2026 EDITION

THALES

CYBERSECURITY

DATA THREAT REPORT

Data security in the agentic age: AI is the new insider threat

cpl.thalesgroup.com

#2026DataThreatReport

Table of Contents

Conducted by

S&P Global
Market Intelligence

Source: 2026 Data Threat Report custom survey from
S&P Global Market Intelligence 451 Research, commissioned by Thales.

Introduction

Data security has taken center stage as the success of enterprise AI initiatives increasingly hinges on consistent, controlled access to proprietary organizational data sources. The **2026 Thales Data Threat Report** examines the complex calculus that organizations must undertake to enable innovation while securing their most valuable asset — their data.

The proliferation of AI and agentic operations is compounding stress on data management and security, as reflected in a 50% year-over-year increase in the proportion of respondents allocating new security budgets specifically for AI. Organizations are struggling with data quality and security as they work to safely deliver access to the raw material from which AI value is built. As agentic applications gain access to greater volumes of data, organizations must improve data security and management practices to ensure that AI does not become a new insider threat.

Organizations face pressure to accelerate their operations, but these efforts are challenged by complexity in security operations exacerbated by sprawling security toolsets and increasingly complex hybrid and multicloud IT infrastructure. AI is forcing the integration of new elements, such as chat interfaces and Model Context Protocol servers, that security teams are wrestling to secure. The threat landscape is also shifting as attackers employ AI and quantum computing risks loom ever larger. Further complicating matters, the AI ecosystem is constantly shifting under security teams' feet.

While there are positive trends in this year's Data Threat Report, much more must be done to secure organizations' most sensitive data. The report captures the insights of more than 3,100 respondents from 20 countries. Most have a fully multicloud operating model, with data and applications located across different cloud provider venues, although not all can be said to have actively embraced this reality.

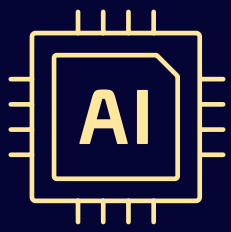
Comparing this year's survey results with previous years reveals notable areas of concern. Significant volumes of sensitive data in the cloud remain unencrypted. Cloud-based applications and cloud management infrastructure remain key targets for attackers. The complexity of security operations in the cloud can be challenging, particularly given staffing constraints. As the name suggests, cloud security demands expertise in both cloud operations and security applications, and both capabilities are in short supply. Added to this is the pressure to deliver ever greater data volumes and computational power for AI applications. As we enter the age of agentic operations, security practitioners will need to address access, authentication and authorization on an even greater scale.

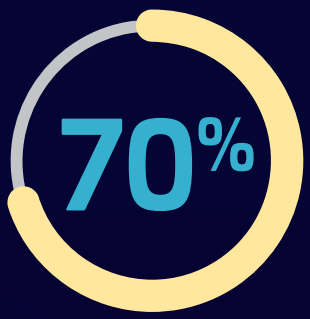
Key findings

Security priorities are changing with AI

Spending on AI security is rising –

30% of organizations now have a dedicated budget for AI security (up from 20%), but more than half **(53%)** still fund AI security using their existing security budgets.





The speed of AI change within AI ecosystems is top of mind when it comes to AI security with 70% citing rate of change as the top AI risk.

61% report their AI applications are being targeted by attackers, with sensitive data being the leading target.

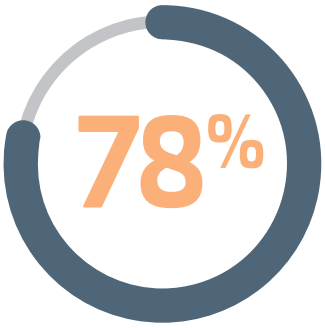
AI-fueled attacks emerge as a prominent threat - **59%** have seen deepfake attacks and

48%

have experienced reputational damage, as a result of AI-generated misinformation.

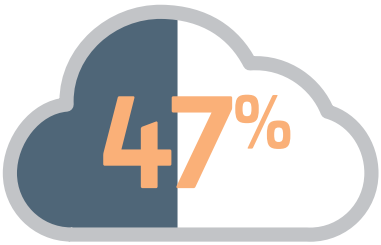
report AI generated misinformation and deepfakes showed the second highest attack increase.

Data protection is critical in the AI age



of the C-suite reported no breach, versus **57%** of their IT and security teams.

52% regard identity and access management as the most pressing security discipline, as attackers exploit credentials.



Only about half of sensitive data in the cloud is encrypted.

have complete knowledge of where their data is stored.

50%

rank secrets management as the leading concern in application security.

Complexity limits clear insight into data security posture

Security complexity creates greater risk –

tool counts are high with **77%** having five or more data protection tools.

7 tools are the average for data protection and monitoring

46% have five or more key management systems

Only 39% are confident in their understanding of data security tools

28% cite Human error as the leading cause of breach, but **63%** rank nation state attackers as one of top three greatest concerns.

Audit failures are linked to higher breach risk –

Only 6% of organizations that failed an audit reported no past breaches, compared with **30%** of those that passed.

Cloud is a significant attack target

Cloud assets are the top three attack targets –
as respondents cited

35% cloud storage, **34%** cloud applications and **32%** cloud management infrastructure as the top three attack targets.

Credential theft is the leading attack technique against cloud infrastructure –

67% are seeing credential theft and misappropriated secrets increasing.

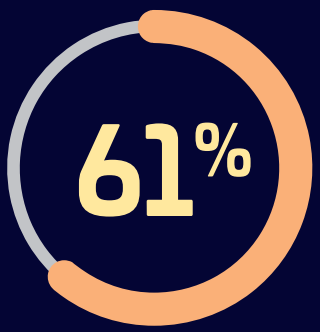
Rising geopolitical risk is reshaping data sovereignty

54% are pursuing reworking and refactoring of application and data architectures as their main focus in achieving sovereignty objectives.

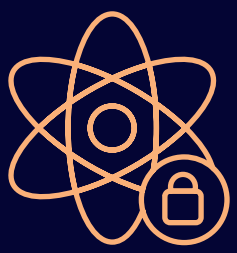
36% believe cryptographic protections such as encryption and key management are sufficient to achieve data sovereignty.

Future risks are here today

Quantum concerns shift to the reality of harvest now, decrypt later (HNDL),



cited as the top concern.



Organizations are moving to mitigate quantum risk

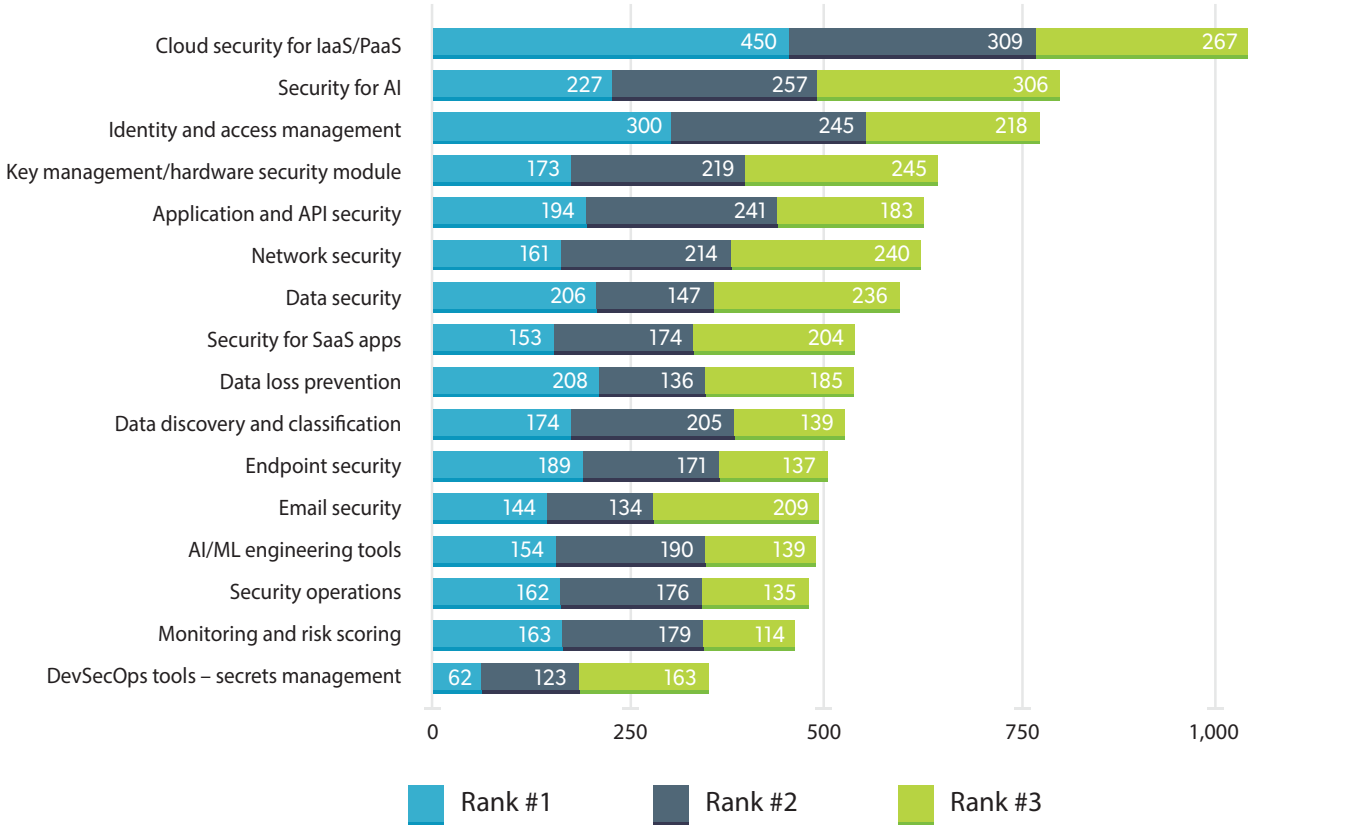
59%

are prototyping and evaluating Post-Quantum Cryptographic (PQC) algorithms.

Security pressures expand with AI and agentic operations

Security teams are grappling with rapid change stemming from enterprise adoption of AI, and the addition of AI agents is further complicating an already complex landscape. In a recent 451 Research Voice of the Enterprise study on agentic AI, **more than a third of enterprises (34%) reported that embedded agents are already in use,** and a majority (73%) said they expect to use them within 12 months. The velocity and volume of data use increases dramatically with agentic applications, and enterprises are already struggling with data management and security. Only a third of respondents to the Data Threat study said they have complete knowledge of where their organization's data is stored, and only slightly more (39%) said they can classify all their data — a necessary step to effective data protection.

SECURITY SPENDING PRIORITIES



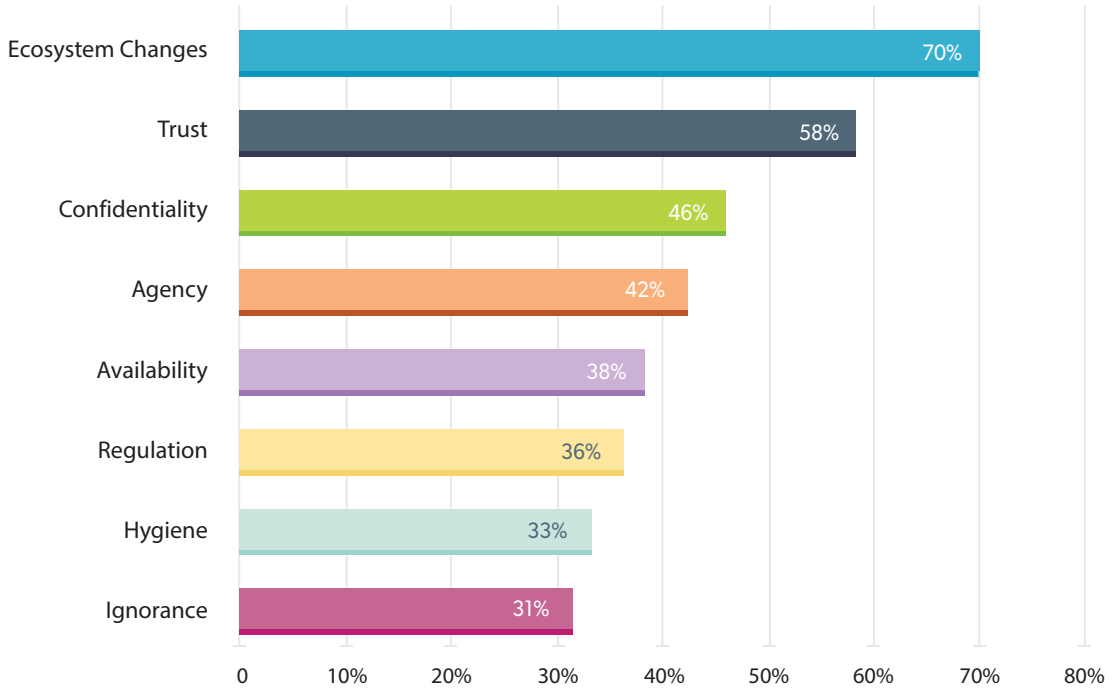
Note: All charts displayed in this document are from S&P Global Market Intelligence 451 Research's 2021-2026 Data Threat custom surveys.

Security for AI is challenging, particularly given the pace of technology evolution. **Notably, rapid change in the AI ecosystem is the leading AI-related security concern: 70% of respondents ranked it among the top three sources of risk.** It is difficult to secure a moving target, and AI agents will only increase the number and velocity of such targets. Among AI- and LLM-based attacks, respondents reported the greatest growth in those aimed at exposing sensitive data. Understandably, AI security spending ranks second-highest in priority, trailing only cloud security, among 17 listed areas. One in four respondents ranked AI security among their top three spending categories.

It is difficult to secure a moving target, and AI agents will only increase the number and velocity of such targets.

AI is also being used by attackers, requiring changes in defense tactics. AI-generated misinformation, including deepfakes, ranks second among AI attack types on the rise. Infrastructure supporting AI applications and data also remains a prime target for attackers: Cloud-based assets remain the top targets in this year's data. Given the large volumes of data used by AI and the increases in discoverability associated with AI agents, encryption is mandatory. If an organization's stakeholders cannot find, classify and secure valuable data, agents will likely find ways to access it, with unpredictable results. In many ways, **AI represents the new insider threat.**

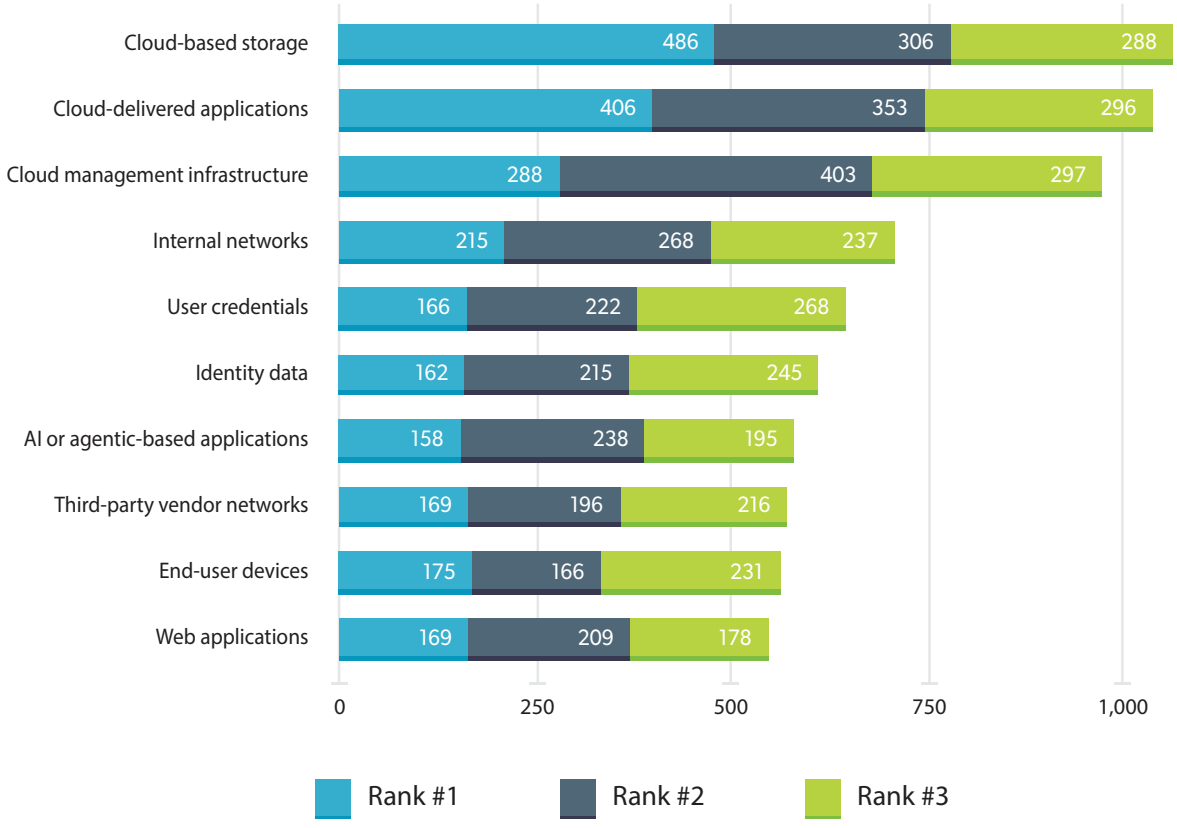
MOST CONCERNING AI SECURITY RISKS



The data threat landscape

The study results help to characterize the data threat landscape. Organizations are observing changes in attacks and working to mitigate new tactics. In this latest survey, **cloud-based assets again represent the top three attack targets,** with the greatest proportions of respondents identifying cloud-based storage (35%), SaaS applications (34%) and cloud management infrastructure (32%) among the top three targets of cyberattacks. Further down the list, shifts in the rankings mirror rising concerns about identity security. User credentials rise from eighth on the list a year ago to fifth, identified by 21% as a top-three target. Meanwhile, identity data climbs from 10th to sixth, with 20% placing it in their top three.

TOP ATTACK TARGETS

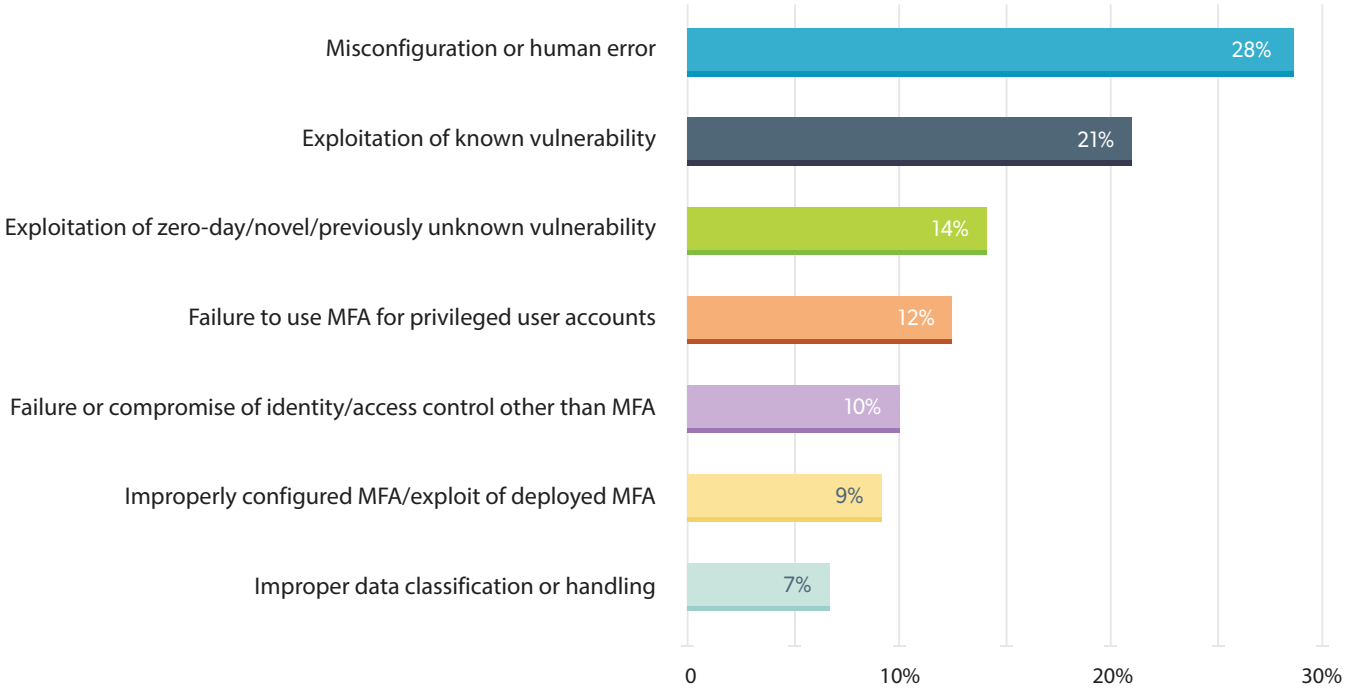


... cloud-based assets again represent the top three attack targets, with cloud-based storage leading at 35% ...

This year's results reflect relative consistency in the prevalence of audit failures and reported breaches. Just over half indicated no history of breaches: 54% reported no cloud breaches, and 57% reported no on-premises breaches. A similar proportion (58%) reported passing all compliance audits in the last 12 months. Continuing the pattern of previous years, those that fail audits are much more likely to report a breach. Among organizations that failed an audit, only 6% reported no breach history, whereas that figure rises to 30% among organizations that passed all audits.

Awareness of breach history may be an issue in some organizations, as the data show differences in reported breach history across job roles. Senior executives are less likely to identify breaches than those in management or practitioner roles. More than three-quarters (78%) of CEOs, presidents and managing directors reported that their organization has not experienced an on-premises breach, while survey-wide — including responses from all levels of practitioners — the figure falls to 58%. The difference for cloud breaches is smaller but still notable: 62% of executives reported no cloud breach history, versus 54% of the total survey population. These discrepancies can have material impacts on how security budgets are prioritized.

MOST COMMON CAUSES OF DATA BREACH



Based on 1,998 respondents whose organization experienced a data breach.

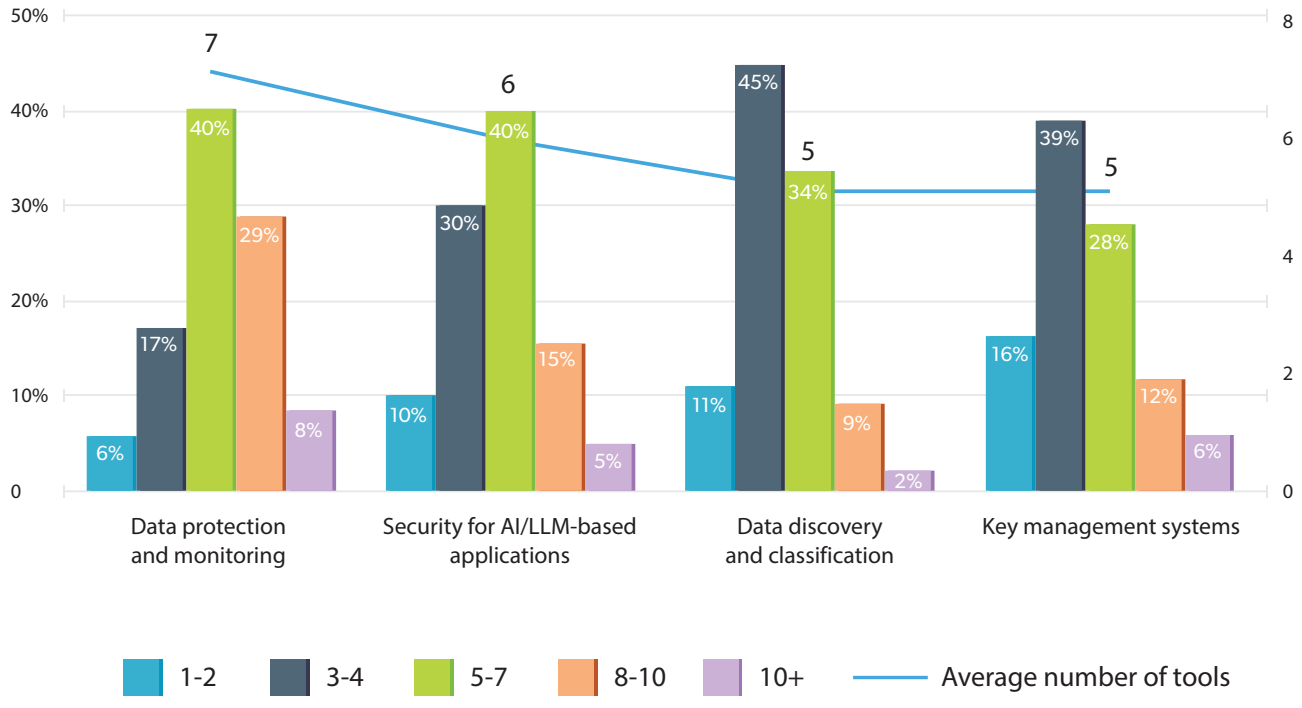
Human error remains the leading cause of data breaches (28%), substantially ahead of the next two most common causes — exploitation of known and unknown vulnerabilities. This suggests that operational issues are among the most significant risk contributors. It also highlights the need to identify and mitigate the human side of security challenges, which in turn requires a perspective shift in security mitigation priorities, since human error is paradoxically not cited as the leading security concern.

Complexity impacts security effectiveness

The detrimental impact of complexity on security operations has been a consistent theme throughout the report's history. This year's survey expands the examination of a major contributor to complexity: security tool sprawl. Tool sprawl worsens complexity by increasing the number of systems that security teams must monitor and maintain. It demands coordination and correlation of results and alerts from various sources, and it can create gaps in coverage. Given that human error is the leading reported cause of breaches, operational complexity may be a major causal factor.

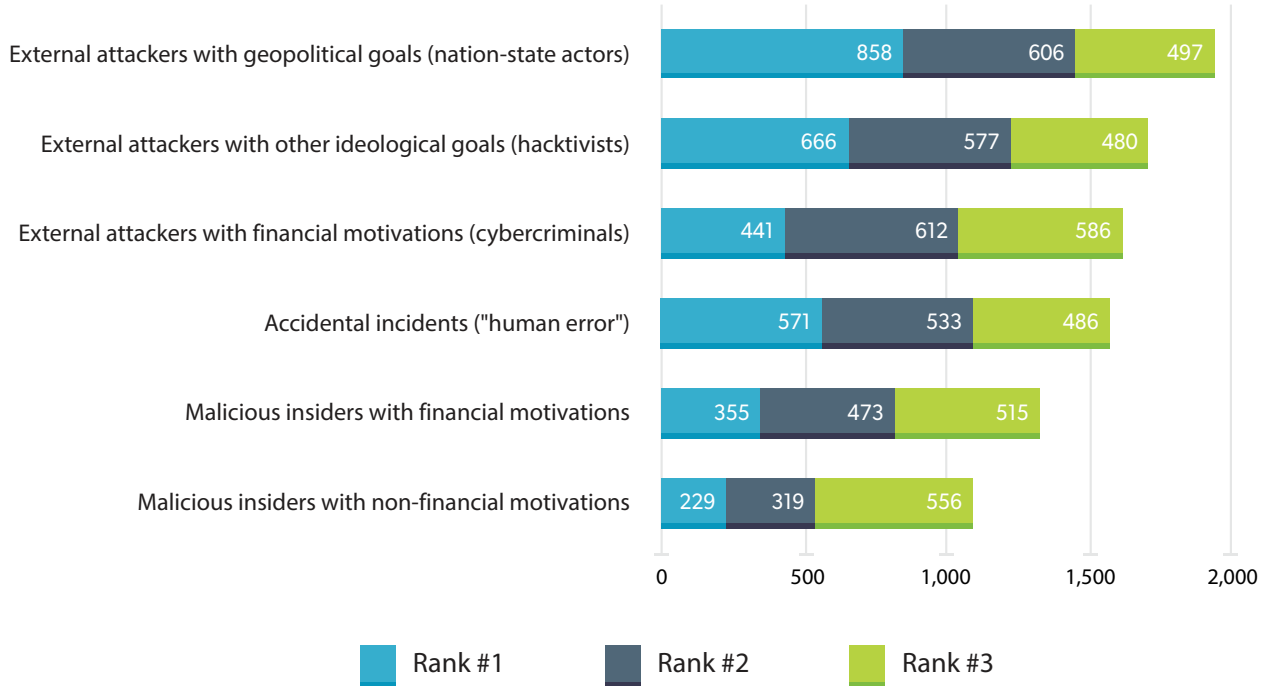
Organizations may increase tool counts both organically and inorganically. In the former case, overlapping tools may be acquired by different teams or for different projects. In the latter case, company mergers and acquisitions may cause multiple tool sets to roll up to integrated security teams. Whatever the cause, the study results show high levels of tool sprawl. The most notable area is in data protection and monitoring, where organizations reported an average of seven tools, and 73% have five or more. This is particularly concerning given the increased focus on data security that accompanies growing AI adoption. AI security tools exhibit the second-highest level of sprawl, with an average of six tools per organization, and 60% of organizations reporting five or more tools in use.

NUMBER OF DATA DISCOVERY, CLASSIFICATION AND KEY MANAGEMENT SYSTEMS IN USE



And yet, there is resistance to consolidating security tools. A decision to remove any security controls should be subject to careful evaluation. However, surprisingly, when asked about the reason for their resistance to tool consolidation, 83% of respondents cited a perceived lack of compatibility or capability in other available tools. This is doubly concerning because only 39% cited high confidence in their understanding and knowledge of existing tools. This implies a contradiction in thinking about tool consolidation — a conviction that alternative tools lack capability, coupled with a general shortage of knowledge about those very tools — and may indicate that security decision-makers are unlikely to change what they do not understand.

THREAT ACTORS OF GREATEST CONCERN

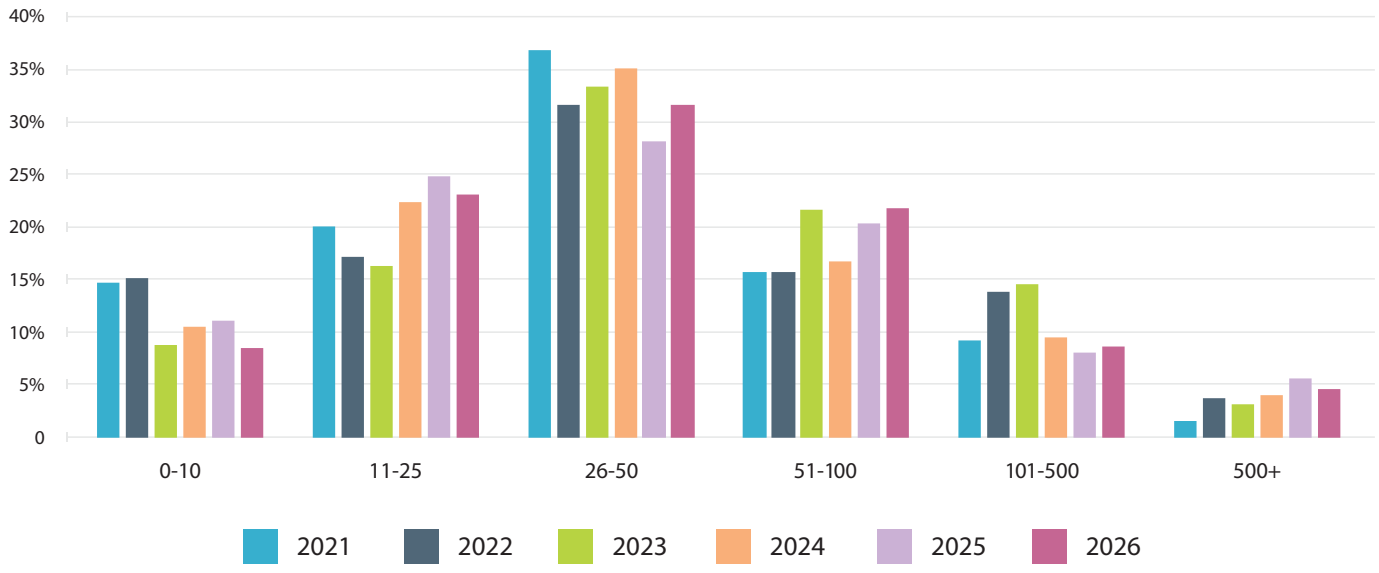


Regardless of the reasons for resistance, tool consolidation is necessary to simplify and scale security operations. **Organizations are becoming ever more hybrid and complex — using more cloud providers and working to secure more applications.** This growing complexity recalls another misalignment in security thinking reflected in the survey results: As noted above, while the leading security concern is nation-state attackers — cited as a top-three issue by 63% of respondents — human error remains the leading cause of data breaches. Reducing complexity reduces the chance for human error among security teams. And to be successful, tool consolidation must not only simplify operations but also support scaling to span modern enterprise infrastructure.

Cloud data is under attack

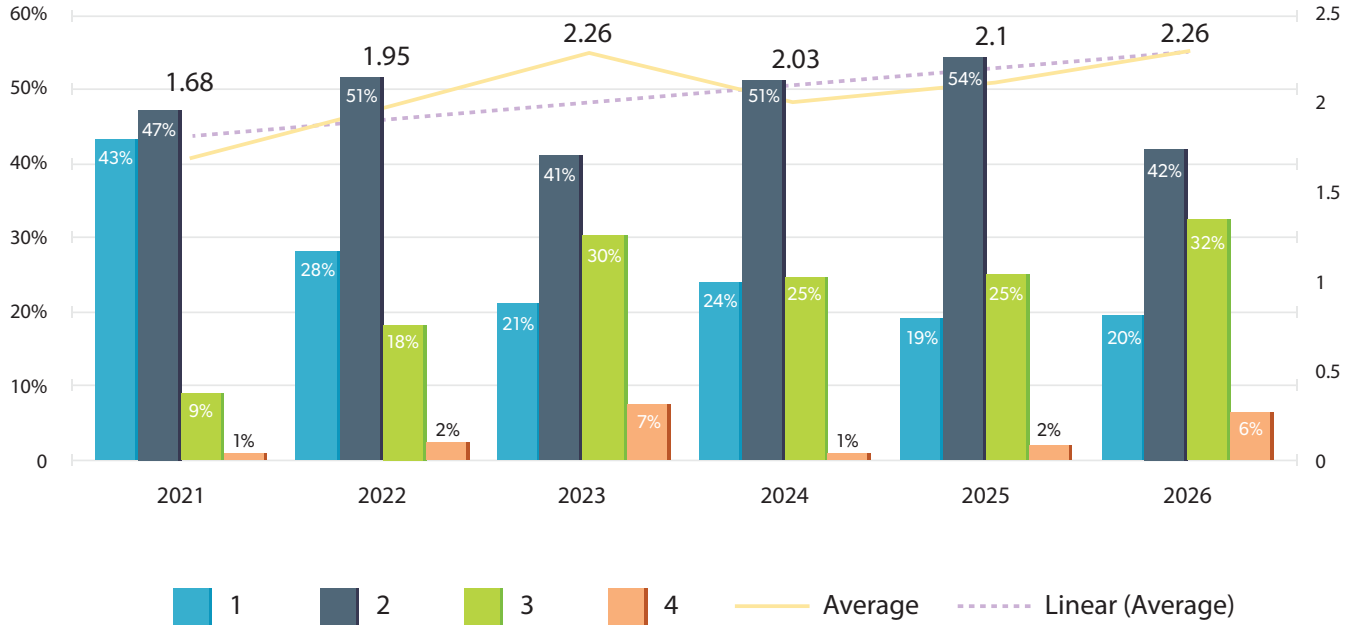
Enterprises increasingly rely on cloud infrastructure for core business operations, and attackers continue to target the critical applications and data that reside there. As noted above, for the third consecutive year, respondents identified cloud-based assets as the top three attack targets. The tendency toward multicloud infrastructure further strains security teams since they must be proficient not only in securing complex cloud computing structures, but also in extending that security across multiple providers' environments. Indeed, the average number of cloud providers in use has ticked up again in the latest survey to 2.26, and the average number of SaaS applications has increased to 89. **Cloud security is once again the top security spending category, indicating that enterprises are working hard to secure this critical resource.**

NUMBER OF SAAS APPS IN USE

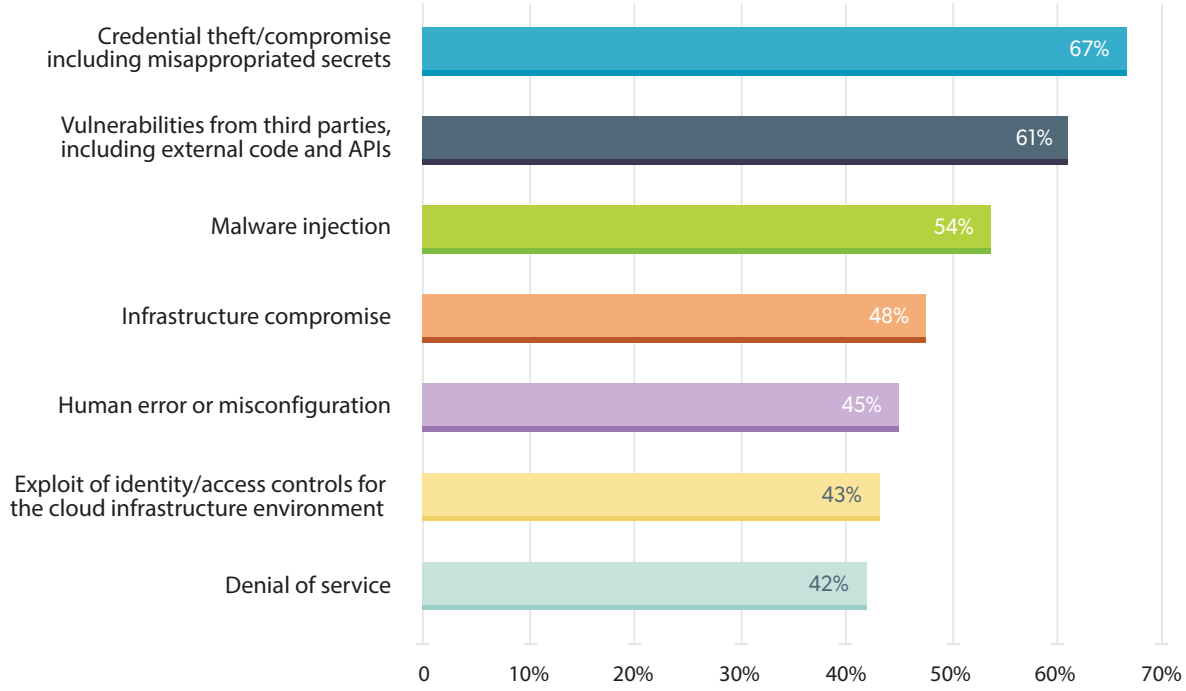


Compounding the challenge, cloud security skills are in short supply. Survey respondents identified cloud skills as the second-most-pressing security discipline, behind only identity and access management skills. The pressure on both identity and cloud security is reflected in the types of attacks targeting cloud management infrastructure. Credential theft/compromise is the most widely cited type of attack on the rise, underscoring the need to adopt sophisticated identity protection measures.

NUMBER OF IAAS CLOUD PROVIDERS IN USE



CREDENTIAL ATTACKS LEAD AGAINST CLOUD MANAGEMENT INFRASTRUCTURE

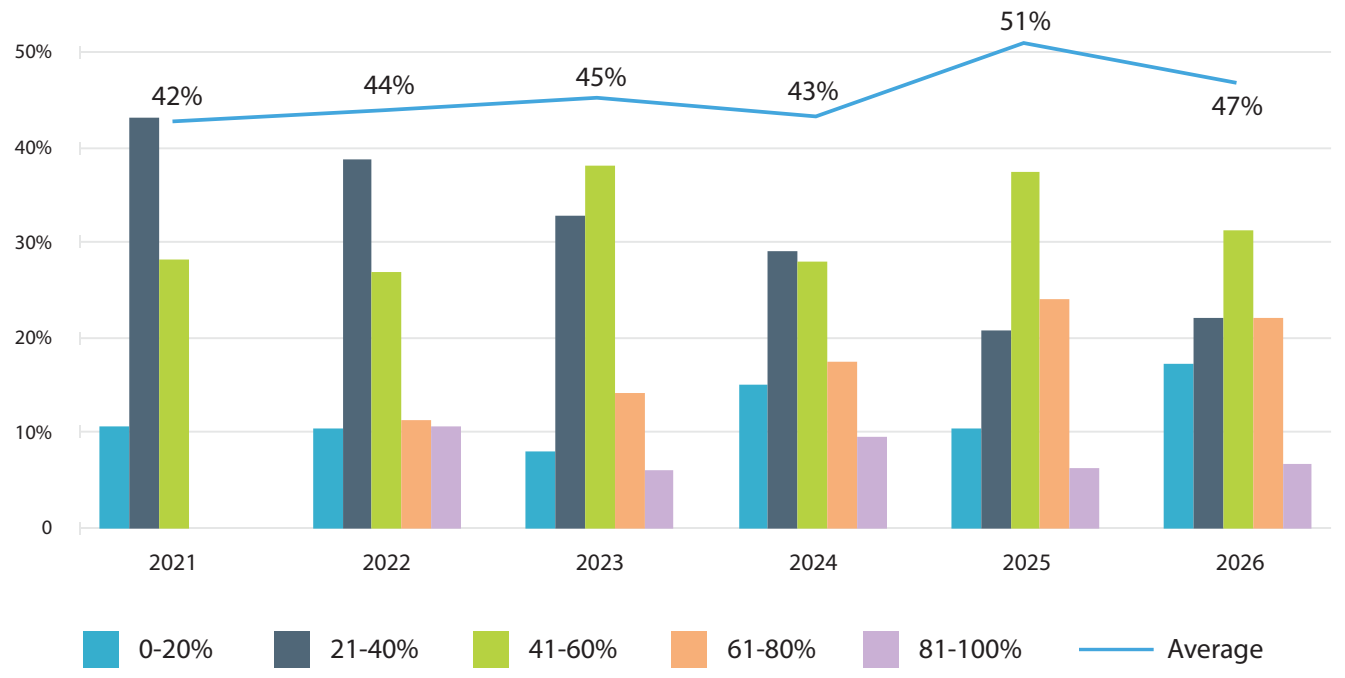


Based on 988 respondents reporting an increase in cloud management infrastructure attacks.

Notably, malware injection has risen to the third spot, from fourth a year ago, in the list of growing cloud attack types. This shift reflects attackers' increasing use of software supply chain attacks and malicious modules and plugins. Countering these attacks requires advanced skills and enhanced data protection capabilities. Data visibility and access protections have become critical, as credential compromise can bypass user access controls.

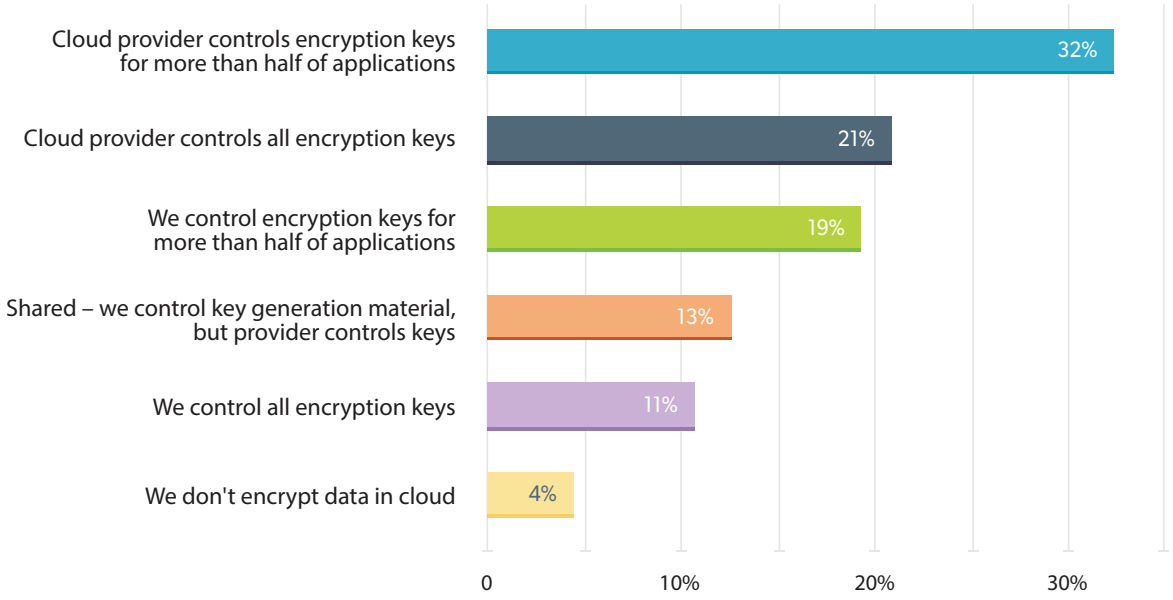
Adding context, the survey reveals a large and growing quantity of sensitive data in the cloud, much of which is not well protected, raising the risk of exposure. The results show a concerning lack of progress in protecting the enterprise's most precious asset — data. **The average share of cloud data categorized as sensitive holds steady at just over half (51%), while the average proportion of sensitive data protected by encryption has dipped slightly to 47%.** As AI applications are granted access to more data and agents gain greater autonomy in data handling, protections must improve. To effectively defend against increasingly powerful, AI-assisted attacks, organizations must be able to locate and classify all their data resources.

PROPORTION OF SENSITIVE CLOUD DATA ENCRYPTED



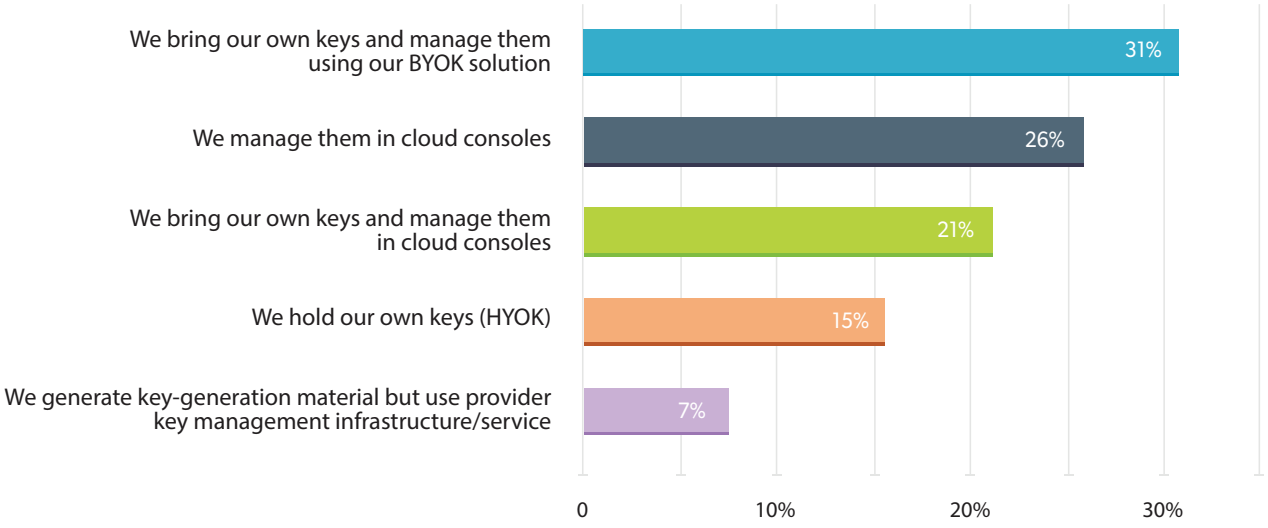
This year's results show little progress in the maturity of organizations' data security capabilities. A majority of organizations (53%) reported that cloud providers control the data encryption keys for more than half of the applications in their environments. That represents a missed opportunity to more effectively secure sensitive data and also reflects unnecessary complexity in data security operations. Without the ability to externally and centrally control encryption management, organizations are subjected to the added complexity of managing keys in multiple environments.

LOCUS OF CONTROL FOR ENCRYPTION KEYS



The survey shows a slight increase year over year in the proportion of organizations bringing their own keys for data encryption. Just under a third (31%) are using a "bring your own keys" (BYOK) approach and managing keys in their own systems. That represents a positive step in reducing the operational complexity of securing data. However, there is room for improvement, with a quarter relying on cloud consoles for key management.

METHODS OF MANAGING ENCRYPTION KEYS



Quantum risk realities

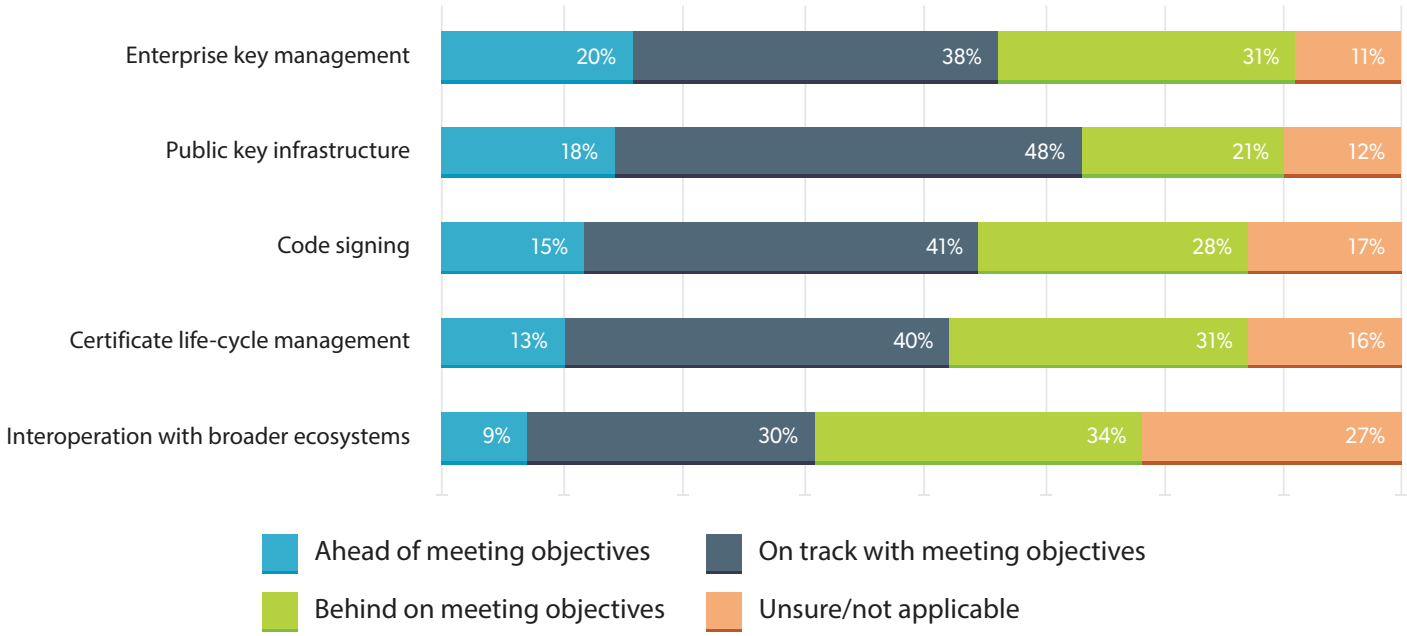
This year's survey also examined the emerging risk category of quantum computing in greater detail. The technology shows great promise but also poses security risks, as quantum computers could break some of the primary cryptographic algorithms in use today. With this in mind, security teams must understand and address the impacts of quantum risk.

Concerns about quantum computing have matured in this year's responses, which indicates a deepening understanding of the risks and increasing efforts toward mitigation. The top-cited risk, selected by 61% of respondents, is future decryption of existing data, known as harvest now, decrypt later (HNDL). The second-highest concern, future encryption compromise, was the top concern in the year-ago survey. While HNDL attacks may entail more near-term risks, encryption compromise can undermine the cryptographic trust that underpins much of data security. That can lead to attacks based on forged data, known as harvest now, forge later (HNFL). Forged data poses concerns for many data uses, notably including AI.

> *The top-cited risk, selected by 61% of respondents, is future decryption of existing data, known as harvest now, decrypt later (HNDL).*

The survey examined organizations' progress in mitigating quantum risks, as reflected in planned security measures for the next 18-24 months. The results show a slight uptick in the proportion of organizations prototyping and evaluating post-quantum cryptographic (PQC) algorithms (59%). The survey also examined organizations' self-assessed progress in implementing PQC in critical elements of their trust infrastructure. More than 50% of respondents rated themselves as on track or ahead of plan for adopting enterprise key management, public key infrastructure and code signing. More than half also placed themselves on track or ahead for certificate life-cycle management (CLM), but this area is more concerning. There is already pressure to improve CLM procedures due to requirements recently passed by the Certification Authority Browser Forum — a group of security certificate issuers and browser software suppliers — that will shorten the maximum lifetime of Transport Layer Security certificates to 47 days by 2029. That change will require greater automation in CLM, and upgrades to management processes can integrate PQC improvements at the same time to prepare for the future.

PROGRESS IN MEETING POST-QUANTUM SECURITY OBJECTIVES



Based on 2,140 organizations surveying, exploring or experimenting with quantum computing.

Survey participants are starting to work on quantum computing projects: Almost a third (32%) have either identified quantum projects or started experimenting with quantum computing. The survey also asked respondents where they expect to see the greatest impact of quantum computing on AI. The largest proportion anticipate improvements in machine learning, such as enhanced classification (57%). Advanced simulation (54%) and concurrent data processing (49%) were also frequently cited.

Almost a third of participants (32%) have either identified quantum projects or started experimenting with quantum computing.

Sovereignty in an agentic world

Amid changing technological and geopolitical landscapes and an evolution toward greater data integration and exposure, enterprises are taking matters into their own hands regarding their sovereignty journeys. Almost half (45%) said portability of some type (software, data or operations) was the primary driver of their sovereignty initiative. This is consistent with the year-ago results and reflects a key motivation of sovereignty initiatives overall. A third of respondents (34%) specifically cited a desire for full control over software and data to ensure future-proof portability.

In enterprise applications, the addition of AI models and agentic layers requires new vigilance for data stewardship and creates new sovereignty risks. GenAI applications face both external and internal challenges. The decoupling of where and how applications operate blurs sovereignty boundaries for certain workloads. Claude Code, for example, is an agentic coding tool that enables users to automate processes using natural language. It typically operates with complete retrieval augmentation from all available data sources. Code base repositories, cloud and local corporate resources may all be accessible. In this type of framework, where agentic technologies fuse processes previously performed using separate tools and data sources, lines of data residency and operational independence can erode.

While 36% of respondents reported that their organization has 50 or more SaaS applications in use, the number alone does not define the risks, as multiple SaaS applications may be integrated. For example, a customer outreach app may tie into customer relationship management and other marketing technology apps. Given these integrations, organizations must be more vigilant about defining and ensuring data residency over time, rather than assessing each application or use case statically. The adoption of agentic tools, such as Notebook LM, Cursor or Claude Code, requires dynamic digital sovereignty. The danger of interconnected applications — and the resulting need for strong sovereignty and security measures — is highlighted by the speed and success of the "ShinyHunters" attack group in compromising connected SaaS applications in 2025.

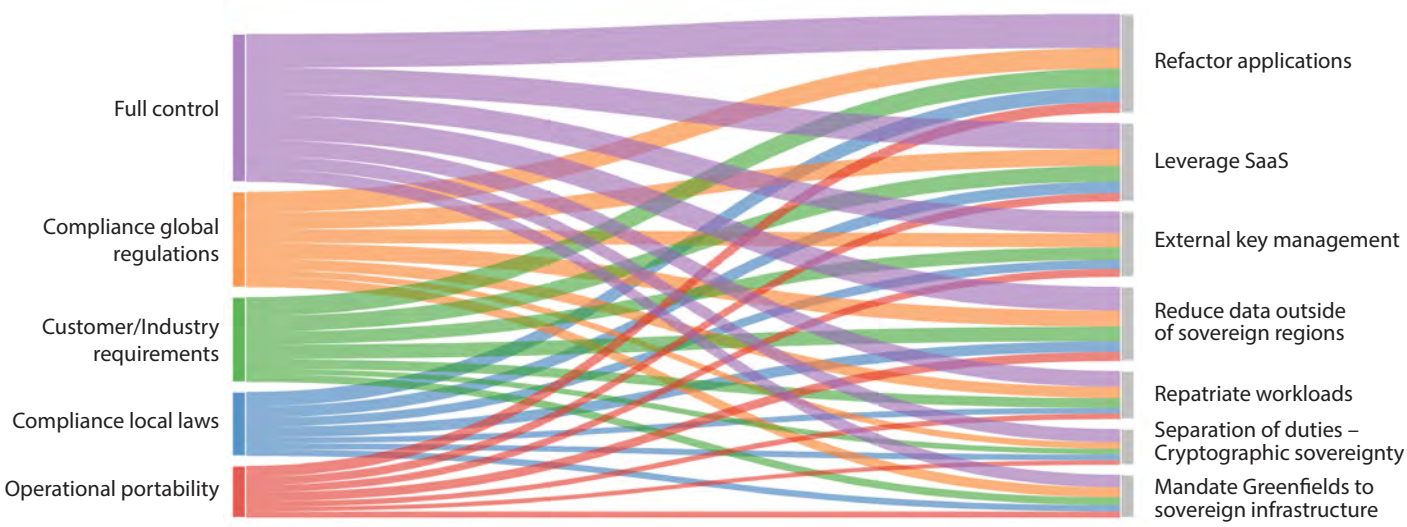
Broadly, digital sovereignty efforts have arisen alongside local and regional privacy regulations. The safe handling of individuals' publicly identifiable information (PII) or non-public information (NPI) ensures that residents' data remains under the appropriate legal jurisdiction. Enterprises that collect, store or process this data have a range of choices to ensure that data is controlled within the proper jurisdiction. To act on these choices is to exercise sovereignty over data.

The first level of sovereignty is data sovereignty. In this scenario, data must either reside in the given territory, or its contents must be strongly encrypted so that only authorized parties or processes in that region can access the data. Nearly half of all respondents (49%) said that the physical location of cloud infrastructure is important for some or all workloads when addressing sovereignty objectives, while another 36% said strong encryption and external key management provide sufficient protection regardless of location.

For more stringent workloads, operational sovereignty is also needed. Beyond cloud workload location, this may mean that all personnel involved in operations must be citizens of the given jurisdiction. Recently, the concept of data embassies has emerged, in which outposts may be housed and operated outside of the originating territory's jurisdiction while still complying with that territory's required controls. Cryptography also has implications for operational sovereignty: 19% of respondents said they will pursue their sovereignty initiatives through more explicit encryption — "cryptographic sovereignty" — and stronger separation of duties between defining and implementing encryption.

Software sovereignty marks another step beyond operational sovereignty, in that data can be removed from any existing application and readily ported to new ones. Full control over data and software is the most widely cited driver of sovereignty initiatives, and enterprises are making meaningful changes to achieve this. Two in five respondents (40%) are working to achieve sovereignty by reducing the amount of data available outside sovereign regions, and 54% are refactoring applications to better segment or isolate data.

FLOW ANALYSIS: FROM SOVEREIGNTY DRIVERS TO SOLUTIONS



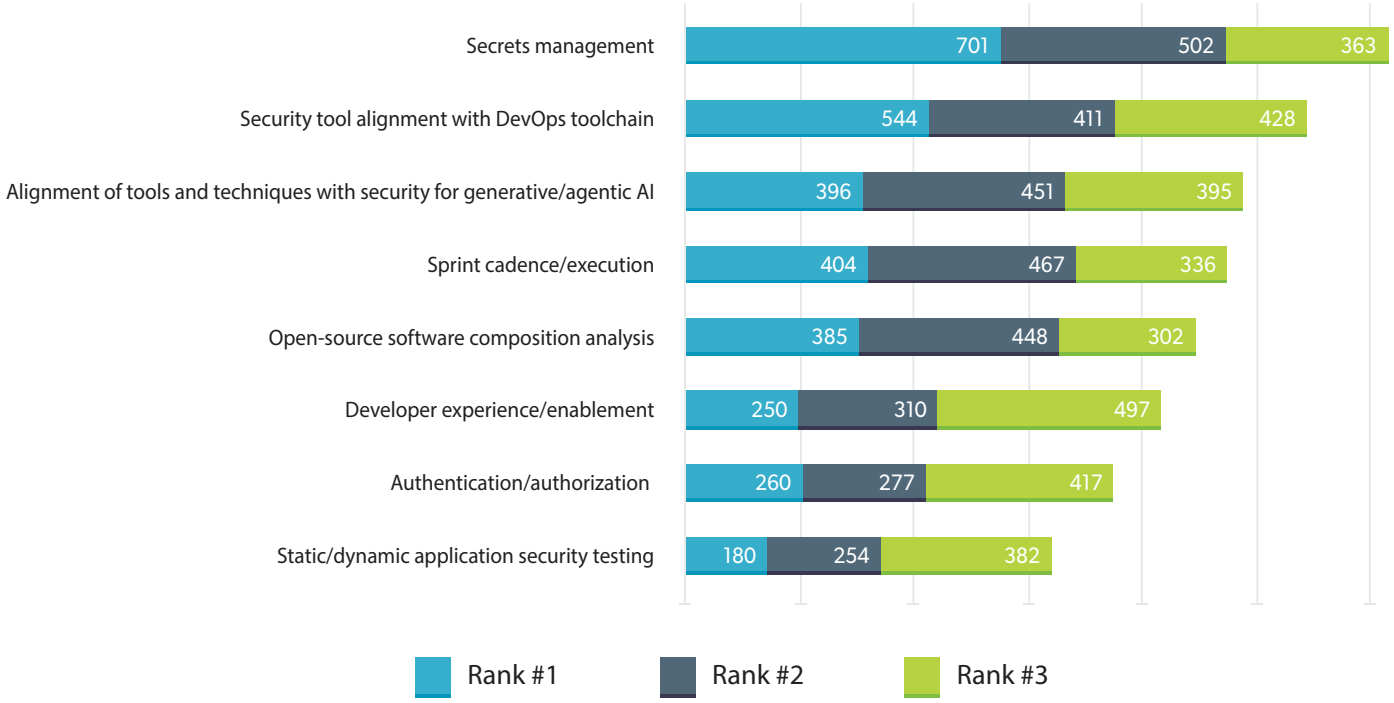
While sovereignty efforts largely began in support of privacy mandates, sovereignty increasingly enables enterprises to switch to more favorable economic venues. The fast-moving AI and SaaS ecosystems have begotten a worldwide data center boom that has placed additional constraints on sustainability, energy and resiliency. Digital sovereignty and full data control reduce the economic risks and technical debt created by isolated or unportable data silos.

Data security for application development

Application development forms the leading edge of effective security operations. Building secure code and application architecture is a foundational practice, and this is another area under pressure from AI and agentic applications. As AI coding and application tools become available to a broader range of users, security teams must ensure that these tools, as well as the applications they generate, are built on secure structures and services. Notably, securing secrets that manage access to data is the top-cited security challenge in DevOps processes.

In this context, data security tools and frameworks must provide scaffolding that enables developers to build secure applications — a mandate that becomes even more critical with agentic applications. This is a particular area of concern, as survey respondents ranked spending levels on DevSecOps and secrets management tools lowest among all listed technology categories. As security teams invest to mitigate the risks posed by agentic applications, development infrastructure and data protection must be prioritized.

BIGGEST SECURITY CHALLENGES IN DEVOPS



Conclusion

Effective data security has never been easy, and the pressures of AI and agentic applications are making it much harder. Data must be available for a wider range of uses, in greater volumes and at higher velocity, all while maintaining strong security controls. Consistent, operational data security is paramount to achieving and sustaining this vision. Data security posture management (DSPM), data monitoring and governance, and data protection must consistently reinforce one another, both to manage growing and evolving risks and to realize significant potential rewards.

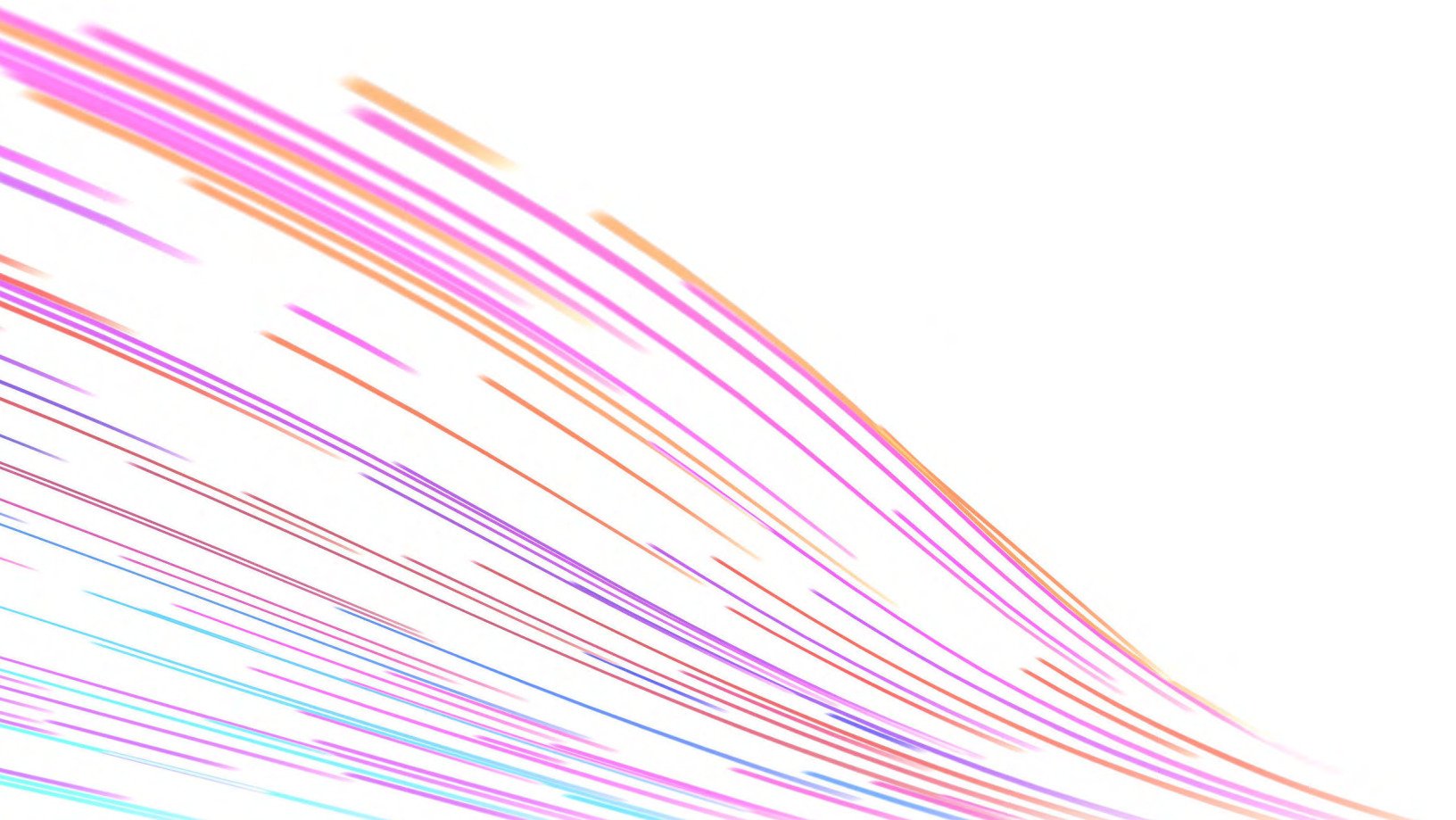
The AI ecosystem is evolving rapidly, and security teams must be prepared for the next pivot, not only with flexible controls but also with better visibility into the data they are tasked with protecting. As organizations embrace greater levels of automation in the next wave of AI and agent-driven integration, they must reduce security complexity to meet the scale and velocity that competitive pressures demand.

The study results suggest several practical next steps:

- **Consistent data identification and controls are critical:** Data assets become quickly interwoven. With organizations reporting an average of 89 SaaS applications in use, the integration of common applications has resulted in many ingress and egress paths for adversaries to exploit. Consistently identifying and controlling data across multiple applications, clouds and jurisdictions requires a platform approach. By contrast, fragmented controls lead to greater complexity and expanded risks.
- **Proactivity is a mandate:** Security leaders must build alliances with both internal stakeholders and industry peers to understand and navigate new competitive pressures. AI shows high potential to expand markets and create new products and services, generating new opportunities. However, when asked about competitive pressure on market growth stemming from the onset of AI, just 19% of respondents said they are leading their peers.
- **Sovereignty is crucial:** Future-proof portability may determine which platforms remain usable, particularly in heavily regulated industries and jurisdictions. Enterprises with data, operational and software sovereignty can more readily migrate to and operate in the best available execution venue. With AI workloads and initiatives increasingly gated by computing, data center and energy constraints, the freedom to choose and exercise controls is more crucial than ever.
- **Trust is built on security.** New dangers from AI-fueled disinformation and misinformation are universal, with 97% of all respondents reporting some form of organizational harm from AI-generated false information, including deepfake business email compromise, trademark or brand abuse, harm to key personnel, reputational damage or hiring fraud. Security tools that consistently meet users and stakeholders where they are will enable better and faster prevention, detection and response.

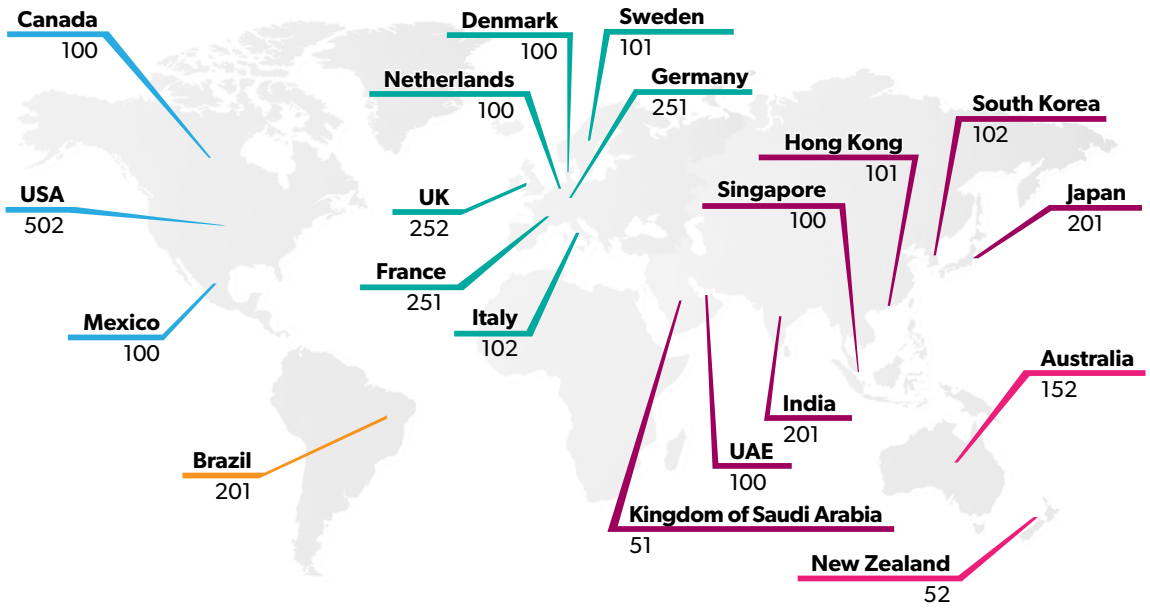
- **Now is the time to act.** Despite the fast-moving ecosystem, enterprises must act with the data they have today. Poor data quality or poor initial data governance is the most widely cited issue limiting AI adoption. Incomplete knowledge about the data estate — what it consists of, where it resides and how best to protect it — begets the second-largest issue: the security risks of exposed data.
- **Simplified, flexible, extensible security tooling can reduce operational complexity.** The level of operational complexity reflected in the study is not sustainable in an agentic world. Security capabilities must be adaptable enough to secure whatever infrastructure is best suited to application requirements. Organizations must be able to use native controls while also extending protections across on-premises environments and multiple clouds. Data encryption is a crucial component; it must span diverse infrastructures and address emerging quantum computing risks.

AI initiatives, including those based on agentic approaches, continue to blur previously clear lines for users. Agents and AI infrastructures increasingly automate, integrate and abstract multiple systems and myriad data sources. For now, AI still largely serves its users, but controls are frequently delegated to a degree that could allow agents to become a new internal threat. To combat this threat, organizations will need to develop, present and enforce policies in consistent, easily understandable ways for individuals, teams and the entire enterprise, enabling opportunities to adapt quickly and prosper securely.



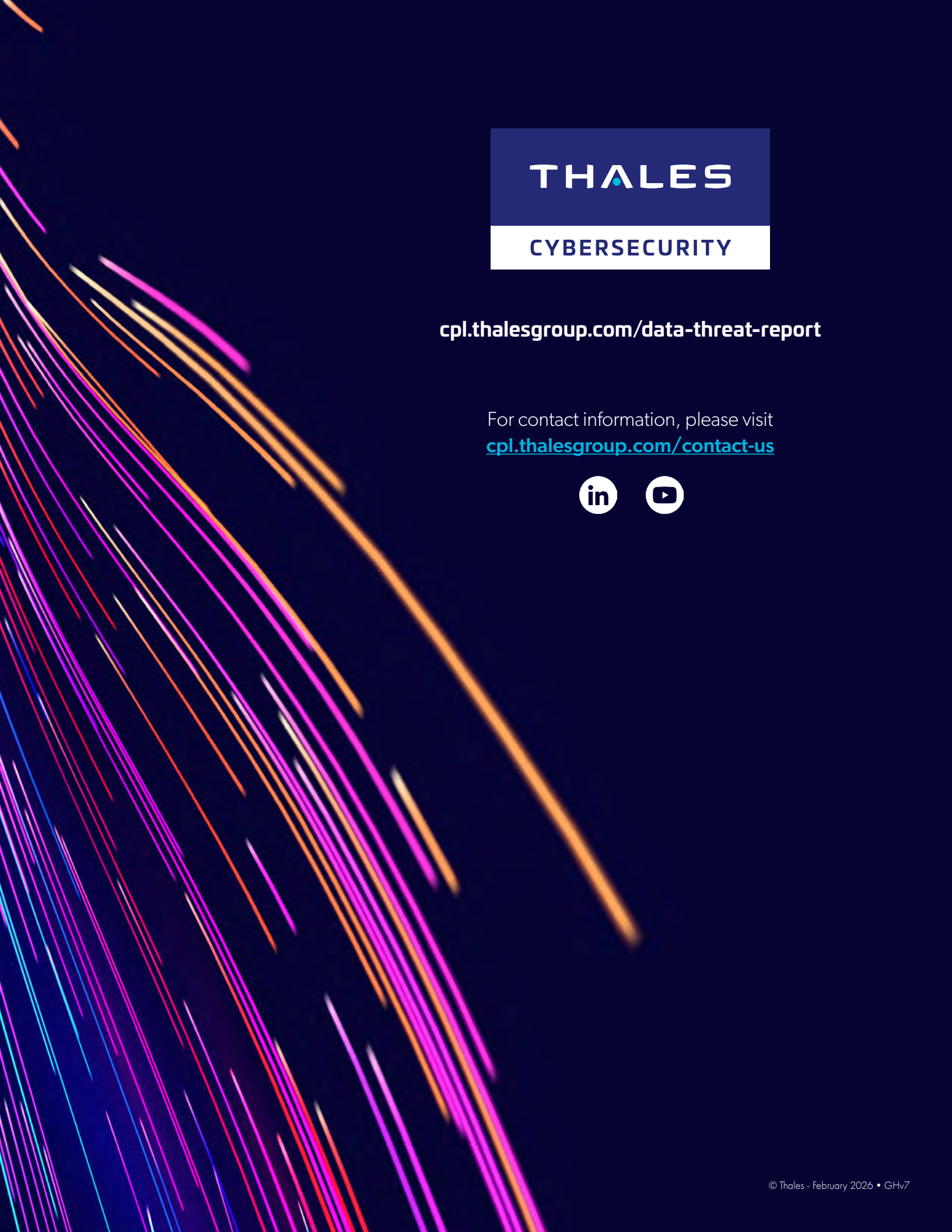
Methodology

This research was based on a global survey of 3,120 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	213
$250m to $499.9m	701
$500m to $749.9m	799
$750m to $999.9m	774
$1 Bn to $1.49 Bn	265
$1.5 Bn to $1.99 Bn	137
$2 Bn or more	231
Total	3,120

Industry Sector	Number of Respondents	Industry Sector	Number of Respondents
Healthcare	263	Travel / Hospitality	181
Retail	255	eCommerce	171
Manufacturing	251	Automotive	166
Financial Services	237	Education	141
Technology	222	Biotechnology	124
Energy & Utilities	213	Defense	115
Government	207	Aerospace	80
Transportation	189	Telecommunications	79
Pharmaceuticals	187	Other	28
Total			3,120



cpl.thalesgroup.com/data-threat-report

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