Global Edition

SafePloy 安策

THALES
Building a future we can all trust

2024 CLOUD SECURITY STUDY

Boom Times for the Cloud: Is Security Ready?

#2024CloudSecurityStudy

cpl.thalesgroup.com

Table of Contents

Introduction

The 2024 Thales Cloud Security Study is in its fourth consecutive year of research. This year's study revisits the latest trends affecting cloud security. With 3,000 respondents from 18 countries across 37 industries, the report reflects the insights of individual contributors and managerial and executive levels within enterprises ranging from $100M USD to +2B USD in annual revenue/turnover.

Along with its sister report, the Thales Global Data Threat Report, this 2024 Thales Cloud Security Study looks into aspects of cloud security and revisits the impact of a dynamically expanding and complex attack surface. Unprecedented demand for compute and a growing volume of data challenge priorities for achieving better, more secure cloud adoption. Fittingly, despite cloud workloads becoming increasingly short-lived, cloud computing has become a more permanent technology for enterprises. While workloads and new architectures in the cloud are increasingly modular and dynamic, the evolving demands they bring for operations and security are constant and increasing.

S&P Global
Market Intelligence

Source: 2024 Data Threat Report custom survey from S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

CLICO

edvance
value added distributor

EXCLUSIVE NETWORKS

Key Findings

Cloud resources have become the biggest targets

When asked about **the leading targets in the cloud for attacks,** the top three prioritized answers were all cloud-based:

- **31%** prioritized SaaS applications
- **30%** prioritized Cloud Storage
- **26%** prioritized Cloud Management Infrastructure

Human action can compromise security

Fueling this concern is the high **number of cloud data breaches**, with 44% of respondents reporting such an incident. 14% reported a breach in the past 12 months.

44%

Human error, issues with vulnerability and configuration management, and failures to use Multi-Factor Authentication (MFA) are all cited as leading contributors.

Investing in cloud security

The need to address cloud security is the highest priority for security spending. At 33% of respondents, cloud security tops all other security spending categories in this study.

33%

Securing sensitive cloud data

On average, **47% of data in the cloud is sensitive** – yet cloud data encryption rates remain stubbornly low with less than 10% of enterprises claiming they have encrypted 80% or more of their cloud data.

47%

Cloud security is a top priority – for now and in the future

65% Nearly two-thirds of respondents (65%) identify it as a current concern.

Even more **(72%)** say it is a future concern – the most frequently cited among all security categories listed in the survey.

Surprisingly,

The #1 driver for digital sovereignty initiatives

was not compliance; it was the need to **'future-proof' the portability of cloud resources**, where enterprises could independently control digital assets regardless of location, operational personnel or software compatibility constraints. The satisfaction of global privacy frameworks was a distant second, at 22%.

#1

Cloud complexity is a significant challenge to compliance and privacy

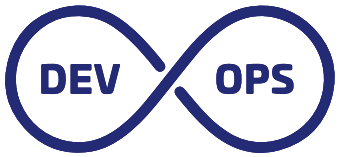
Nearly half of respondents said they 'agree' or 'strongly agree' that it is more difficult to manage compliance and privacy with cloud complexity – the fourth year that this has remained near or above 50%.

Here, too, complexity challenges the management of encrypted content. The number of key management systems in use remains high, with 53% indicating that they use five or more systems.

The impact of developer and operator experience

Cloud security affects and is affected by DevOps — the integration of cloud technology development, implementation and operations. Among the challenges of incorporating security into DevOps for cloud, secrets management is the top-cited issue at 56%.

56%



Fortunately, DevOps process maturity in the cloud is on a good footing, with 53% reporting a formal security champions program.

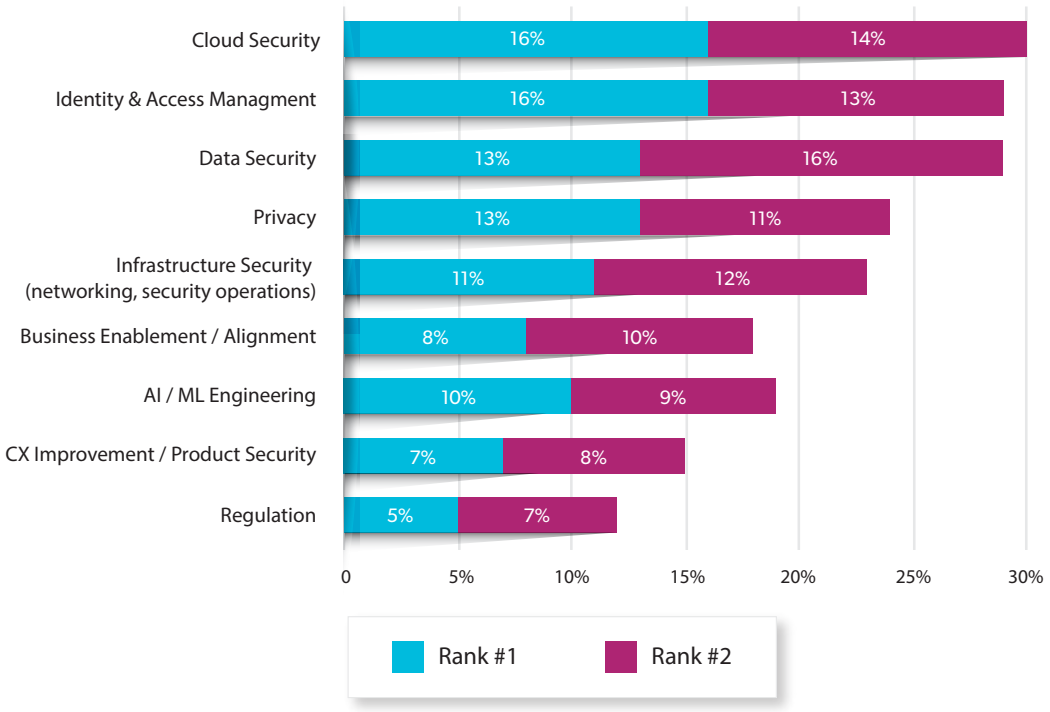
Top-Ranked Enterprise Security Priorities

Cloud, data and access: the top-ranked security priorities

Over the last several years, cloud computing has grown from an innovative IT alternative to a strategically vital focus for a wide spectrum of technology. Today, that strategic criticality has made cloud security an enterprise priority. While nearly two-thirds of this year's respondents (65%) see cloud security as among the most pressing current security disciplines, even more (72%) identify it as a source of emerging concern — the most frequently cited among all security categories identified in our survey.

However, respondents are also prioritizing data security and identity/access management among security disciplines. These domains, along with cloud security, stand out as key areas of focus.

The most pressing security disciplines



Source: S&P Global Market Intelligence 451 Research's Cloud Security Study 2024

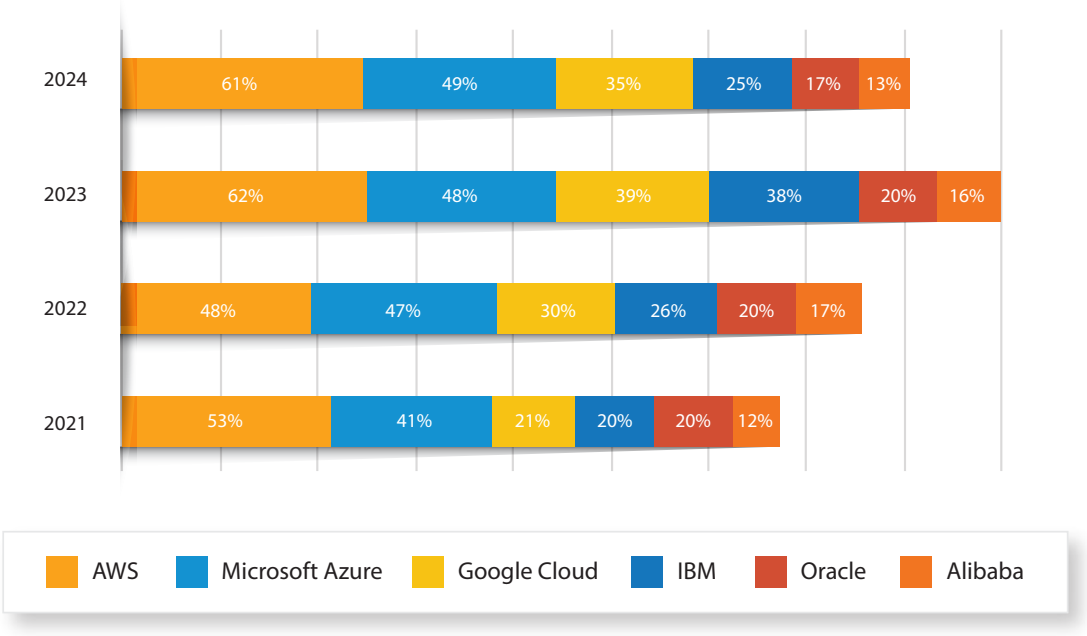
The Impact of Cloud Complexity on Shaping Security Demands

Cloud complexity amplifies the challenge

A substantial contributor to these priorities is the sheer complexity of enterprise cloud environments. The demand for a host of cloud computing approaches and techniques has given rise to a highly diverse market, where any one organization may be served by multiple providers and deployment models, each with its own security needs.

This year's survey data shows that multicloud remains the reality for enterprises, with the average number of cloud providers declining slightly to 2.02 from 2.26 last year. Industry verticals do not have a substantial bearing on this number; in our findings, the average enterprise has just as many cloud providers across banking, financial services and insurance respondents.

Adoption patterns - public cloud providers

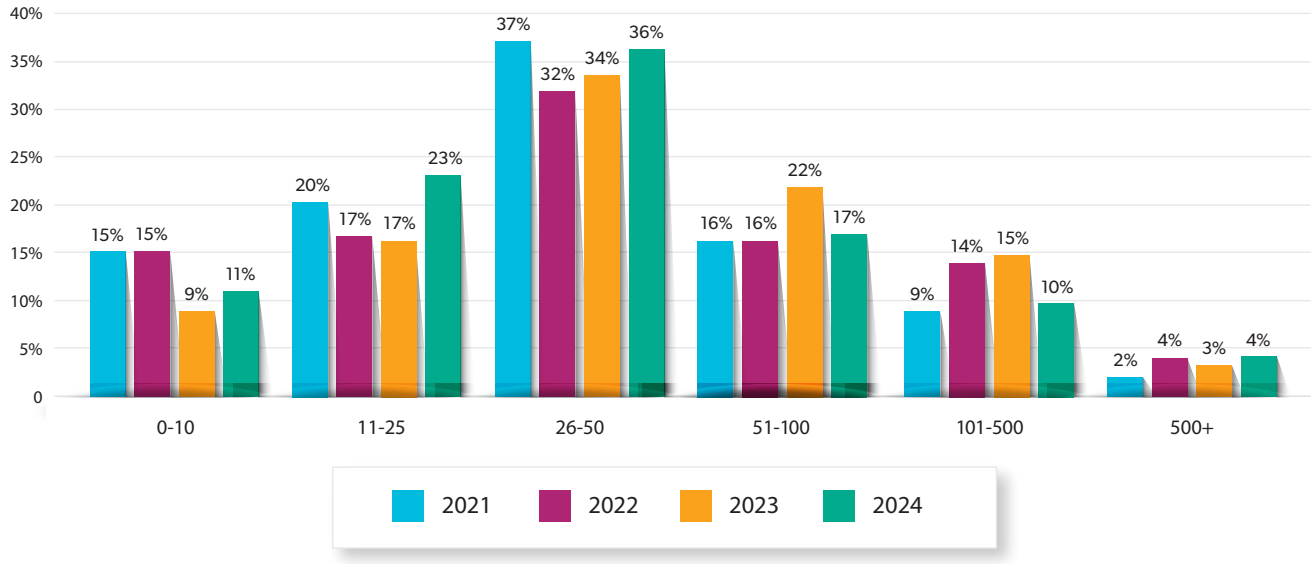


Source: S&P Global Market Intelligence 451 Research's Cloud Security Studies 2021-2024

Cloud offerings are also growing in diversity, with new offerings for generative AI and the underlying access to high-speed graphics processing unit (GPU) arrays. Even if enterprises have a single public cloud provider, there remains tremendous technology variety. AWS featured one SKU in its original launch, today the **451 Research Cloud Price Index** tracks over 100,000 AWS SKUs.

Nor is that variety confined to the plethora of offerings among infrastructure as a service (IaaS) providers; adoption of software as a service is flourishing as well. More than 60% of respondents report more than 25 SaaS applications, and 30% have more than 50. Securing SaaS applications presents a range of particular problems.

Number of software as a service (SaaS) applications in use



Source: S&P Global Market Intelligence 451 Research's Cloud Security Studies 2021-2024

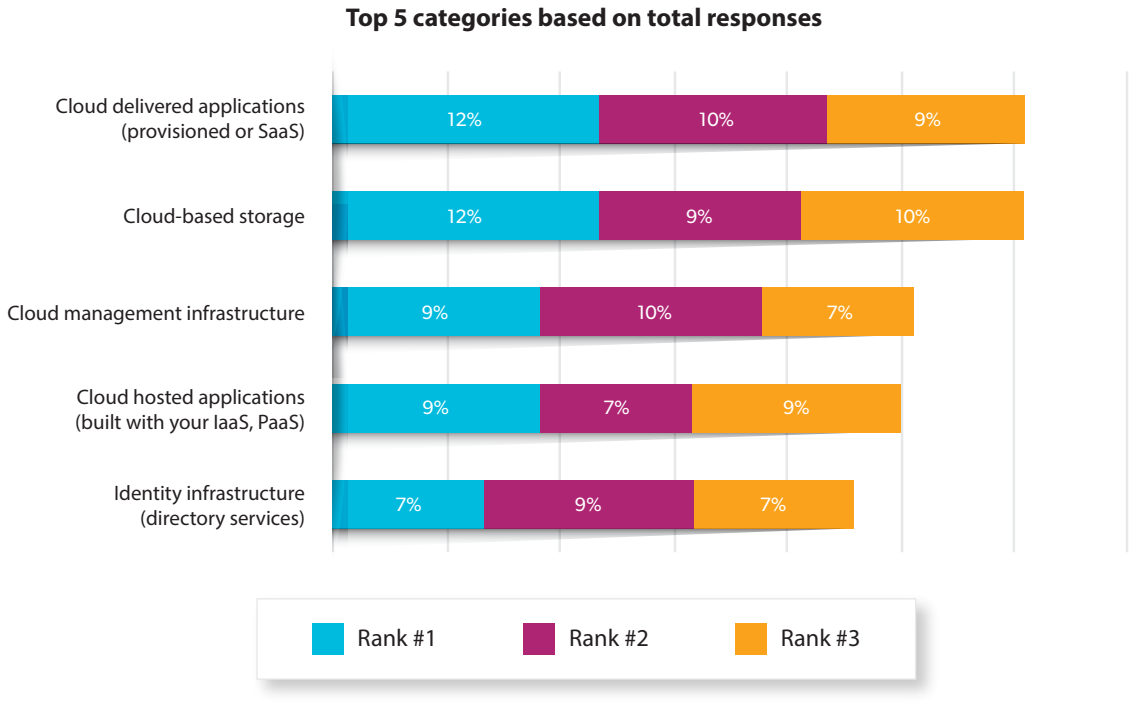
It is, therefore, hardly surprising that 51% agree that it is more complex to manage privacy and data protection regulations in a cloud (multicloud/hybrid) environment than on-premises. Nearly one in five (18%) agree strongly with that statement. Additional factors beyond the scale and complexity of cloud resources and deployment options include the scope changes in organizations undergoing transformation and the highly dynamic and ephemeral nature of cloud resources. Workloads are spun up and down to satisfy highly elastic demand. Machine identities in such environments vastly outnumber human accounts. The organizational challenges of finding and retaining people with cloud security expertise is a further complication.

The Rise of Cloud Resources as the Biggest Targets of Attack

Cloud resources have become the biggest targets

Given these priorities and concerns, and the complexity of cloud environments that motivate them, it is not surprising that cloud resources predominate among the top-ranked targets of cyberattacks, followed by a notable finding on the targeting of identity infrastructure.

Top-cited targets for cyberattacks



Source: S&P Global Market Intelligence 451 Research's Cloud Security Study 2024

The inclusion of two categories of infrastructure among top targets — identity and cloud management — is noteworthy. Of those who identified cloud management infrastructure as a target, the greatest proportion cited underlying infrastructure compromise (72%) as a target of increasing attacks. There is motive in attackers targeting the supporting infrastructure for critical cloud security controls:

- Infrastructure compromise to help adversaries persistently navigate and access cloud environments is a grave risk; further compromise to disable auditing or monitoring in that infrastructure would almost certainly increase attack severity.
- Compromising identity and access architecture opens the door to giving attackers more than just access to individual accounts. It could give attackers broad latitude within the target environment.

Given the criticality of their potential impact if compromised, these environments must be sufficiently hardened. They require highly resilient controls on access and interaction, such as strong authentication and authorization, cryptographic security, and the threat-resistant management of materials critical to control, such as secrets and cryptographic keys.

KEY STATISTIC

Of those who identified cloud management infrastructure as a target, the greatest proportion cited underlying infrastructure compromise (72%) as a target of increasing attacks.

72%

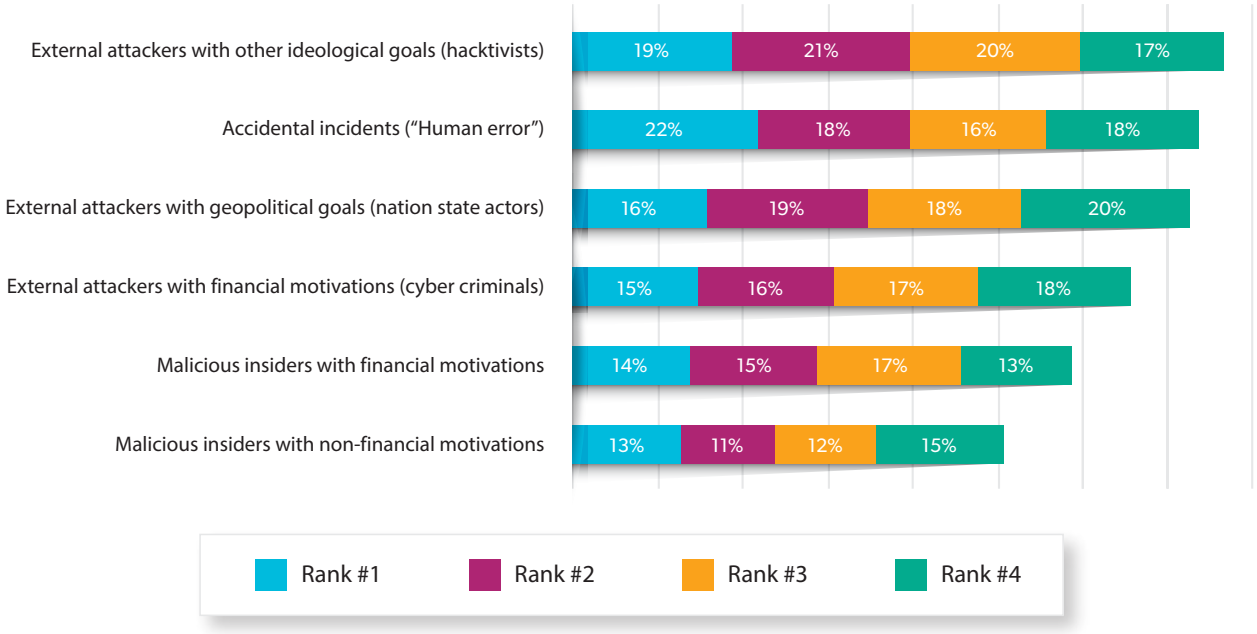
Implications of Human Factors in Cloud Security

The human factor

The inclusion of identity resources among top targets is significant for another reason: identity and access management (IAM) is a primary means of linking people with policy and control over technology access and use. Infrastructure and technology aren't the only aspects of cloud environments exposed to risk. Technology, after all, exists to serve people — which means that the interaction of people with technology, and the degree to which human action can compromise technology, is a factor in cybersecurity.

The impact of human interaction is evident in the types of threats respondents are most concerned about. **While external attackers and malicious insiders ranked highly, human error — evident in incidents such as unintended actions — was often ranked number one.**

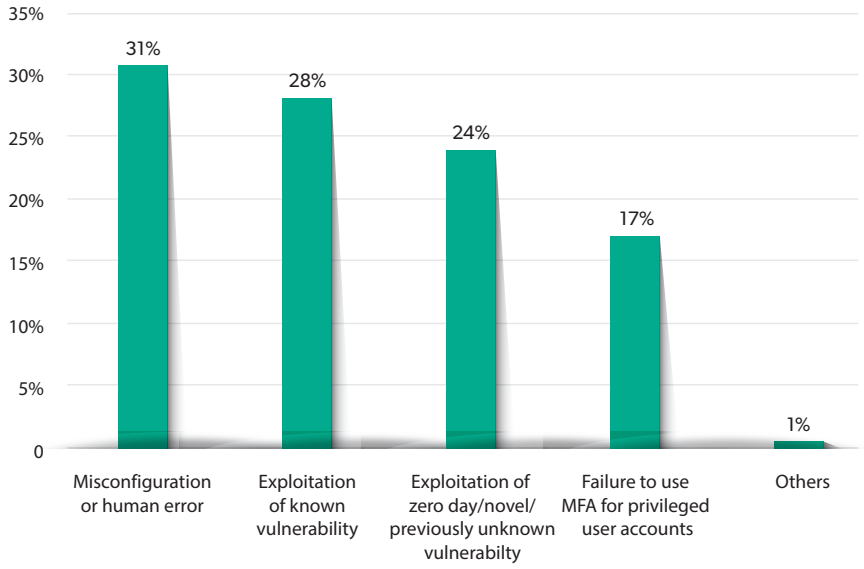
Threat categories of greatest concern



Source: S&P Global Market Intelligence 451 Research's Cloud Security Study 2024

The impact of human factors is further evident as the leading root cause of data breaches in the cloud. In this study, 44% of all respondents reported having experienced a cloud data breach, and 14% had experienced such an incident in the past 12 months. Among all those who reported a cloud data breach, 31% identified misconfiguration or human error as the root cause, ahead of vulnerability exploits or failure to implement controls on highly privileged access such as multi-factor authentication.

Root cause of cloud data breaches



Source: S&P Global Market Intelligence 451 Research's Cloud Security Study 2024

KEY STATISTIC

44% of all respondents reported having experienced a cloud data breach. 14% had experienced such an incident in the past 12 months.

44%

How Organizations Are Investing In Securing Cloud Assets—And How Standing Still Means Falling Behind

Investment in cloud security: Are organizations modernizing fast enough?

The strong emphasis on cloud, data, identity and access security is reflected in the areas where security teams are investing. Security for IaaS and platform as a service (PaaS) environments was the top category of security spending, reported by 33% of all respondents.

However, respondents are not as convinced about which controls are most effective in protecting sensitive data in the cloud from cyberattack. **While 24% of respondents prioritize cloud security measures as effective, other, more traditional (and arguably better-known) categories such as workforce IAM (30%) and endpoint security (31%) were chosen more frequently.** This makes for an interesting contrast, as security teams may favor the tools they are most familiar with rather than work with development teams to integrate security controls directly into cloud environments. Modern cloud security tools and techniques are increasingly implemented by developer and operator teams that often work together as "DevOps" organizations. Solutions such as secrets management and authorization are directly used by developers with potentially less oversight by central security teams. Given the ongoing changes in cloud security complexity, it's essential to consider the developer and operator experience when planning and implementing security programs.

Resisting the changing directions of cloud security implementation may also run the risk of limiting investment in these more modern security controls for the cloud. In other words, old habits may be dying hard. If security teams continue to prioritize network and endpoint security, the available "wallet share" for tackling the high-priority security challenges of the cloud may not expand as needed.

The Need To 'Future-Proof' Investments In Areas Such As Digital Sovereignty

Case in point: 'Future-proofing' digital sovereignty

The need to modernize cloud investments to stay abreast of changing needs is also evident in areas such as digital sovereignty, and how organizations plan to address it going forward. In general, digital sovereignty principles have stemmed from privacy and data sovereignty regulations for handling sensitive data. The residency, security, operation and even future compatibility of regulated cloud data has also evolved as organizations seek to make both the data and its environment sovereign to country or region. Enterprises are working to minimize data dependencies based on operator nationality, location, or even future software compatibility with any given environment.

This, however, may run counter to current cloud practices such as shared responsibility. While enterprises are experienced in shared responsibility models of security and operations within public clouds, their sovereignty motivations reflect a greater desire for self-sufficiency. This speaks to why, when asked what was driving their sovereignty requirements, respondents reported future-proof portability as the number one answer, ahead of local or global requirements or even addressing specific customer segments.

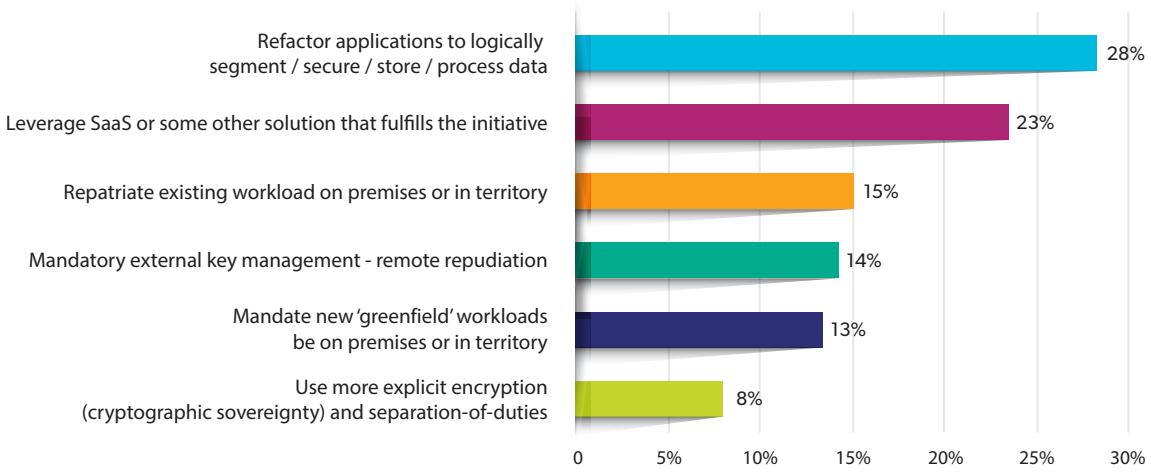
This has specific implications for how organizations factor these drivers into their cloud deployments. **For respondents who prioritized sovereignty as an emerging security concern, refactoring applications (28%) was the number one way they said they would attain sovereignty initiatives.** Other less involved approaches, such as repatriating workloads to satisfy data and operational sovereignty (15%) or transferring the risk to an external SaaS application (23%), were less popular.

KEY STATISTIC

When asked what was driving their sovereignty requirements, respondents reported future-proof portability as the number one answer.

#1

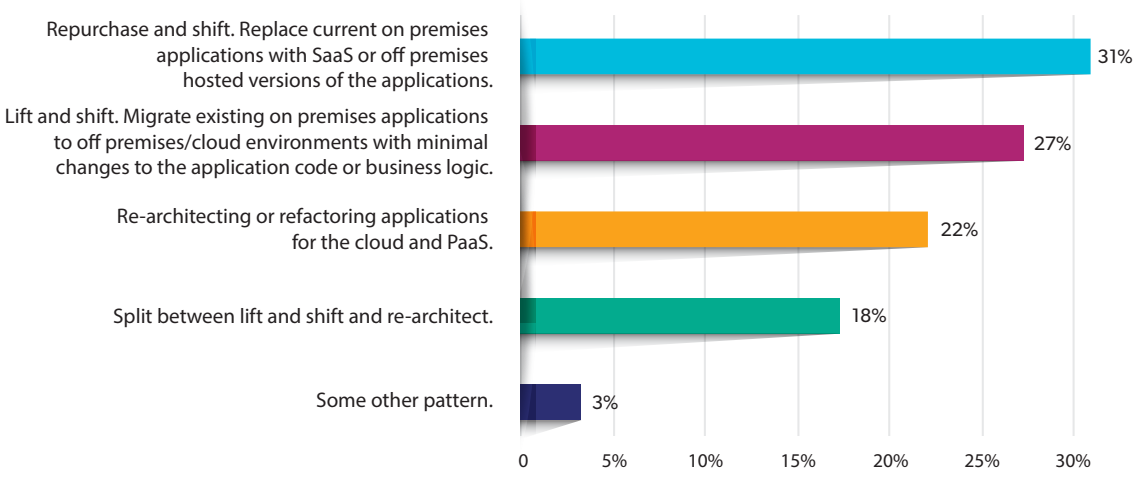
Top-cited methods for achieving digital sovereignty



Source: S&P Global Market Intelligence 451 Research's Cloud Security Study 2024

Yet this is in contrast to the primary migration strategy for IaaS and PaaS cloud applications, where respondents prioritized repurchase and shift to SaaS (31%) or lift and shift to other IaaS (27%). Refactoring applications was comparatively less popular as an IaaS/PaaS migration strategy, at 22%.

Primary migration strategies for IaaS/PaaS applications



Source: S&P Global Market Intelligence 451 Research's Cloud Security Study 2024

The promise of full software sovereignty is enticing. Enterprises must wrestle between public cloud provider lock-in and their desire to go to market with little opportunity cost. Moreover, it may not be so easy to achieve the ideal of a sovereign enterprise that can switch cloud providers freely with full software, data and operational portability. Each cloud provider may provide compatibility, but each public cloud has its own nuances and learning curve. To impose a switch without considering the effect on DevOps performance may distract the enterprise from its core competency.

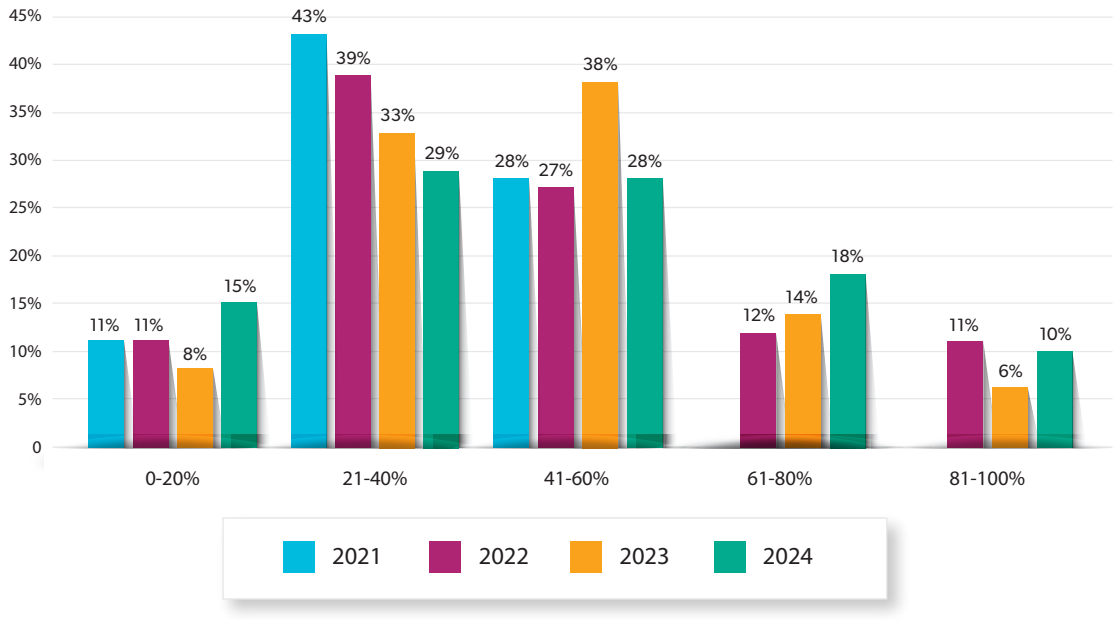
Securing cloud data: Standing still means falling behind

Just as digital sovereignty priorities illustrate the need to "future-proof" cloud investments, the pace of digital transformation centered on the cloud demonstrates how it can outstrip an organization's current approach to security. The scale and diversity of cloud resources may be growing dramatically — but if organizations maintain the same levels and types of control, they are effectively falling behind.

This is particularly evident in the growth of the cloud attack surface — and not least in an explosion of cloud data. For the last four years, this study has asked respondents what percentage of their cloud data is encrypted. The distressing finding is that the proportion of unencrypted data in the cloud remains stubbornly high. **In the most recent survey, less than 10% of enterprises said they have encrypted 80% or more of their cloud data.** Moreover, controlling for regulated industries such as finance or larger enterprises with revenue over $1 billion showed no significant difference in rates of encryption adoption. While certain technologies such as AWS S3 storage have enabled encryption by default, there are many workloads that require stronger encryption and key management controls than what is provided by the cloud service providers.

Here, too, the complexity of encryption management may be a contributing factor. More than half of respondents (53%) have five or more key management systems. As new cloud environments are added, organizations must be able to centralize their key management capabilities rather than create new ones that must be managed independently. This level of complexity also raises the risk of human error.

Percentage of cloud data encrypted

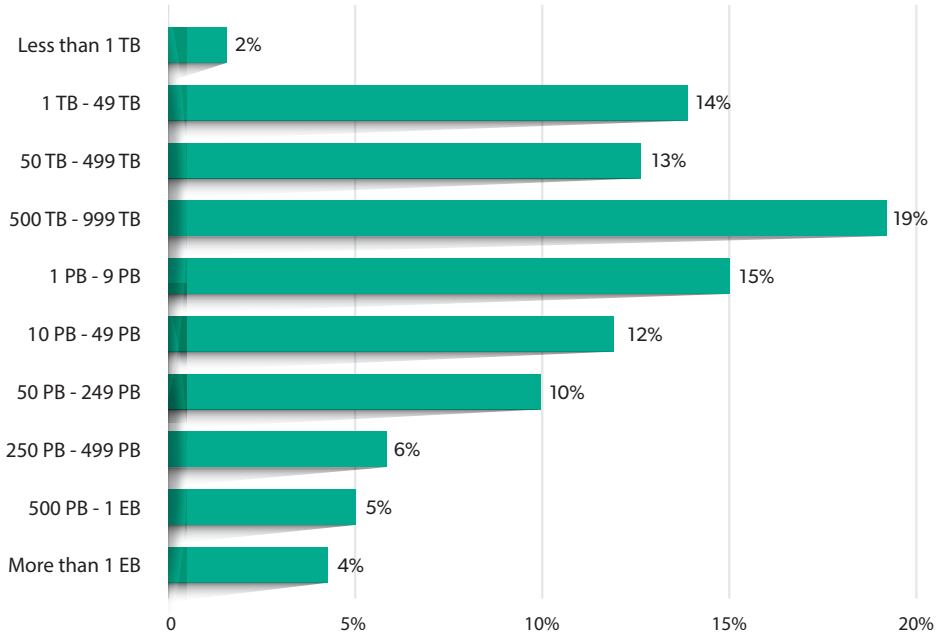


S&P Global Market Intelligence 451 Research's Cloud Security Studies 2021-2024

The sensitivity and volume of data in the cloud is growing, yet the proportional adoption of controls lags. A greater awareness of sensitive data does not correlate to greater encryption controls. **Of those who reported at least 80% of their data in the cloud as sensitive, only 58% said that data is encrypted.**

As concerning as these figures are, the growth of data, sensitive data in particular, yet to come in the cloud — and the security controls that data may require — illustrate even more dramatically how enterprises fall behind even if they maintain the status quo. Few areas highlight this more dramatically than the acceleration in the growth of cloud data demanded by artificial intelligence workloads. According to 451 Research's Voice of the Enterprise: AI & Machine Learning, Infrastructure 2023 study, one in seven respondent enterprises will use at least 250 petabytes of data to build and train AI/ML models.

Amount of data used to build and train AI/ML models



S&P Global Market Intelligence 451 Research's Cloud Security Study 2024

KEY STATISTIC

Of those who reported at least 80% of their data in the cloud as sensitive, only 58% said that data is encrypted.

58%

The DevOps Experience

The impact of developer and operator experience

As suggested by the disconnect between cloud security as a stated priority and investment in more modern techniques, this year's respondents further reveals both technological and procedural challenges with securing the cloud. Encouraging and enabling security principles to "shift left" requires the right technology and the right organization for success.

When asked about the top security challenges in their DevOps programs, respondents identified secrets management (56%) and workforce IAM (52%) as the top two challenges overall. Because workforce IAM includes privileged access management and delegated administration, it represents both a technological and organizational challenge. Other widely cited organizational challenges include difficulty achieving security sprints within a scrum framework (45%) and issues with developer experience (39%).

Within DevOps programs, 53% of organizations reported having a formal security champions program, and 49% have aligned their product and security roadmaps. Yet it remains challenging to ship products quickly. Of those respondents who said they have both a formal security champions program and aligned product and security roadmaps, 46% still are challenged to achieve security sprints.

KEY STATISTIC

When asked about the top security challenges in their DevOps programs, respondents identified secrets management (56%) and workforce IAM (52%) as the top two challenges overall.

56%

Pathways to Better Cloud Utilization

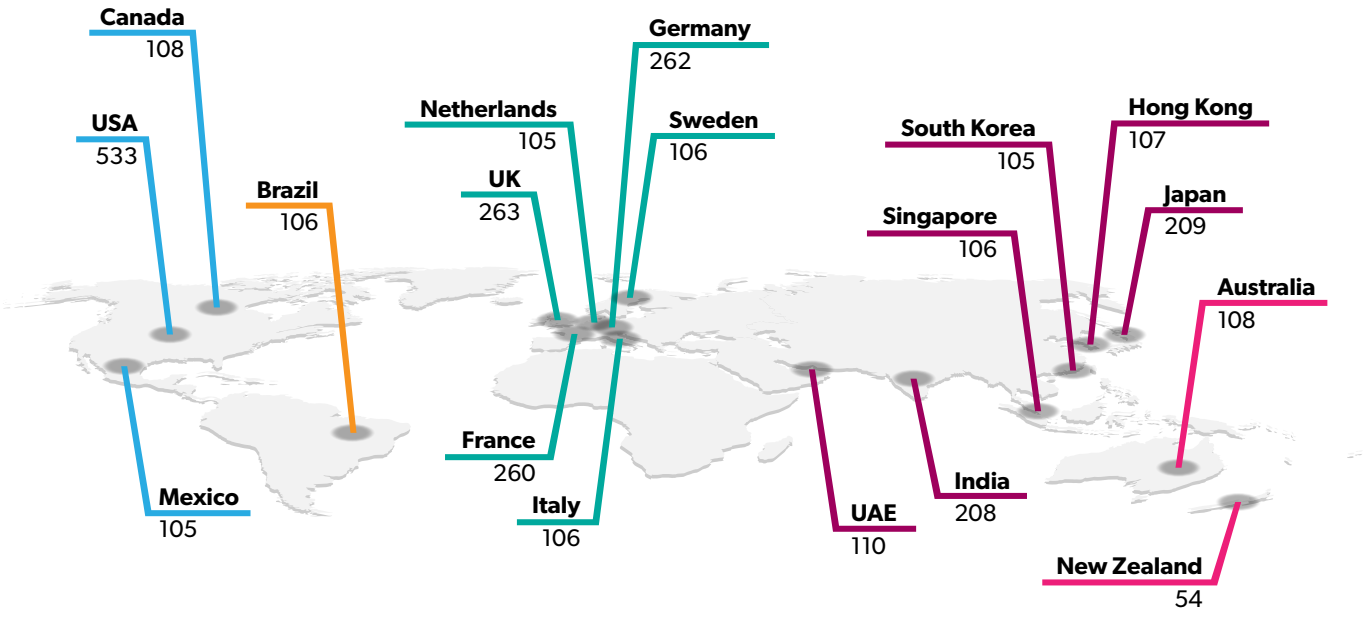
Respondents this year offered both encouragement and caution regarding improvements to cloud utilization and cloud security against the backdrop of increased cloud security threats. Respondents suggested several pathways to better and more secure cloud utilization, including:

- **Drive security proactively.** While enterprises cannot guarantee prevention of security events such as cloud data breaches, they can take measures within their spheres of control to achieve better outcomes. For instance, enterprises that successfully passed their security audits had significantly lower incidence of cloud data breaches in the last 12 months. Overall, 14% of respondents reported a cloud data breach in the last 12 months, compared to only 4% of those that passed their compliance audits.
- **Strengthen command and mastery of new cloud technologies.** While 58% of respondents said that they were deploying cloud security solutions such as cloud-native application platform protection (CNAPP) and 51% said they were using data encryption to protect cloud data, respondents still expressed more familiarity with the efficacy of existing tools. When asked what tools were effective against breaches, endpoint controls were still the most frequently cited choice.
- **Strengthen developer and security partnerships.** New threats and vulnerabilities from cloud operations will require stronger developer and security partnerships. Just over half (51%) of cloud data breaches were attributed to known and unknown vulnerabilities, and 48% of respondents reported that open-source software composition analysis was one of their greatest DevOps challenges. Vulnerability management, encryption, secrets management and identity & access management are all being democratized to address the changing threat landscape, and the imperative to form strong security and developer partnerships will only increase.
- **Offer platforms and centralized tools for decentralized teams.** Organizational alignment will better enable organizations to face common enterprise challenges and external adversaries. The decentralization of security via developer enablement and formal security champions programs allow security teams to better understand and manage the risks their lines of business face. To facilitate effective efforts among decentralized stakeholders, security teams can provide consistent and manageable tools and capabilities for developers and other teams to use. In this process, there are opportunities for consolidation and tech debt retirement. Of enterprises with formal security champions programs, 52% reported having more than five encryption key management solutions.

Significant security challenges lie ahead. Threat actors exploiting weaknesses stemming from cloud complexity target vast amounts of cloud storage and databases. Areas of vulnerability include human factors related to poor developer and operator experience. Pathways to more secure cloud utilization must be guided by security teams working closely with other stakeholders to design and build trustworthy tools and processes. Accounting for the booming growth in data and the increasing concentrations of sensitive cloud data, security teams, cloud developers and operators, line-of-business and regulatory teams must defend their enterprise data together.

About This Study

This research is based on a global survey of 2,961 respondents that was fielded in November and December 2023 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	138
$250m to $499.9m	847
$500m to $749.9m	773
$750m to $999.9m	704
$1 Bn to $1.49 Bn	216
$1.5 Bn to $1.99 Bn	103
$2 Bn or more	180

Industry Sector	Number of Respondents	Industry Sector	Number of Respondents
Retail	153	Financial Services	108
Manufacturing	150	Federal Government	106
Healthcare	144	Telecommunications	101
Technology	140	Automotive	96
Public Sector	110	Pharmaceuticals	86

THALES

Building a future we can all trust

For contact information, please visit
https://www.safeploy.com/dp

中国地区联络热线：400 600 9103