that securely manage data throughout its life cycle and across hybrid infrastructures gain a competitive advantage that extends beyond data protection. This change has been in progress for some time. The need for improved data protections to address regulatory mandates such as data sovereignty should have already spurred improvements. The risks of quantum computing should be driving enhanced crypto agility. Organizations face a convergence of pressures that highlight the need for foundational improvements — not just to protect data, but to maximize data's potential to drive productivity and competitiveness.

Technology changes must align with an organization's mission and vision. GenAI represents a new pillar in the structure of many organizations. Effective data security management enables pillars such as GenAI to deliver their full value to the organization via whichever infrastructure proves most suitable.

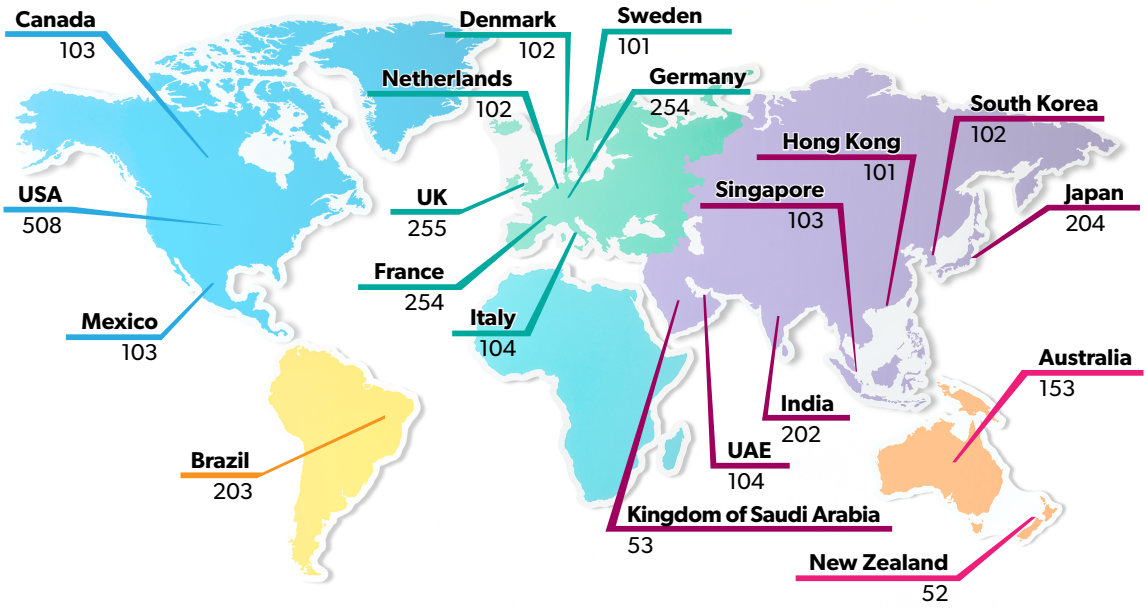
The study results suggest several practical next steps:

- **Application security requires a clear picture of the API landscape:** To protect its applications, an enterprise must conduct a comprehensive inventory of existing APIs, which may number in the thousands.
- **Data identification and control are key:** Data assets must be identified and understood for effective management and deployment. This understanding must span cloud and on-premises environments, with unified operational control to tame complexity. For many, this will mean deploying a data security platform.
- **Data protection must scale:** Fragmented controls and management infrastructure cannot meet the needs of modern, hybrid infrastructure. Tooling is necessary to translate and unify protection policies across dissimilar controls and protect against errors and misconfiguration. Data security posture management capabilities have become a critical requirement for effective risk mitigation.
- **Sovereignty is crucial:** Future-proof portability may determine which platforms remain usable, particularly in heavily regulated industries and jurisdictions.
- **Consolidation is necessary:** The number and complexity of security tools performing similar activities taxes security teams. Simplification and automation are needed.
- **Data security next steps:** Control capabilities must be unified and strengthened. Data protection must seamlessly extend across on-premises and cloud environments to enhance encryption and simplify security management. Hybrid is the new reality.

While this year's survey results indicate improvements in security posture, much more is needed to elevate operational data security to fully support the capabilities of emerging technologies such as GenAI and to pave the way for future innovations.

About this Study

This research was based on a global survey of 3,163 respondents fielded via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million and with US$100 million-$250 million in selected countries. This research was conducted as an observational study and makes no causal claims.



Revenue	Number of Respondents
$100m to $249.9m	187
$250m to $499.9m	802
$500m to $749.9m	842
$750m to $999.9m	770
$1 Bn to $1.49 Bn	226
$1.5 Bn to $1.99 Bn	111
$2 Bn or more	225
Total	3,163

Industry Sector	Number of Respondents	Industry Sector	Number of Respondents
Retail	301	Other	170
Manufacturing	291	Travel / Hospitality	166
Healthcare	274	Pharmaceuticals	164
Financial Services	258	E-commerce	149
Government	255	Automotive	144
Technology	217	Education	137
Energy & Utilities	198	Telecommunications	128
Transportation	187	Biotechnology	124
Total			3,163

THALES

Building a future we can all trust

For contact information, please visit
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/data-threat-report