THALES
Building a future we can all trust

#2025CloudSecurityStudy

2025

CLOUD SECURITY STUDY

Securing a Hybrid and Multicloud World

cpl.thalesgroup.com

Table of Contents

Executive Summary

Cloud-based services have become a common and critical part of enterprise infrastructure, but organizations still struggle to secure them. This latest edition of the **Thales Cloud Security Study** examines organizations' challenges, successes and strategic plans related to their cloud-based infrastructure and services. While most enterprises have integrated cloud resources into their operations, many need to improve their ability to secure these environments and the data they contain. Despite cloud security's status as respondents' top security spending priority, most organizations require significant advancement in their cloud security posture and operations. The rapid push to support AI initiatives, which are often heavily cloud-dependent, further intensifies the urgency, as effective and efficient data protections are required to deliver on the promise of AI.

This year's edition of the Thales Cloud Security Study includes insights from nearly 3,200 respondents across 20 countries, capturing executive, managerial and practitioner perspectives on the evolving cloud security landscape. As cloud infrastructure continues to expand, cloud security remains the top security spending priority for organizations worldwide. However, the growing complexity of hybrid and multicloud environments is placing increasing strain on security teams. A rising number of respondents report challenges in securing their cloud assets, an issue that is further amplified by the demands of AI projects that often operate in the cloud and require access to large volumes of sensitive data. Compounding this issue, four of the top five targeted assets in reported attacks are cloud-based. In this environment, strengthening cloud security and streamlining operations are essential steps toward enhancing overall security effectiveness and resilience.

S&P Global
Market Intelligence

Source: 2025 Cloud Security Study custom survey from
S&P Global Market Intelligence 451 Research, commissioned by Thales.

Sponsored by

Arrow Five Years Out · CLIMB · Exclusive Networks · TD SYNNEX

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

Key Findings

Cloud Remains at the Forefront of Security Considerations

64% of all enterprises regard cloud security as a pressing security discipline.

52% indicated that AI security spending is eating into or taking over existing security budgets.

Only 8% of respondents encrypt 80% or more of their cloud data.

54% of data in the cloud is sensitive, up from 47% last year.

Attacks Target Cloud Resources

54% cited an increase in direct attacks to compromise infrastructure.

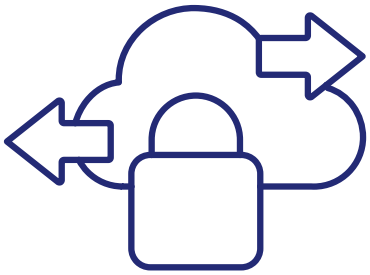
The Liability that is the Human in the Loop

68% cited credential and stolen secrets as the fastest-growing cloud infrastructure attack tactics.

Complexity is the Enemy of Cloud Security

85 The average number of SaaS applications in use, a 6% increase.

2.1 The average number of public cloud providers used by enterprises.



55% report that securing cloud environments is more complex than securing on-premises venues, up from 51% last year.

57% are using five or more key management systems, up from 53% last year.

Digital Sovereignty in a Hybrid World

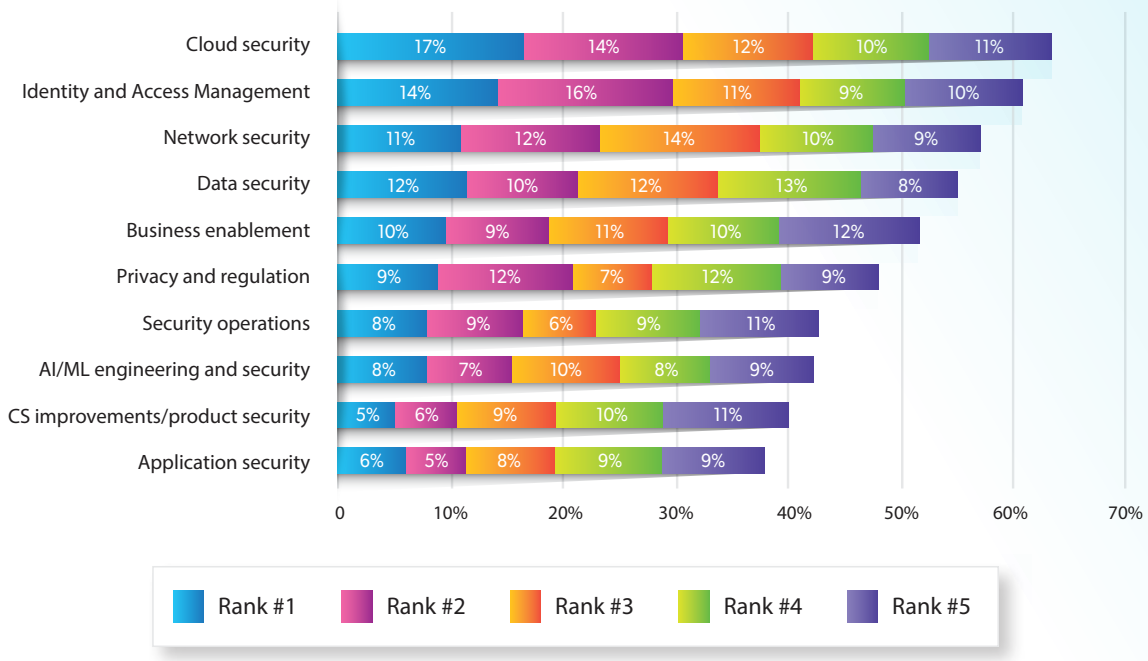
42% cite encryption and key management as sufficient to achieve sovereignty objectives regardless of data's physical location.

33% regard future-proofing portability for workloads and data as primary drivers for digital sovereignty initiatives.

Cloud Remains at the Forefront of Security Considerations

Enterprise infrastructure has evolved such that cloud is no longer simply an option — it is a key resource and an expected element in the modern infrastructure portfolio. However, many organizations are still developing their cloud operations skill sets. Securing cloud data and infrastructure requires a distinct mindset, and controls and capabilities can vary among cloud providers. That presents challenges for security teams as they work to effectively and efficiently secure their cloud assets. AI initiatives — and the resulting push to bring more data into cloud-based AI services — are adding further pressure to cloud data security efforts.

Most pressing security disciplines

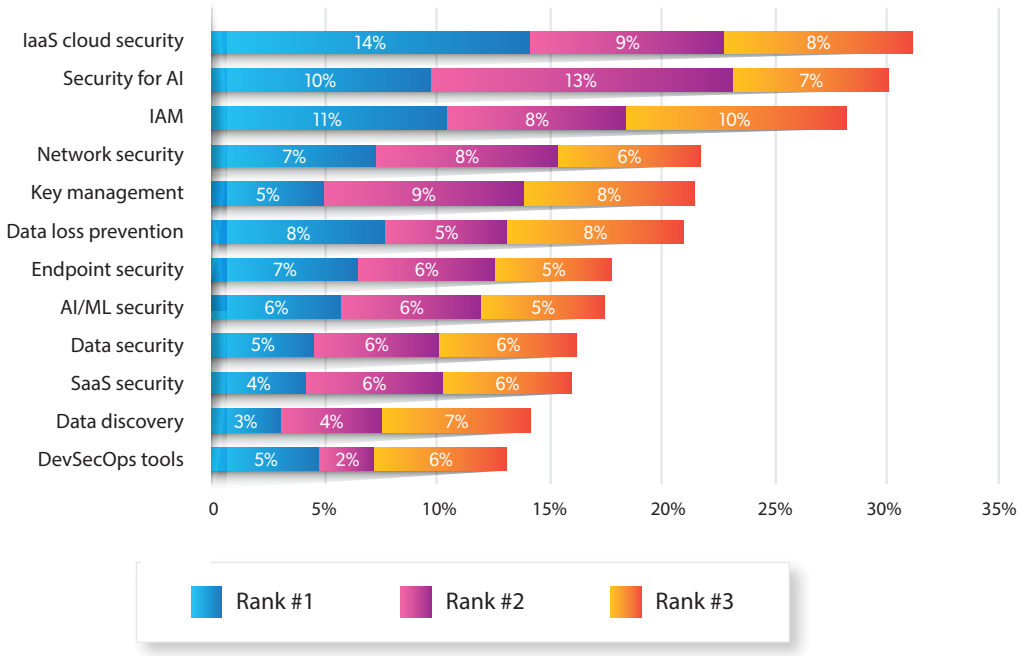


Cloud security remains the most pressing area of concern in this year's study, highlighting the ongoing difficulties organizations face. These challenges involve not only protecting cloud environments but also maintaining the skilled workforce needed to manage them effectively. Nearly two-thirds of respondents (64%) identified cloud security as one of the top five most pressing security disciplines, with 17% ranking it as the No. 1 discipline. The fact that cloud security tops the list year after year, despite considerable investment, illustrates the issue's complexity and persistence. It's not just a technical challenge, but a multifaceted one involving operations, staffing and evolving threats.

More than half (52%) of respondents indicated that AI security spending was eating into existing security budgets.

Spending on cloud security remains strong, once again topping the list of security investment priorities. Cloud services are constantly evolving with new technologies, services and security functionality. That evolution leaves enterprises playing catch-up with both their skills and capabilities, putting them on a continuous cloud journey that requires ongoing investment. The rush to deploy AI capabilities is intensifying pressure on cloud security. Security for AI, a new addition to the list of spending priorities this year, ranked second overall, highlighting its growing importance. However, the source of funding may raise questions about strategic alignment and effective resource allocation. More than half (52%) of respondents indicated that AI security spending was eating into existing security budgets. With large amounts of AI work being done in the cloud, this could impact cloud security spending.

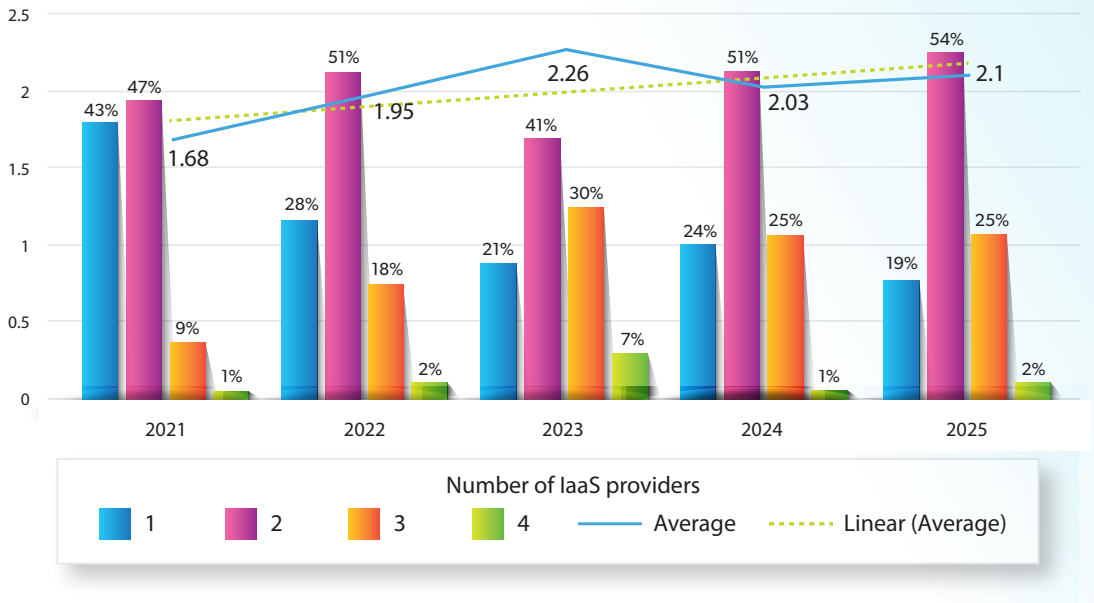
Top security technologies by spending level



Complexity is the Enemy of Cloud Security

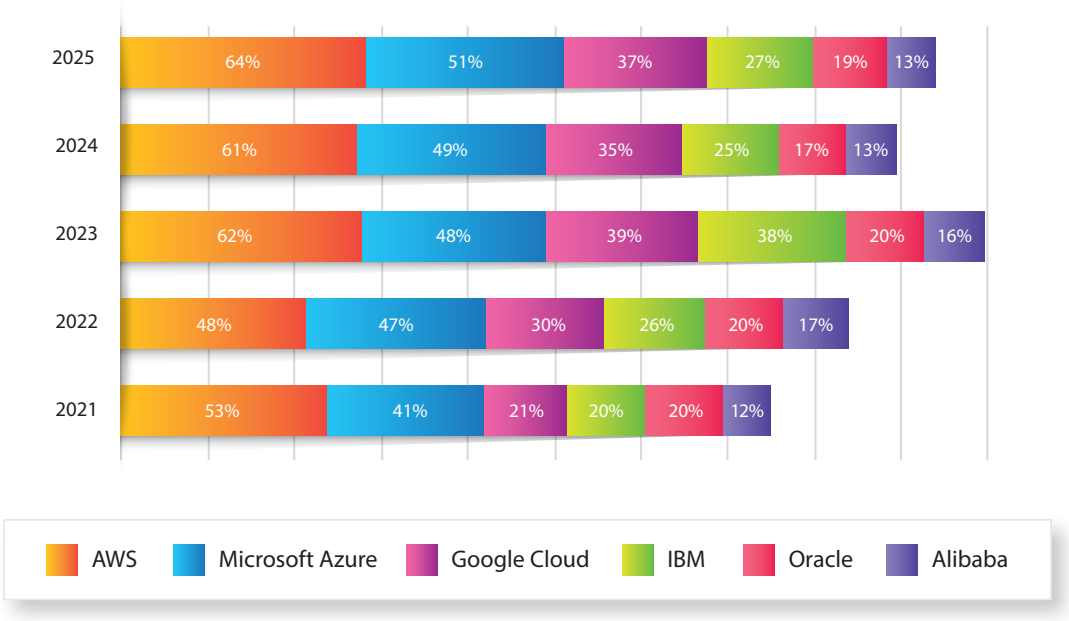
Cloud security continues to attract significant attention and investment largely because of the complexity of today's cloud environments. Most enterprises use multiple IT venues as well as multiple cloud providers, making infrastructure increasingly hybrid and multicloud. This year, the average number of public cloud providers rose slightly to 2.1 as most organizations are now managing at least two cloud platforms in addition to their on-premises systems. This growing complexity is a key driver of increasing cloud security challenges. In fact, 55% of respondents said securing cloud environments is more complex than securing on-premises infrastructure, marking a 4-percentage-point increase from last year.

Multicloud Infrastructure-as-a-Service (IaaS) adoption



Having multiple IaaS providers means security teams must be skilled in translating controls across platforms. As the chart below illustrates, adoption is growing across almost all providers. Most organizations can expect to add new providers, whether through organic growth or mergers and acquisitions.

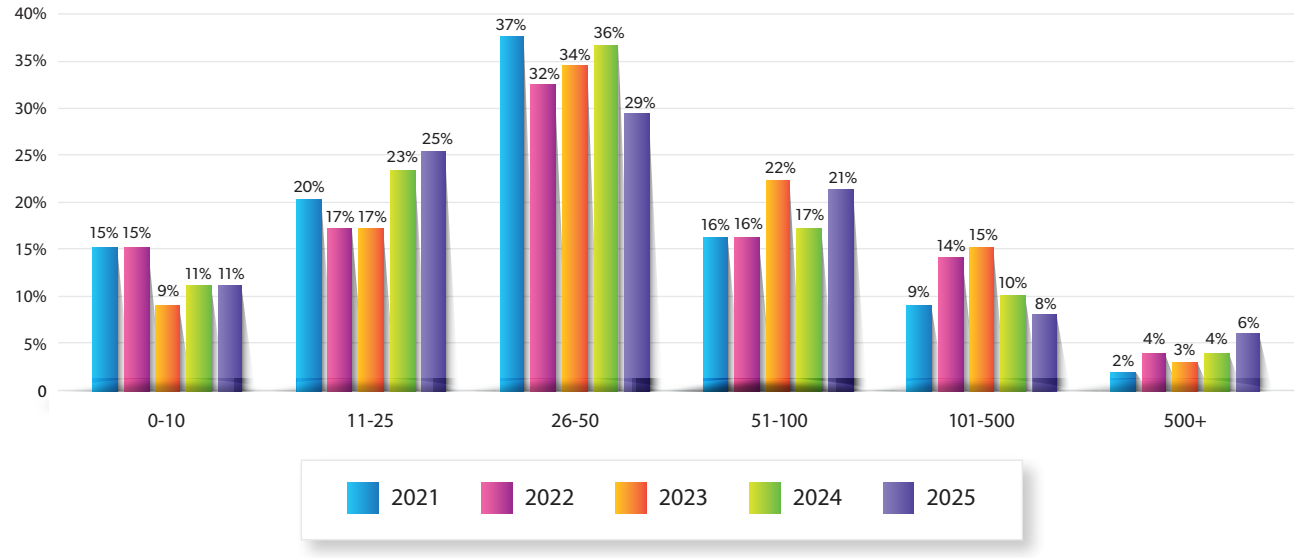
Cloud adoption trends across providers



The number of SaaS applications is also increasing. While SaaS environments can simplify some aspects of security operations, they may also be more difficult to secure, given that controls for access and data protection may be less transparent, more complex to access, and provide less visibility and control of data, which in turn has implications for data sovereignty. Respondents on average reported 85 SaaS applications in use, a 6% increase from last year. When working across multiple cloud environments and SaaS applications, with different controls and levels of operational visibility, security teams may struggle to align all elements with their existing policies and procedures, especially regarding the security of identities, access and data.

Respondents on average reported 85 SaaS applications in use, a 6% increase from last year.

Software-as-a-Service (SaaS) application counts



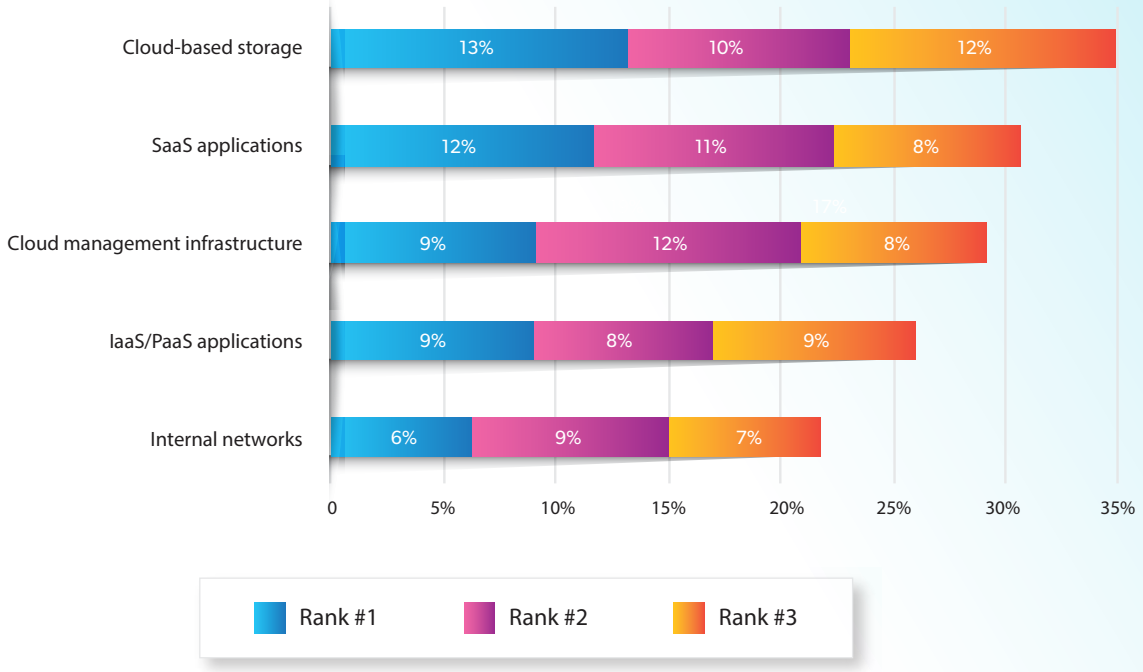
Security Tool Sprawl

The growing number of security tools, often referred to as tool sprawl, is further complicating cloud security. The saying that complexity is the enemy of security holds especially true in the context of cloud data security, as reflected in the study's findings. Nearly two-thirds of respondents, or 61%, reported using five or more tools for data discovery, monitoring or classification. Similarly, 57% of respondents use five or more enterprise key managers to manage encryption. This proliferation of tools increases the risk of misconfiguration and operational errors. When working with multiple cloud providers, it may be tempting to use a separate key management system for each provider. The native key management systems are the default in their respective clouds, they don't easily extend to other clouds, and they can be challenging to integrate with on-premises key management systems. Given that the average enterprise has more than two cloud providers, that can create islands of management, making encryption life-cycle management more complex. To streamline data protection, key management must be integrated across the full infrastructure portfolio and extendable to new cloud providers as they are brought on board. Managing keys with a common, unified platform can simplify operations and improve data protection.

Attacks Target Cloud Resources

Cloud infrastructure has become a primary target for attackers. As cloud adoption has surged and organizations continue to face challenges in securing these environments, threat actors are seizing the opportunity. According to the study, four of the top five reported attack targets are cloud-based. As attackers place greater value on data, they are naturally gravitating toward the environments where data is most concentrated. Cloud platforms often present a broader attack surface, increasing the likelihood of compromise if not properly secured.

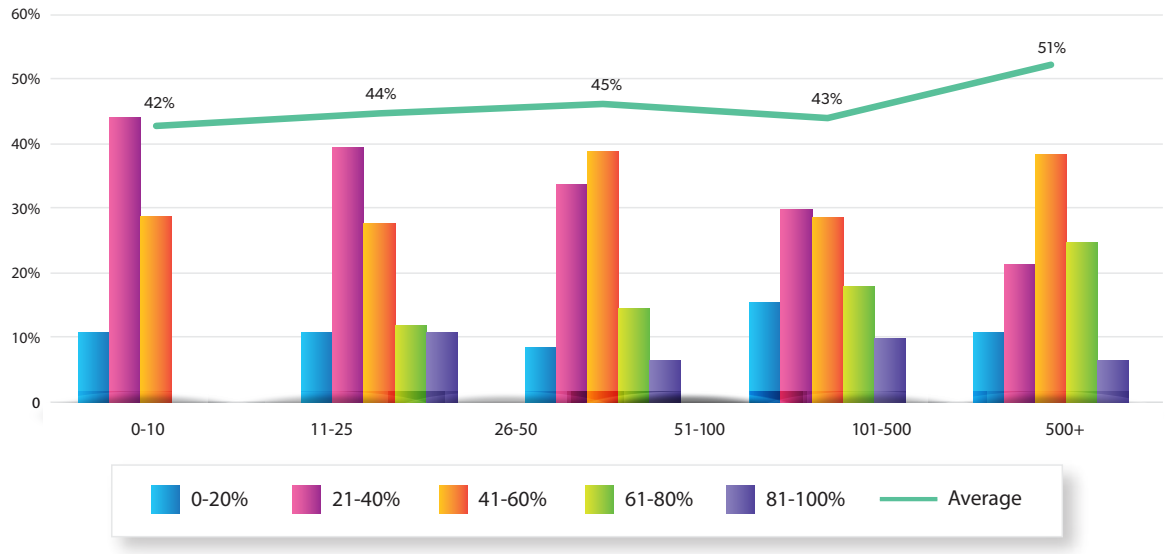
Top cloud security targets



The most prevalent types of attacks on cloud infrastructure are changing. While about half of respondents cited an increase in direct attacks to compromise infrastructure (54%), more than two-thirds reported an increase in access-based attacks leveraging stolen credentials and secrets (68%). This presents a critical risk where access controls are the lone protection for data. Meanwhile, organizations continue to place more sensitive data in cloud: 85% of respondents reported that 40% or more of their cloud data is sensitive, up from 61% of respondents last year. Encouragingly, organizations on average reported that they are encrypting an increasing proportion of their sensitive cloud data, but the figure remains far short of where it should be. Considering the increasing prevalence of authentication-based attacks, encryption must be in place to thwart attackers who break through access protections.

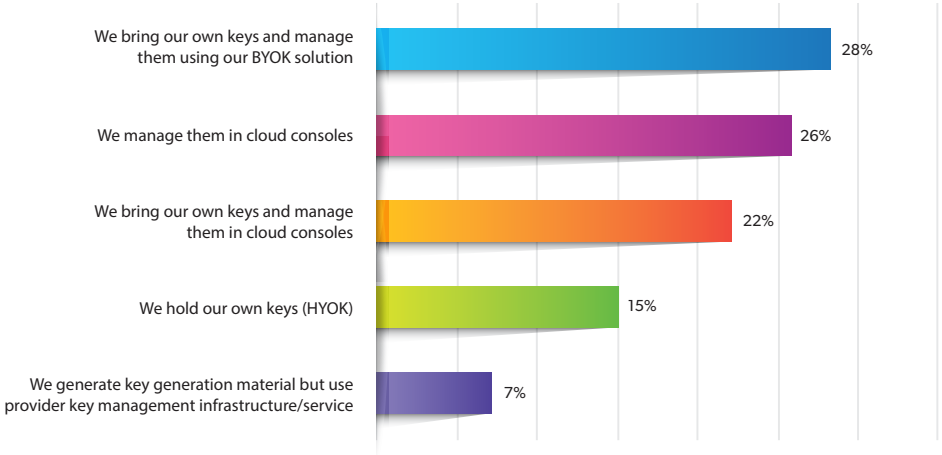
However, access protections need improvement, as well. While use of more sophisticated authentication is growing, only 65% reported that multifactor authentication (MFA) is in place to defend cloud access. The combination of weak authentication and unencrypted sensitive data represents a critical risk for enterprises.

Proportion of sensitive cloud data that is encrypted



There is encouraging progress in how organizations are approaching key management. This year's study shows an increase in the use of bring-your-own-key (BYOK) strategies, with 28% of respondents using this method, up from 25% last year, making it the single most common approach. However, 48% still manage encryption keys through cloud provider consoles, which continues to add complexity, especially in multicloud environments. To manage keys effectively and reduce operational burden, a unified key management system is becoming essential.

Methods for controlling encryption keys



Digital Sovereignty in a Hybrid World

Greater use of the cloud raises concerns about data sovereignty. Although one of the benefits of cloud has been that organizations didn't have to worry about location, data sovereignty mandates have turned this into an area of concern. Effective data management capabilities are critical to meeting digital sovereignty requirements. In fact, encryption-based data protections (42%) are broadly considered an effective means to mitigate data location concerns. Of course, regulatory requirements may mandate that data reside in a particular location, but the top reported driver for data sovereignty efforts is to ensure data and workload portability (33%), significantly ahead of meeting local (16%) or global (21%) regulatory mandates. This is consistent with last year's results, indicating a strong focus on cloud portability.

Encryption-based data protections (42%) are broadly considered an effective means to mitigate data location concerns.

The Liability that is the Human in the Loop

AI adoption grows, there are increasing calls to keep humans in the loop to validate AI decisions and actions. However, in security, human fallibility remains a weak link. This point of contradiction is reflected in the survey data, which reveals a disconnect between organizations' concerns and the actual causes of breaches. While external attackers are the primary concern, human error remains the leading cause of security breaches.

Human error ranks third among reported attack concerns. This discrepancy reflects an issue regarding how organizations are prioritizing protections, particularly in cloud. The skills gap and increasing complexity of cloud security operations only make this situation worse. Credential and stolen secrets attacks were cited as the fastest-growing cloud infrastructure attack tactics (68%). As discussed earlier, compromising a user's identity can give an attacker access to unprotected data.

One effective way to reduce error is to reduce the possibility of error by increasing the strength of authentication controls. The study results show some positives here. For example, MFA remains the most widely deployed mechanism to secure cloud access (65%), but it is not universally applied. Phishing-resistant authentication techniques were added to the study this year, and biometrics and passwordless approaches showed notable levels of adoption. Adoption of privileged access management (PAM) — a technology that could be particularly effective in cloud environments — remained relatively low (38%). Organizations can also reduce the possibility of error by simplifying security operations through consolidation and integration.

Reported attack concerns

2024	2025
External attackers — hacktivists	**External attackers — hacktivists**
Human error	**External attackers — nation-state actors**
External attackers — nation-state actors	**Human error**

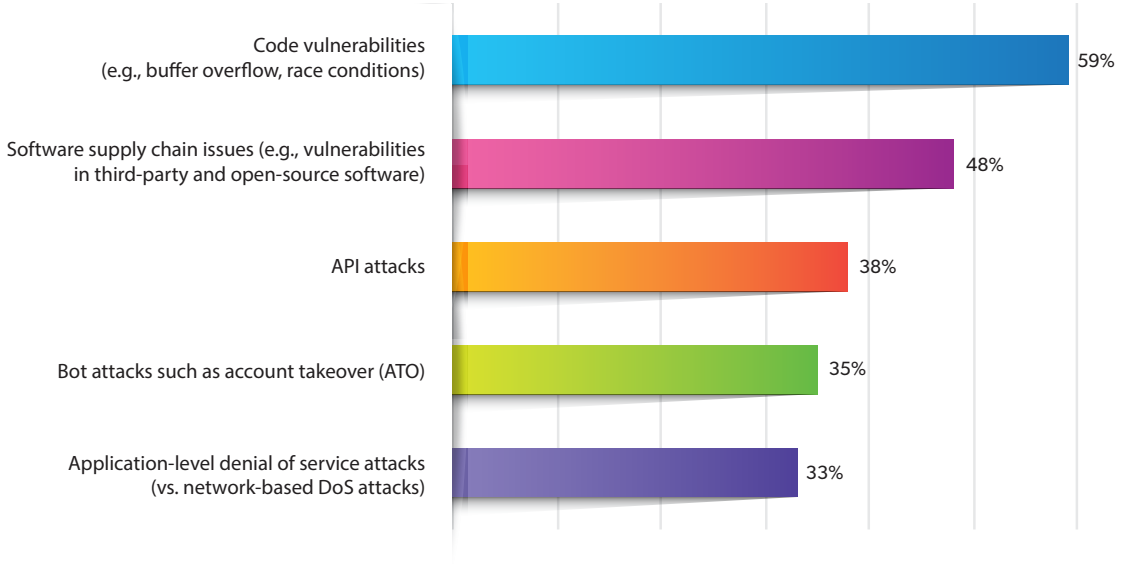
Credential and stolen secrets attacks were cited as the fastest-growing cloud infrastructure attack tactics (68%).

AppSec and DevOps Security and the Cloud

Many of the latest advancements in application development and architectures take place in cloud infrastructure. Implementing cloud-native development methods and infrastructure as code can speed the delivery of new applications. However, these advances also require new security measures to address both the scope and the velocity of application deployment and operation. Foremost is the need to secure the growing use of APIs. Automating cloud operations relies heavily on APIs, and more than a third of organizations reported using 500 or more.

Mature use of AI services also typically takes place through APIs, making their security critical to AI initiatives. Regarding application security, concerns about API attacks (38%) took a back seat to code vulnerabilities (59%) and software supply chain issues (48%). However, it is important to note that APIs themselves are also subject to code vulnerabilities, and that an API can become a vector of access for an upstream supply chain compromise.

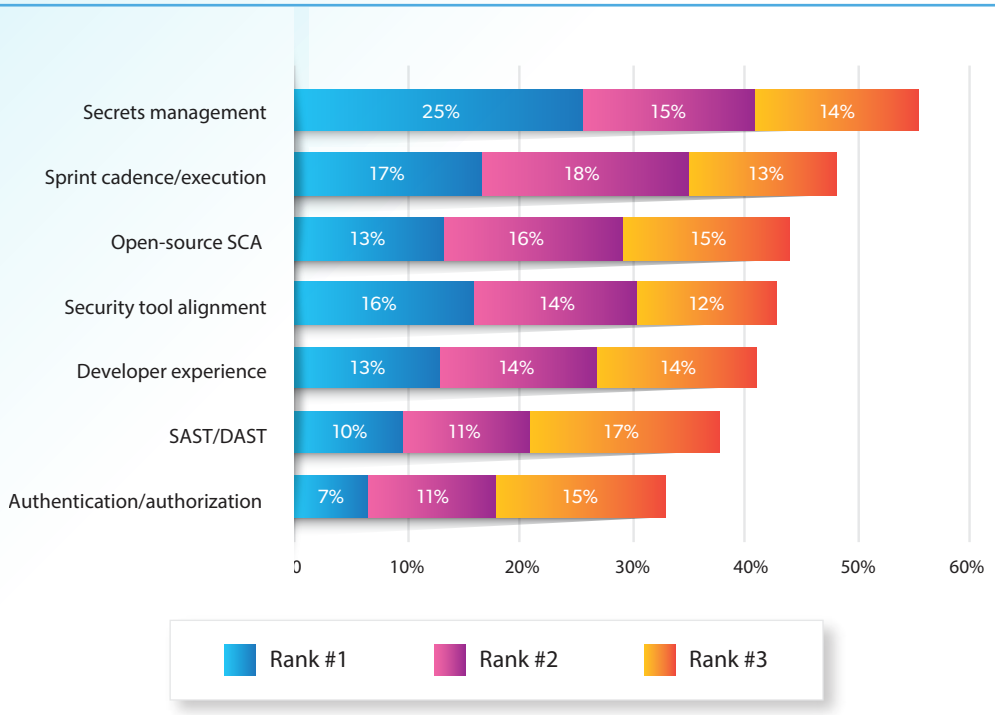
Top concerns about application security



Secrets management was cited as the top application development security challenge. The concern is well founded, given that misappropriated secrets top the list of cloud management infrastructure attack vectors. Effectively managing credentials and secrets is critical in cloud environments, but it can be challenging for development teams to master the skills in implementation and even more of an issue for security teams to assess the resilience of application environments. Approaches such as platform engineering, where development pipelines are built with validated tool chains, can be effective. Concerningly, only 16% identified DevSecOps tools for secrets management as one of the top three most effective technologies for protecting data. Given the limited degree of encryption applied to sensitive data in cloud, this poses a significant hazard. By abusing compromised secrets, attackers can gain access to unencrypted data.

Securing cloud applications requires not only knowing where data is stored but also being able to classify and protect it effectively. Data management, classification, encryption and access protection must all work together seamlessly.

Top DevSecOps challenges



Progress to a More Secure Cloud

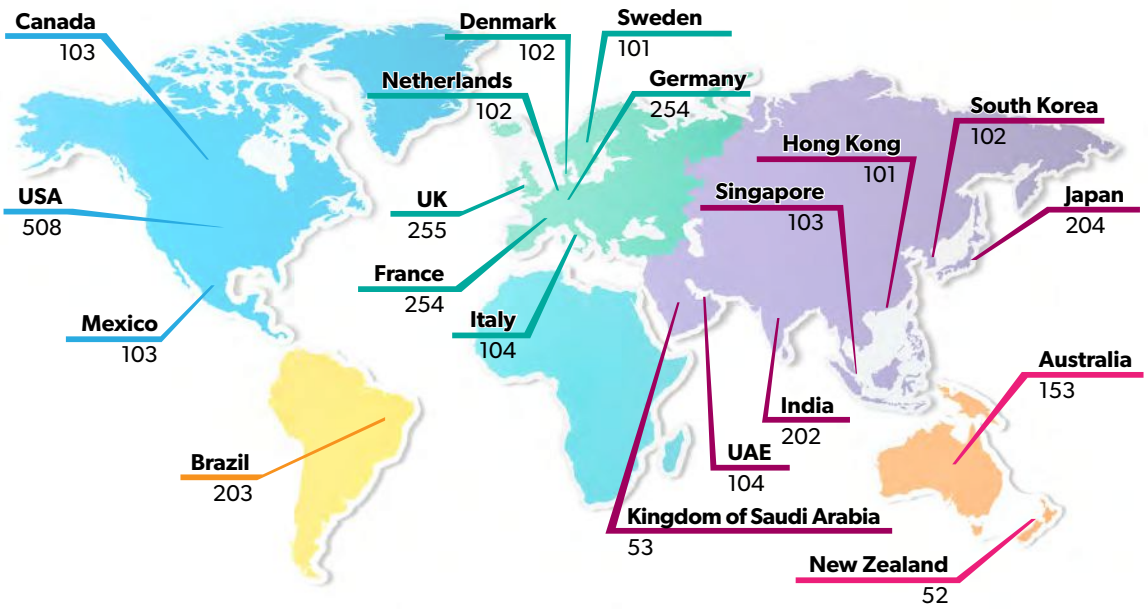
Cloud has become a fundamental component of modern enterprise infrastructure, and organizations must secure its use effectively to maintain customer trust and remain competitive. While encryption use is improving as a data protection measure, much remains to be done. The significant portion of unencrypted sensitive data in the cloud represents a manageable risk that organizations should address with urgency. Organizations must also simplify cloud security management by integrating tools and leveraging common platforms. A unified security management system that spans both on-premises and cloud environments reduces the burden on security teams while easing adaptation to changes in workloads or cloud providers, enabling innovation and optimization. These changes are exemplified by the growing use of AI and its expanding demands on security budgets, infrastructure and data availability. Security management must lead the way in responding to these shifts, rather than holding organizations back. The modern enterprise runs on hybrid IT infrastructure, and security systems should reflect that reality.

Organizations must also simplify cloud security management by integrating tools and leveraging common platforms.

Improving the productivity and efficiency of security teams is key to reducing human error, which remains the leading cause of cloud data breaches. By creating a unified security environment, organizations can free up security teams to focus on strategic initiatives, unlocking new business opportunities and harnessing the potential of emerging technologies such as AI. Effective cloud security helps to give enterprises a strong foundation from which they can innovate boldly and embrace the future with confidence.

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 regarding level of knowledge on the general topic of the survey, the screening criteria for the survey excluded respondents affiliated with organizations with annual revenue of less than US$100 million, and with revenue of 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/cloud-security-research