2026 EDITION

RETAIL AND E-COMMERCE

THALES

CYBERSECURITY

DATA THREAT REPORT

Data security in the agentic age: AI is the new insider threat to retail and e-commerce organizations

cpl.thalesgroup.com

#2026DataThreatReport

Table of Contents

Conducted by

S&P Global
Market Intelligence

Introduction

Retail and e-commerce ("retail") organizations are categorized into three primary enterprise types: traditional brick-and-mortar retailers operating physical locations; pure-play e-commerce businesses that sell exclusively online through websites and third-party marketplaces; and omnichannel retailers, which integrate both physical and online operations. Since these organizations manage vast amounts of sensitive customer data, protecting this data from increasingly sophisticated attacks is a key concern.

Securing online transactions and customer accounts is a key challenge for these organizations as cybercriminals empowered with advanced AI continuously develop new ways to commit payment fraud and take over customer accounts for unauthorized purchases. This leads to a conundrum: Retailers must balance inherent trade-offs between maximizing security — verifying user identity and securing credentials — and minimizing friction in the customer experience.

Securing complex digital infrastructures is another major challenge. IT environments increasingly include cloud services and AI-driven platforms, resulting in expanded digital attack surfaces and increased difficulty securing intricate, interconnected systems. AI has introduced significant risks stemming from rapid operational and ecosystem changes, trust issues with third-party systems and sensitive data exposure. Meanwhile, quantum computing continues to pose concerns about future encryption compromise and "harvest now, decrypt later" data threats.

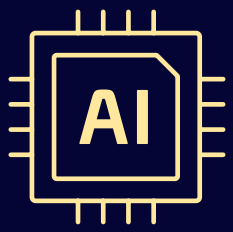
The **2026 Data Threat Report** executive summary for the retail industry is based on survey data from 426 IT and security professionals working in retail organizations across 20 countries. The survey examined their attitudes and actions regarding data security. This summary highlights key findings from that study while drawing comparisons to the overall 2026 Data Threat Report survey data to reveal evolving trends and notable differences in the threat landscape and security posture.

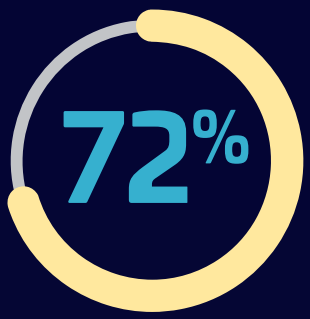
Key findings

Security priorities are changing with AI

Spending on AI security is rising –

32% Nearly one-third of retail organizations have a dedicated budget for AI security (up from 19% a year ago), but more than half **(52%)** still fund AI security using their existing security budgets.





Nearly three-quarters of retail organizations expressed concerns about rapid change in AI ecosystems, making this the top-cited AI security risk. The pace of change challenges the ability of security tools or technology to keep up.

85%

A large majority of retail organizations have invested in specific security tools or services due to concerns about AI.

AI-fueled attacks emerged as a prominent threat -

61%

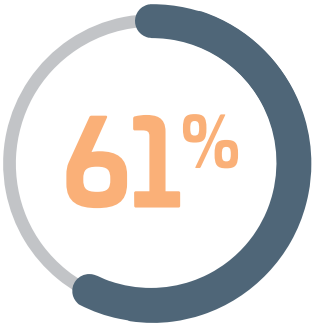
Many respondents have experienced deepfake attacks or **reputational damage (48%) stemming from AI-generated misinformation.**

61%

AI applications are being targeted by attackers, with sensitive data disclosure **(61%)** and misinformation/ deepfakes **(57%)** as the top categories in which AI/LLM attacks are increasing.

Over half of retail respondents reported an increase in prompt injection attacks, placing this category third among AI attack types on the rise.

Data protection is critical in the AI age



Nearly two-thirds of retail C-suite respondents reported no history of cloud data breaches, versus **52%** of their security teams.

51%

Half of retail respondents ranked identity and access management among the top three most pressing security disciplines, as attackers increasingly exploit credentials.

On average, about half (53%) of retail organizations' sensitive data in the cloud is encrypted, up slightly from 50% in 2025.

of retail organizations said they have complete knowledge of where their data is stored, but this is up from 32% year over year.

50%

Half of retail respondents ranked secrets management as a leading concern in application security.

Complexity limits clear insight into data security posture

Tool counts are high – **76%** of retail organizations have five or more data protection tools.

7 tools are the average for data protection and monitoring

49% have five or more key management systems

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

27% About one-fourth of retail organizations that have experienced a data breach cited human error as the cause — the top response. The greatest proportion of respondents cited nation-state attackers and hacktivists as their top sources of concern.

Audit failures are linked to significantly higher breach risk –

67% of retail organizations that have failed an audit reported at least one cloud breach, compared with **33%** of those that passed all audits.

Cloud is a significant attack target

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

37% cloud storage,

37% cloud-delivered applications

32% and cloud management infrastructure

as top attack targets.

Credential theft is the top-cited rising attack technique against cloud infrastructure –

71% of retail organizations reported an increase in credential theft and misappropriated secrets, slightly higher than 67% surveywide.

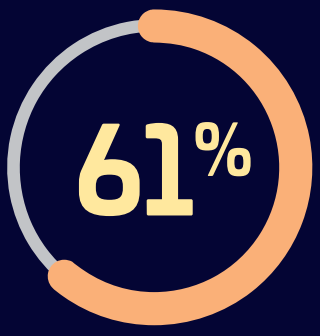
Rising geopolitical risk is reshaping data sovereignty

54% More than half of retail respondents are reworking and refactoring application and data architectures as their main focus in achieving sovereignty objectives, identical to surveywide results.

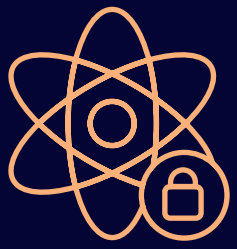
39% More than one-third (39%) believe cryptographic protections such as encryption and key management are sufficient to achieve data sovereignty, similar to surveywide results (40%).

Future risks are concerns today

Future decryption of existing classically encrypted data (also known as harvest now, decrypt later) is the top quantum computing concern,



cited by retail organizations.



Organizations are moving to mitigate quantum risk

61%

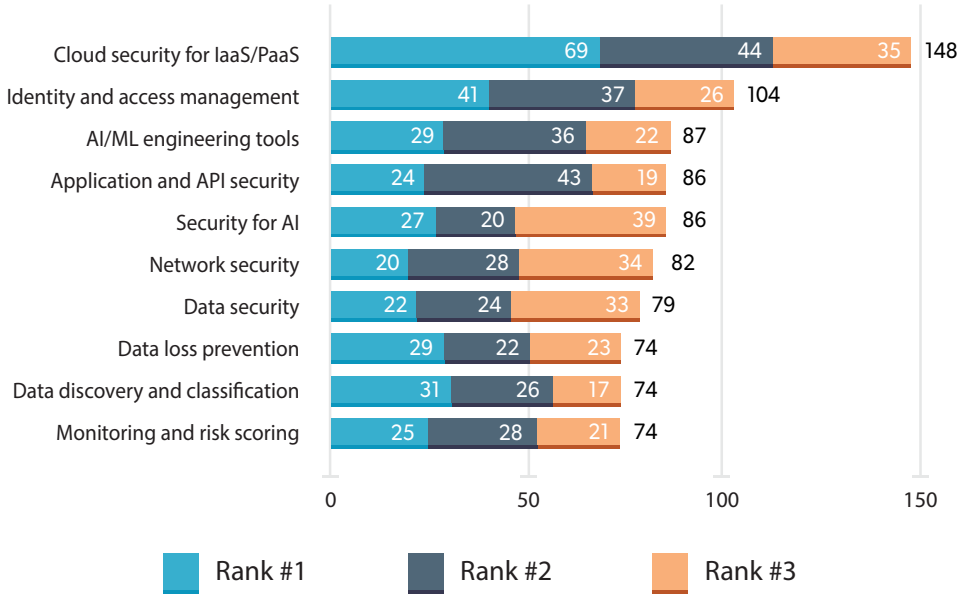
are prototyping and evaluating post-quantum cryptographic algorithms, slightly higher than surveywide and 7 points higher than last year's survey.

Retail observations

Continued structural and geopolitical tensions in 2026 are forcing a sea change in enterprise security strategies, and retail organizations remain among the top targets for attackers due to the large volumes of high-value data they collect, including personal, financial and transactional information. This year's retail-industry Data Threat Report shows that while spending on security operations and cloud security remain the highest priorities, AI security spending is rapidly increasing. Most retail organizations (84%) are investing in specific tools and services to address AI-related security concerns — slightly higher than surveywide — and 32% have a dedicated AI security budget, up from 19% a year ago. However, more than half (52%) still fund AI security using existing security budgets.

Retail organizations exhibit other key differences compared to the survey population as a whole. These include reporting a higher percentage of sensitive data stored in the cloud (53% versus 47% surveywide) and, encouragingly, greater implementation of sensitive data encryption: 23% of retail organizations reported that they encrypt 75%-100% of sensitive cloud data, compared with only 14% surveywide. Improvement in the latter metric is clearly needed across all organizations.

RETAIL AND E-COMMERCE 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.

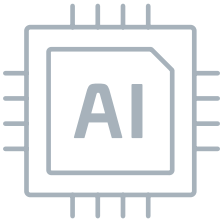
From a spending perspective, retail organizations prioritize security operations spending (SIEM/SOAR/threat intelligence) more than organizations surveywide (42% versus 34%). Email security spending also ranks higher among retail respondents than surveywide (35% versus 30%). Curiously, retail organizations are less likely to prioritize data security spending (28%) and endpoint security spending (24%) compared to the entire survey population (35% and 38%, respectively). This is counterintuitive, given that many retail organizations store highly valuable customer data, and that retail endpoints, such as point-of-sale devices, are frequent attack targets.

Security pressures expand with AI and agentic operations

Security teams are grappling with rapid change stemming from enterprise AI adoption, and the addition of AI agents is complicating the landscape further. In a recent 451 Research Voice of the Enterprise study on agentic AI, one-third of enterprises (34%) reported that embedded agents are already in use, and most (74%) expect to use them within 12 months. Agentic applications dramatically increase the velocity of data movement and the volume of data in use, and enterprises are already struggling with data management and security.

Only 37% of retail respondents to the Data Threat study said they have complete knowledge of where their organization's data is stored (compared with 34% surveywide), and only slightly more (41%) said they can classify all their data — a necessary step to effective data protection. Among key areas of security spending, cloud security for IaaS/PaaS is the most highly prioritized, with 35% placing it in their top three categories, followed by identity and access management (24%), security for AI (20%) and AI/ML engineering tools (20%). This is unsurprising, given that AI workloads run predominantly in cloud environments and depend heavily on APIs, and concern about the security of AI systems is high.

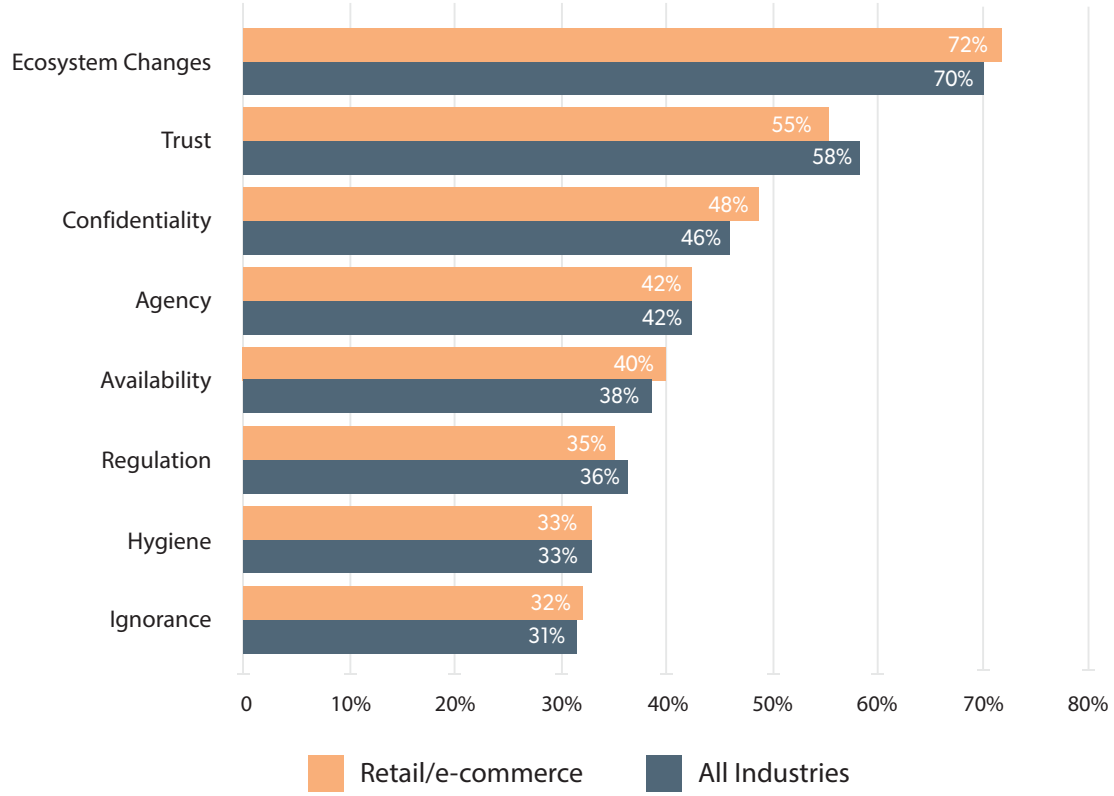
Only 37% of retail respondents to the Data Threat study said they have complete knowledge of where their organization's data is stored



Security for AI is challenging. With the pace of technology evolution, and with retail enterprises tending to trail other industries in early adoption of new technologies, rapid change in the AI ecosystem is their top AI-related security concern: 72% of respondents identified it as a top source of risk, slightly higher than the entire survey population. Trust (55%) and confidentiality (48%) are the second- and third-ranked concerns.

Attackers are also using AI, necessitating 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-cited targets in this year's survey. Given the large volumes of data used by AI and the increases in discoverability associated with AI agents, encryption is critical. 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.

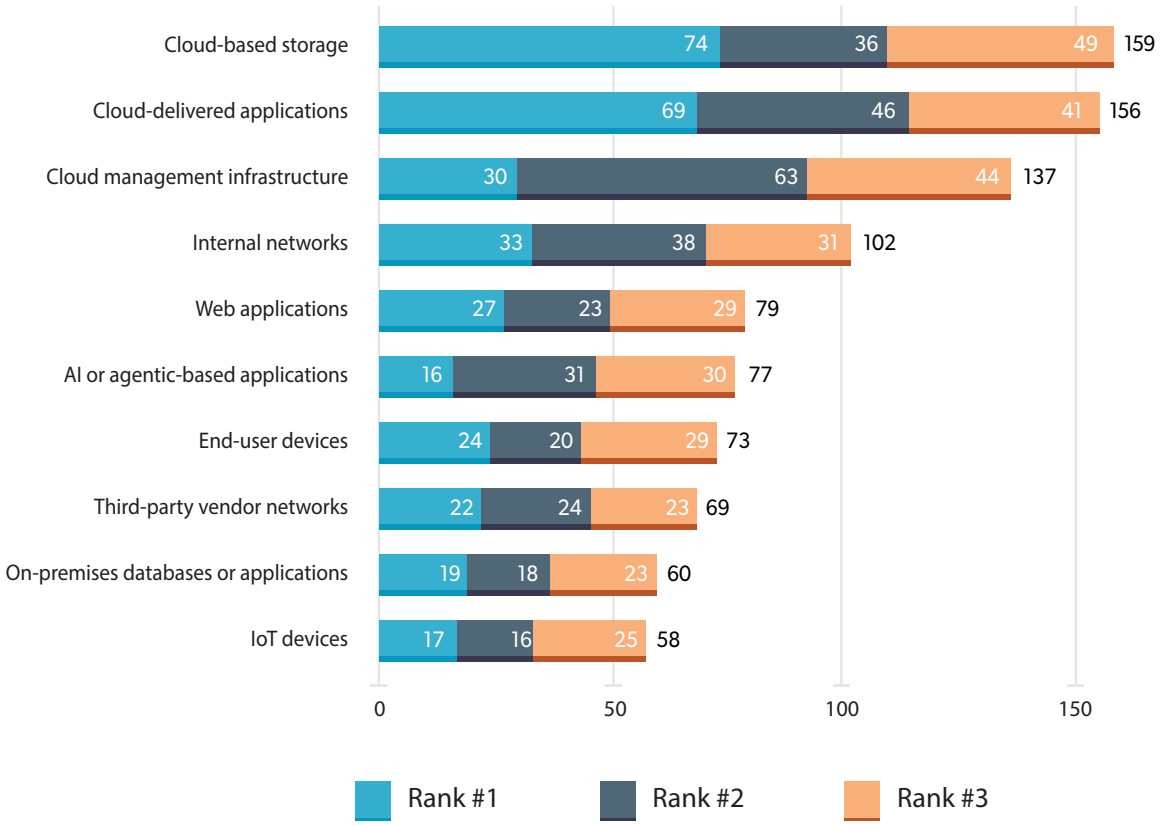
MOST CONCERNING AI SECURITY RISKS



The data threat landscape

The data threat landscape continues to shift. Retail organizations are observing changes in attacks and working to mitigate new tactics. In this survey, cloud-based assets represent the top three attack targets, in line with surveywide results.

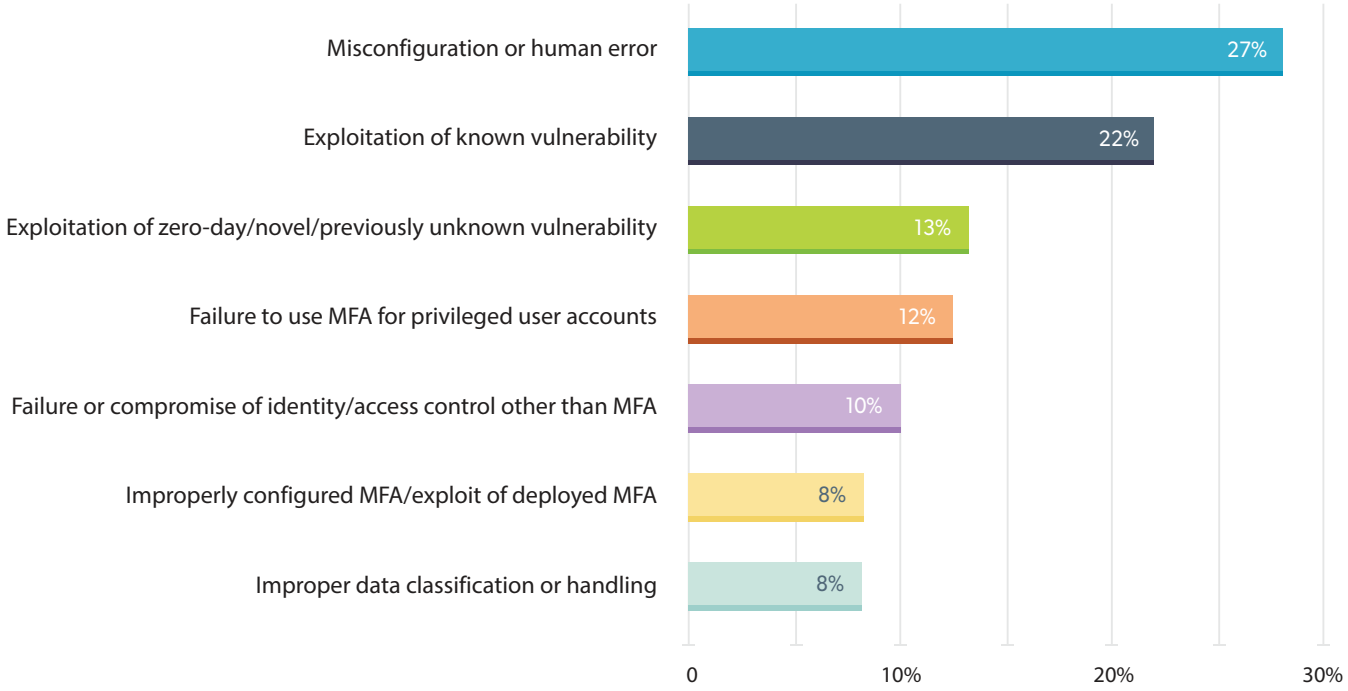
TOP RETAIL/E-COMMERCE ATTACK TARGETS



This year's results reflect relative consistency in the prevalence of audit failures and reported breaches. Just over half (56%) of retail respondents indicated no history of cloud breaches, similar to surveywide results, and 58% reported no on-premises breaches. Three in five (60%) reported passing all compliance audits in the last 12 months. Continuing the pattern of previous years, retail organizations that fail audits are much more likely to report a breach: Among organizations that failed an audit, 67% reported a cloud breach and 54% reported an on-premises breach, compared to 33% and 46%, respectively, for those that passed all audits.

Awareness of breach history may be an issue in some organizations, as the data shows differences in reported breach history across job roles. Senior executives are less likely to identify breaches than those in management or practitioner roles. A high percentage (61%) of retail executives reported that their organization has not experienced a cloud breach, while only 52% of practitioners believe that to be so. The difference for on-premises breaches is similar: 65% of executives reported no breach history, versus 57% of practitioners. These discrepancies can have material impacts on how security budgets are prioritized.

MOST COMMON CAUSES OF DATA BREACHES AMONG RETAIL/E-COMMERCE ORGANIZATIONS



Based on 426 respondents whose retail organization experienced a data breach.

Human error (27%) remains the leading cause of retail data breaches, similar to surveywide results. Exploitation of known vulnerabilities ranked No. 2 (22%), substantially ahead of the next most common cause: exploitation of zero day/novel/previously unknown vulnerabilities — a situation likely to change over the next year due to advances in offensive AI technologies. 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 requires a perspective shift in security mitigation priorities, since human error is paradoxically not cited as the leading security concern.

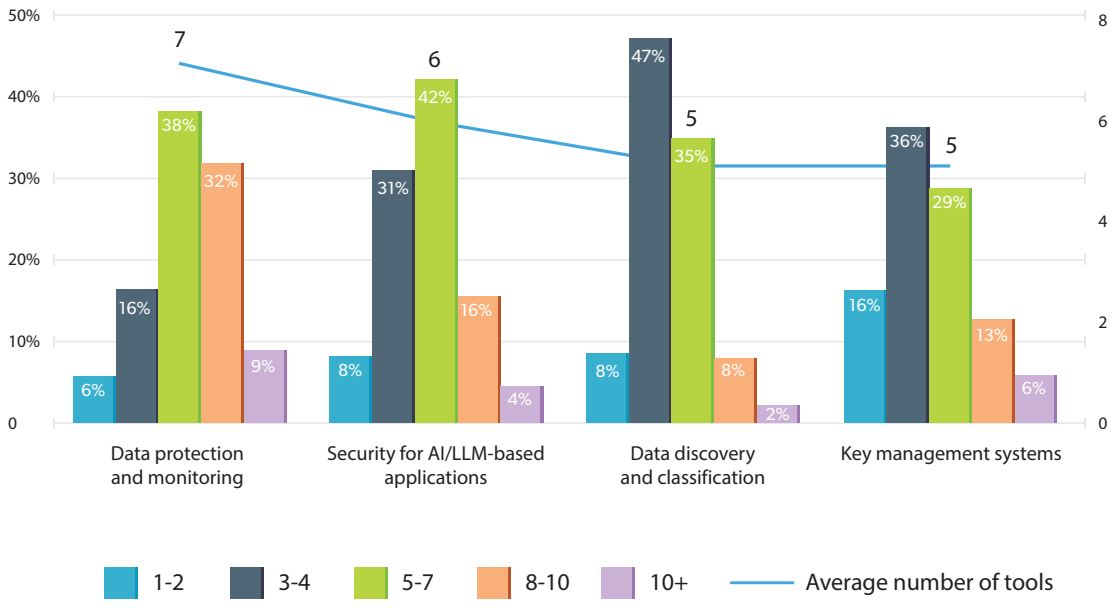
Complexity impacts security effectiveness

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 toolsets to roll up to integrated security teams. Whatever the cause, the study results show high levels of tool sprawl.

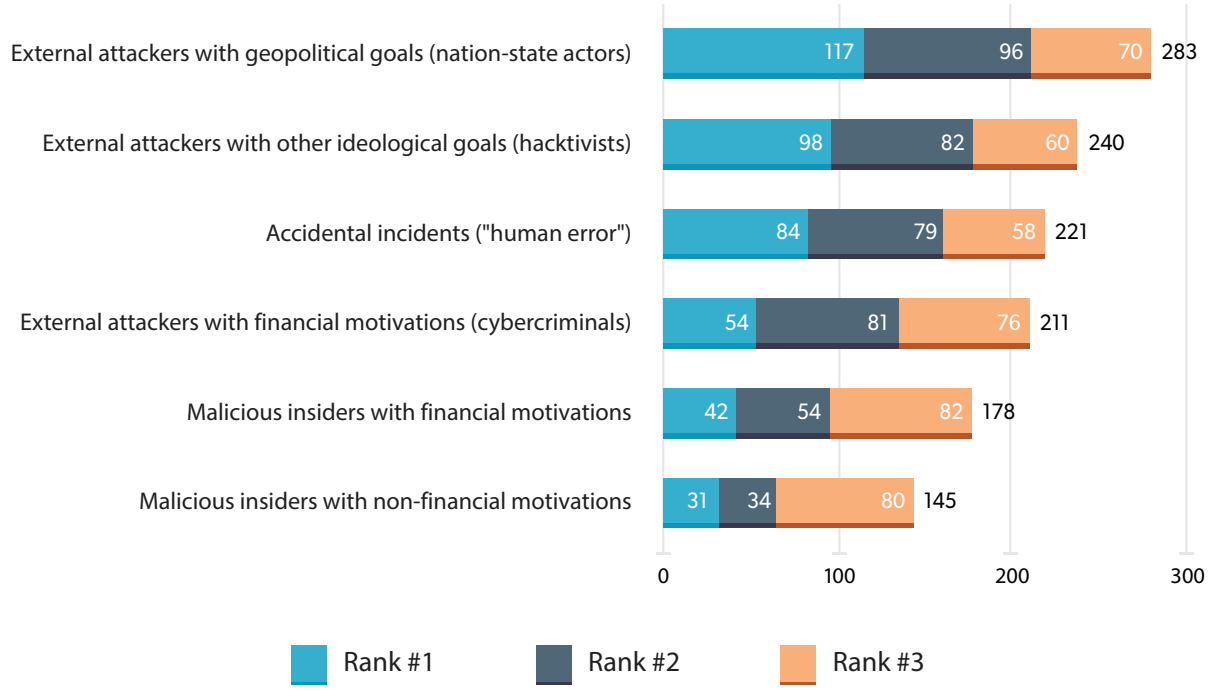
The most notable area is data protection and monitoring, where retail and e-commerce respondents combined reported an average of seven tools, and 76% have five or more. This is particularly concerning given the increased focus on data security that accompanies growing AI adoption. AI security tools exhibited the second-highest level of sprawl, with an average of five tools per organization, and 58% of retail organizations reported five or more tools in use. Comparing classic retailers against e-commerce firms, retailers have slightly higher tool counts (7 for retailers versus 6 for e-commerce), likely because they have larger IT estates that include on-premises systems.

NUMBER OF DATA DISCOVERY, CLASSIFICATION AND KEY MANAGEMENT SYSTEMS IN USE BY RETAIL/E-COMMERCE ORGANIZATIONS



Nevertheless, survey respondents expressed resistance to consolidating security tools. A decision to remove any security controls should be subject to careful evaluation. Surprisingly, however, when asked about the reason for their resistance to tool consolidation, 62% of retail respondents cited a perceived lack of functionality or capability in other available tools, and 57% cited a lack of compatibility. This is doubly concerning because only 39% of retail respondents cited high confidence in their understanding and knowledge of existing data security 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 TO RETAIL/E-COMMERCE



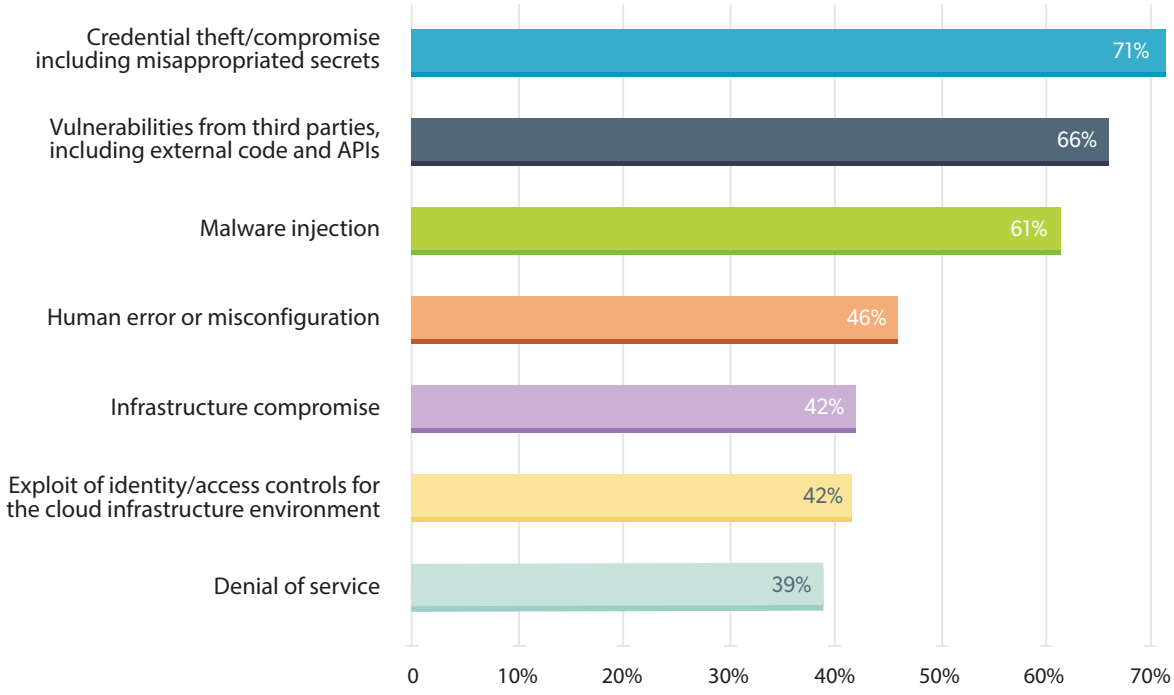
Regardless of the reasons for resistance, tool consolidation is necessary to simplify and scale security operations. Organizations are becoming ever more hybrid and complex — using more cloud providers and working to secure more applications. This growing complexity recalls another misalignment in security 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 66% of retail respondents (down 8 points year over year but still in the top spot) — 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 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.

Retail organizations have on average 2.3 cloud providers, and 40% of respondents indicated they have three or more cloud providers, similar to surveywide results and up from 2.0 in the 2022 study. On average, retail organizations have 88 SaaS applications in use, similar to the surveywide average of 89. Interestingly, when considered separately, classic retailers average 106 SaaS apps while e-commerce firms average 60 — potentially due to significant differences in organizational IT strategies and build-vs.-buy attitudes that some younger e-commerce firms exhibit. **Cloud security is once again the top security spending category, indicating that enterprises are working hard to secure this critical resource.**

RISING MODES OF ATTACK AGAINST RETAIL/E-COMMERCE ORGANIZATIONS' CLOUD MANAGEMENT INFRASTRUCTURE



Among the types of cloud infrastructure attacks on the rise, credential theft and compromise increased from 66% to 71% year over year, followed by third-party vulnerabilities, which increased from 54% to 66%. Malware injection dropped to the third spot from second a year ago (down 4 points). Meanwhile, denial-of-service attacks dropped to seventh place (down 8 points). This shift reflects attackers' increasing use of software supply chain attacks and malicious modules and plug-ins. 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 suggest a concerning lack of progress in protecting the enterprise's most precious asset — data. The average share of cloud data categorized as sensitive grew from 54% in 2025 to 56% this year, while the average proportion of sensitive retail data protected by encryption is just 53%, up slightly from 50% a year ago. Approximately half of all sensitive cloud data is not encrypted, representing a significant potential attack surface.

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.

The average share of cloud data categorized as sensitive grew from 54% in 2025 to 56% this year, while the average proportion of sensitive retail data protected by encryption is just 53%, up slightly from 50% a year ago.

Quantum risk realities

This year's survey examined the emerging risk category of quantum computing in greater detail. Quantum computing poses a systemic, forward-looking risk to retail organizations because it threatens the cryptography that underpins everything from interbank payments and trading platforms to mobile banking and customer data protection. The technology shows great promise but also poses security risks, as quantum computers could break some of the primary cryptographic algorithms in use today.

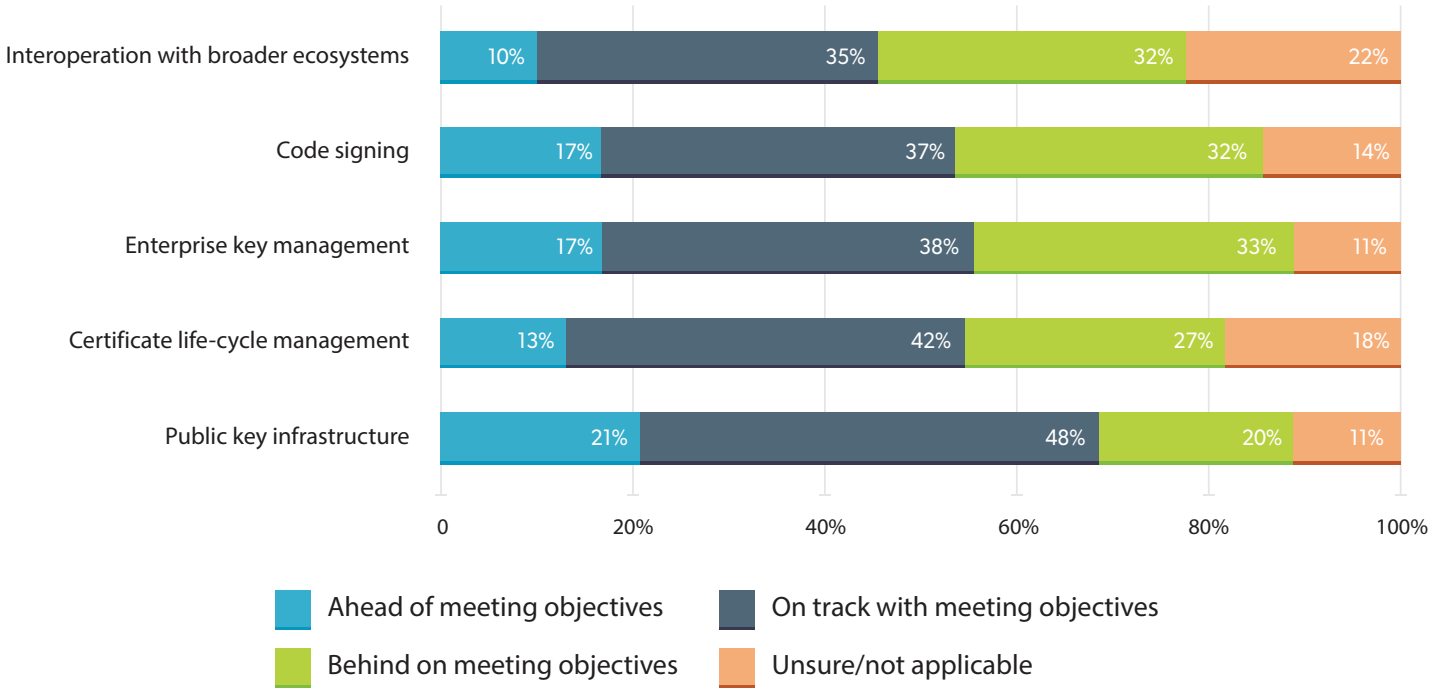
Concerns about quantum computing have matured in this year's responses, indicating a deepening understanding of the risks and increasing efforts toward mitigation. Decryption of existing data, known as harvest now, decrypt later (HNDL) was the top-cited risk (61%), followed closely by future encryption compromise (58%). 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. Forged data poses concerns for many retail data applications, notably including AI.

The survey examined retail organizations' progress in mitigating quantum risks, reflected in planned security measures for the next 18-24 months. The results show an uptick in the proportion of organizations prototyping and evaluating post-quantum cryptographic (PQC) algorithms (61%, up from 54%). The survey also examined organizations' self-assessed progress in implementing PQC in critical elements of their trust infrastructure. Most respondents rated their organizations as on track or ahead of plan for adopting public key infrastructure (68%), enterprise key management (55%) and code signing (54%).

The results show an uptick in the proportion of organizations prototyping and evaluating post-quantum cryptographic (PQC) algorithms (61%, up from 54%).

More than half (55%) also placed their organizations on track or ahead of plan 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



Survey participants are starting to work on quantum computing projects: One-third (34%) of retail organizations have either identified potential quantum projects or started experimenting with quantum computing — similar to the overall survey sample (32%). The survey also asked respondents where they expect to see the greatest impact of quantum computing on AI. The largest proportion anticipate improvements in advanced simulation of complex systems (58%) and machine learning, such as enhanced classification (56%). Concurrent data processing (50%) was also frequently cited.

One-third (34%) of retail organizations have either identified potential 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 control of their sovereignty journeys. One-third of retail respondents (33%) said full control over software and data to ensure future-proof portability is the primary driver for their digital sovereignty initiatives, along with 11% who cited operational portability to run systems in specific jurisdictions.

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 38% of retail respondents reported that their organization has 50 or more SaaS applications in use (similar to surveywide results), the number alone does not define the risks since multiple SaaS applications may be integrated. For example, a customer outreach app may be tied 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.

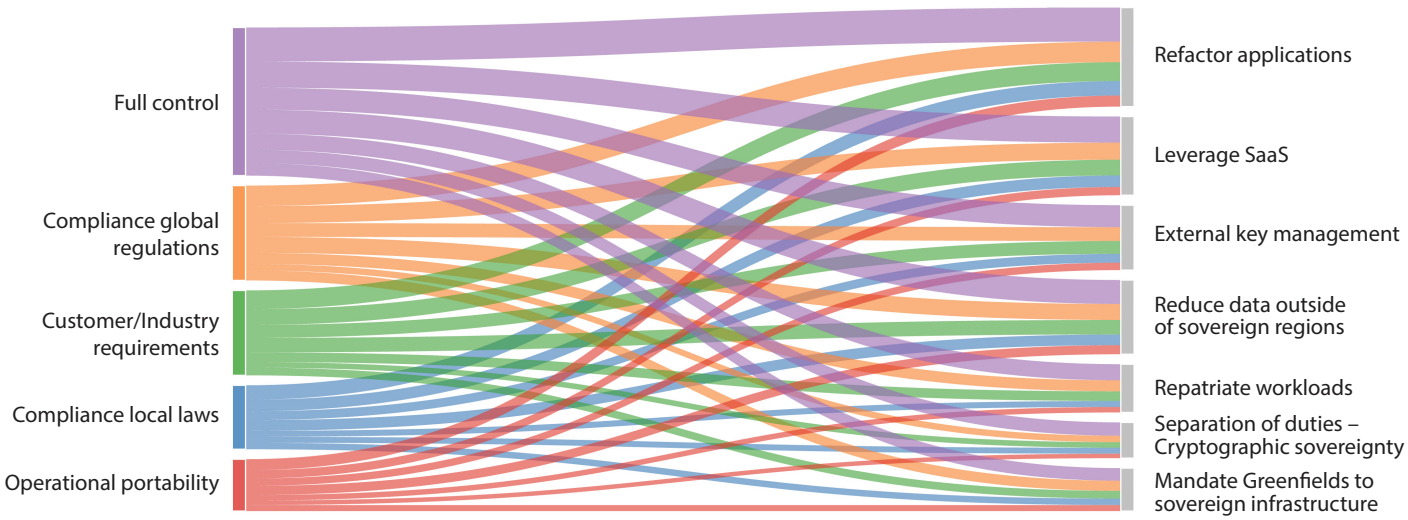
Broadly, digital sovereignty efforts have arisen alongside local and regional privacy regulations. The safe handling of individuals' publicly identifiable information or non-public information ensures that residents' data remains under the appropriate legal jurisdiction. Enterprises that collect, store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

Data sovereignty represents the first of several sovereignty levels. To achieve data sovereignty, data must either reside in the relevant territory or be strongly encrypted so that only authorized parties or processes in that region can access it. Half of retail respondents (51%) said the physical location of cloud infrastructure is important for some or all workloads when addressing sovereignty objectives, while another 39% 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 the originating territory's jurisdiction while complying with that territory's required controls. Cryptography also has implications for operational sovereignty: 17% of retail respondents indicated 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. Nearly two in five respondents (37%) are working to achieve sovereignty by reducing the amount of data available outside sovereign regions, similar to 40% surveywide, and 54% are refactoring applications to better segment or isolate data, identical to the survey population as a whole.

FLOW ANALYSIS: FROM SOVEREIGNTY DRIVERS TO SOLUTIONS



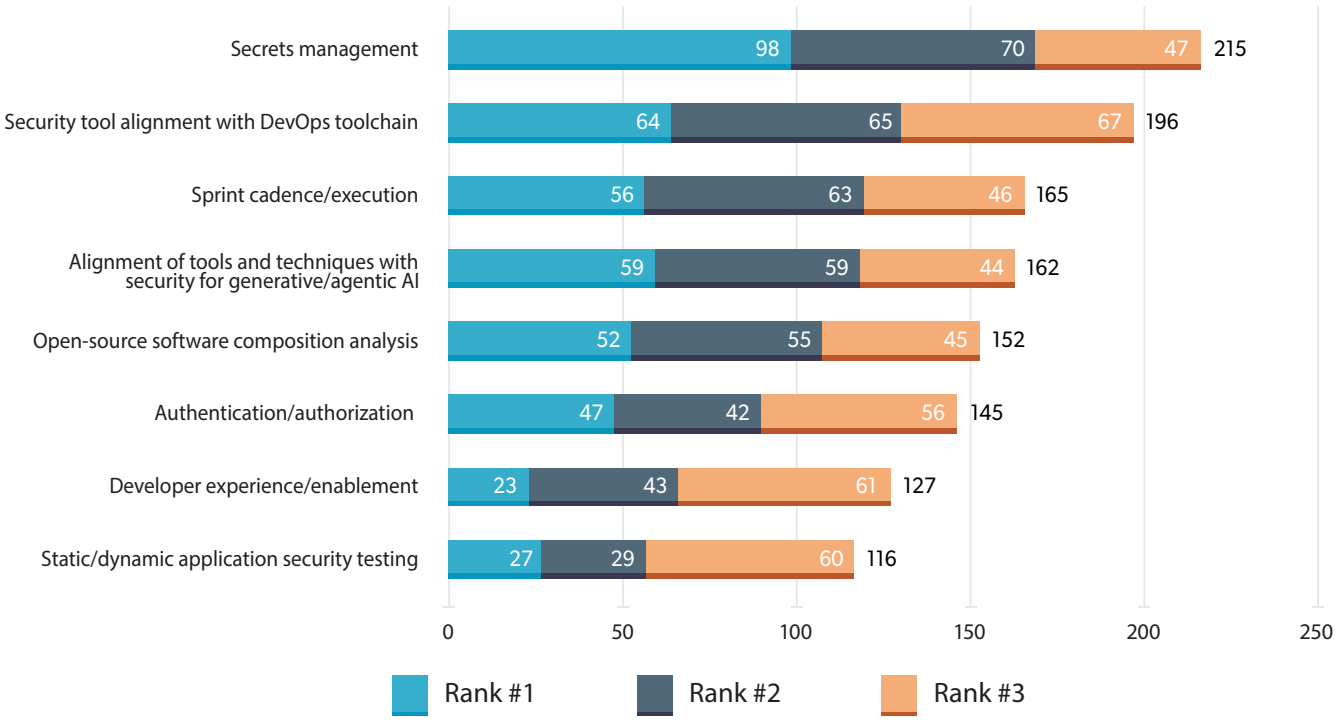
While sovereignty efforts largely began to support privacy mandates, sovereignty increasingly enables enterprises to switch to more favorable economic venues. The fast-moving AI and SaaS ecosystems have begotten a worldwide data center boom that has placed additional constraints on sustainability, energy and resiliency. Digital sovereignty and full data control mitigate 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 was 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 because 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 more difficult. 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, 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 suggests several practical next steps for retail organizations to consider:

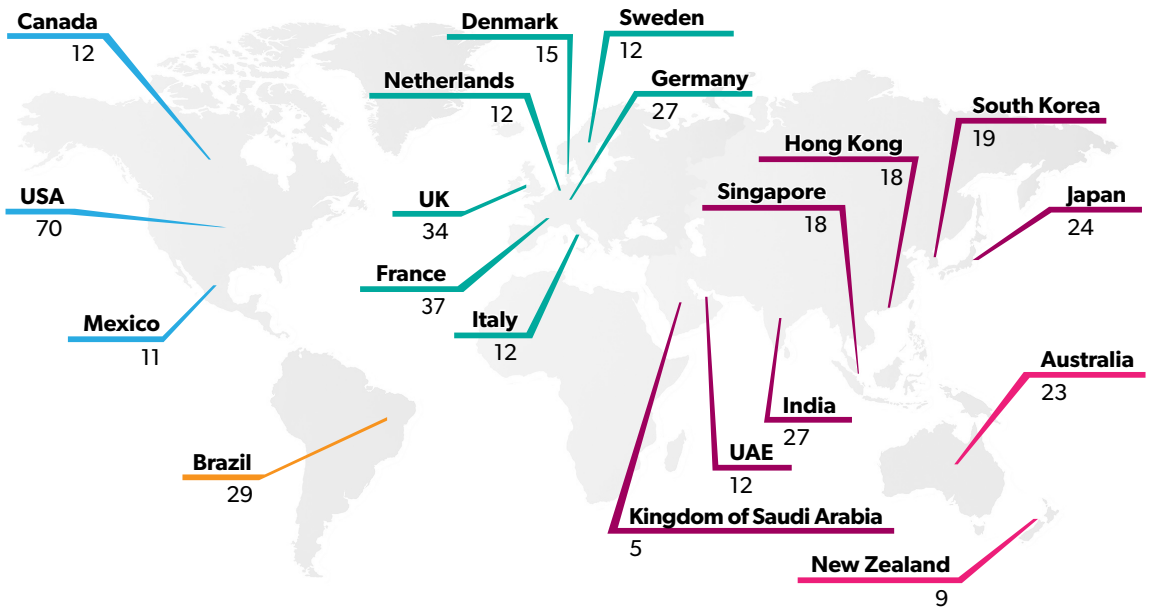
- **Strengthen fundamental data security and management:** Enhance efforts to understand and map the full scope of organizational data storage locations, both on-premises and in the cloud. A significant portion of organizations are not fully confident that they know where their data is stored. Prioritize initiatives to fully classify all organizational data, recognizing that only 41% of retail organizations can fully classify all their data. Increase the encryption of sensitive data stored in the cloud, as retail organizations on average reported that nearly half (47%) of their sensitive cloud data remains unencrypted. Address underlying issues that lead to compliance audit failures, since 40% of organizations failed a compliance audit in the past 12 months. Businesses can achieve many of these objectives by improving their overall data security posture with platforms that offer unified visibility, monitoring, control and protection.
- **Improve breach prevention and incident response:** Invest in robust breach prevention and response strategies for both cloud and on-premises environments, given that 16% of retail respondents experienced a cloud breach and 14% experienced an on-premises breach within the last 12 months. Implement stronger controls and training to mitigate misconfiguration/human error, which remains the leading root cause of data breaches. Ensure timely patching and vulnerability management to address the exploitation of known vulnerabilities, cited as the second most common root cause of breaches.
- **Optimize security tooling and capabilities:** Address security tool sprawl and complexity by focusing on consolidation where feasible and tackling barriers such as incompatibility and operational inflexibility. Improve staff understanding and confidence in operating deployed data security tools, as only 11% are very confident in understanding all tools. Strategically invest in key security technologies, continuing to prioritize cloud security for IaaS/

PaaS, data security and key management/hardware security modules. Leverage and enhance identity and access management, network security and endpoint security.

- **Address the evolving threat landscape and actors:** Fortify defenses against malware, phishing/whaling/business email compromise and ransomware, identified as the fastest-growing types of threats for retail organizations. Develop strategies to counter threats from nation-state actors and financially motivated cybercriminals while also implementing measures to reduce accidental incidents and human error. Strengthen security for cloud-based storage, cloud-delivered applications and identity infrastructure since these are perceived as the biggest targets for cyberattacks. Prioritize mitigating credential theft or compromise and third-party vulnerabilities in cloud management infrastructure.
- **Prepare for quantum computing security challenges:** Accelerate exploration of quantum computing impacts, particularly addressing concerns about future encryption compromise (harvest now, decrypt later) and key distribution. Prototype and evaluate PQC algorithms and assess encryption strategies to prepare for quantum security threats. Develop resilience contingency plans to address potential security concerns related to quantum computing. Prioritize efforts to meet PQC adoption objectives, especially interoperability with broader ecosystems, where 32% of retail organizations are behind.
- **Secure AI adoption and mitigate AI-specific risks:** Proactively manage risks associated with the rapid evolution of AI ecosystems, issues of trust in third-party systems and potential exposure of sensitive data through AI models. Implement specific security measures to counter increasing AI/LLM attacks such as prompt injection, sensitive information disclosure and misinformation/deepfakes. Address key limitations to AI adoption, such as poor data quality and governance and the perception that AI initiatives move too quickly for proper security. Strategically invest in AI-specific security tools and services, leveraging a mix of cloud providers, established security vendors and specialized AI security startups.
- **Advance digital sovereignty initiatives:** Develop and execute digital sovereignty strategies driven by the need for full control over software and data and compliance with local, regional and global privacy laws. Emphasize control of encryption and key management capabilities as a primary mechanism to achieve cloud and data sovereignty where this provides sufficient protection. Focus on refactoring applications for logical data segmentation and reducing data outside sovereign regions to meet sovereignty objectives.

Methodology

This research was based on a segment of **426 retail and e-commerce** respondents extracted from a global survey of 3,120 respondents commissioned by Thales and conducted by 451 Research, from S&P Global, 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.



RETAIL AND E-COMMERCE ORGANIZATIONS ANNUAL REVENUE

Revenue	Number of Respondents
$100m to $249.9m	22
$250m to $499.9m	98
$500m to $749.9m	104
$750m to $999.9m	108
$1 Bn to $1.49 Bn	40
$1.5 Bn to $1.99 Bn	20
$2 Bn or more	34
Total	426

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

cpl.thalesgroup.com/retail-data-threat-report