THALES
Building a future we can all trust

GLOBAL EDITION

2023 CLOUD SECURITY STUDY

The Challenges of Data Security and Sovereignty in a Multicloud World

#2023CloudSecurityStudy

cpl.thalesgroup.com

Introduction

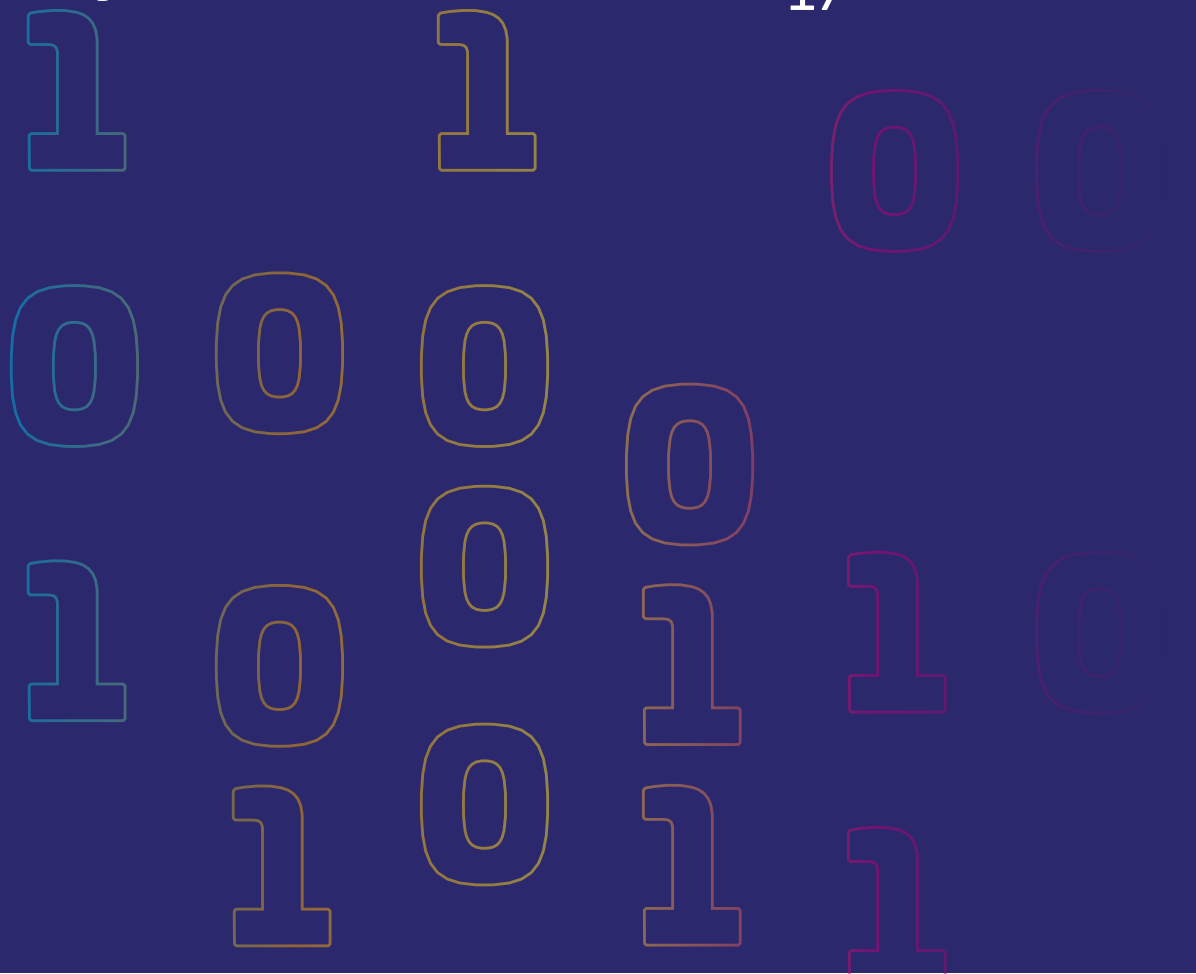
If there's a dominant theme that the data from the 2023 Thales Global Cloud Security Study conveys, it's that the world has become cloud-first, multicloud and that it's more complex to secure the cloud. The latest edition of the survey of nearly 3000 respondents in 18 countries explores challenges of security in cloud environments that have become a critical element in modern digital infrastructure and services. While there has been improvement in the overall cloud security posture from the previous year, there is still work to be done to simplify and secure cloud operations, especially when it comes to addressing human error. Multicloud operations bring with them operational complexity, something that needs to be tamed to secure cloud environments efficiently and effectively.

S&P Global
Market Intelligence

Source: 2023 Cloud Security custom survey from S&P Global Market Intelligence, commissioned by Thales.

Sponsored by

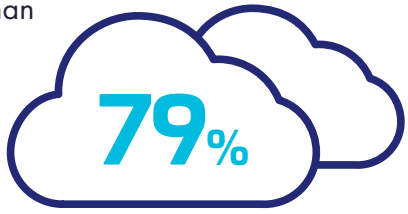
Contents



Key findings

Multicloud is a reality.

The average number of cloud infrastructure providers is well above two (2.3). More than three quarters (79%) of this year's respondents have more than one cloud provider.



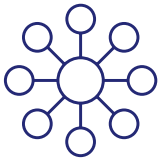
SaaS usage is growing.

97

The reported use of SaaS applications has expanded, with the mean rising to 97 applications, increasing the number of points of use where data must be secured.

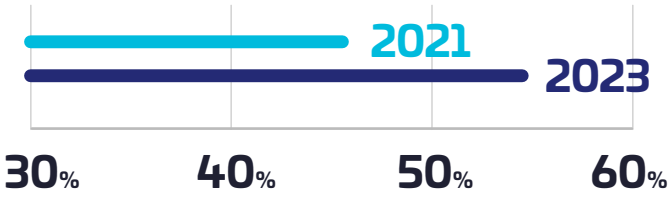
38%

SaaS applications garnered the most votes as the leading targets for attackers (ranked first as a target by 38%), followed closely by cloud-based storage (ranked first as a target by 36%).



Securing data in the cloud is seen as becoming more complex.

It has increased to 55% from 46% just two years ago.



Dramatic increase in sensitive data reported in the cloud.

75%

of respondents report that 40% or more of their data in the cloud is sensitive, up from 49% in 2021.

We're only human:

Human error is the leading cause of cloud data breaches

55% of respondents chose human error as the leading cause of cloud data breaches, well ahead of exploitation of vulnerabilities, the second highest selection at 21%.

Complex encryption key management creates security and operational risks.

Respondents report multiple key management systems in use.

62% say they have five or more key management systems in place.

ONLY 14% say that they control all of their own encryption keys in cloud environments.

Levels of sensitive data encryption must be higher.

ONLY 22% of respondents report that 60% or more of their cloud data is encrypted. On average, only 45% of sensitive data is encrypted.

Digital sovereignty issues around cloud usage loom large on multiple fronts.

Respondents report high use of cloud provider-dependent encryption key management, alongside growing concerns about sovereignty mandates.

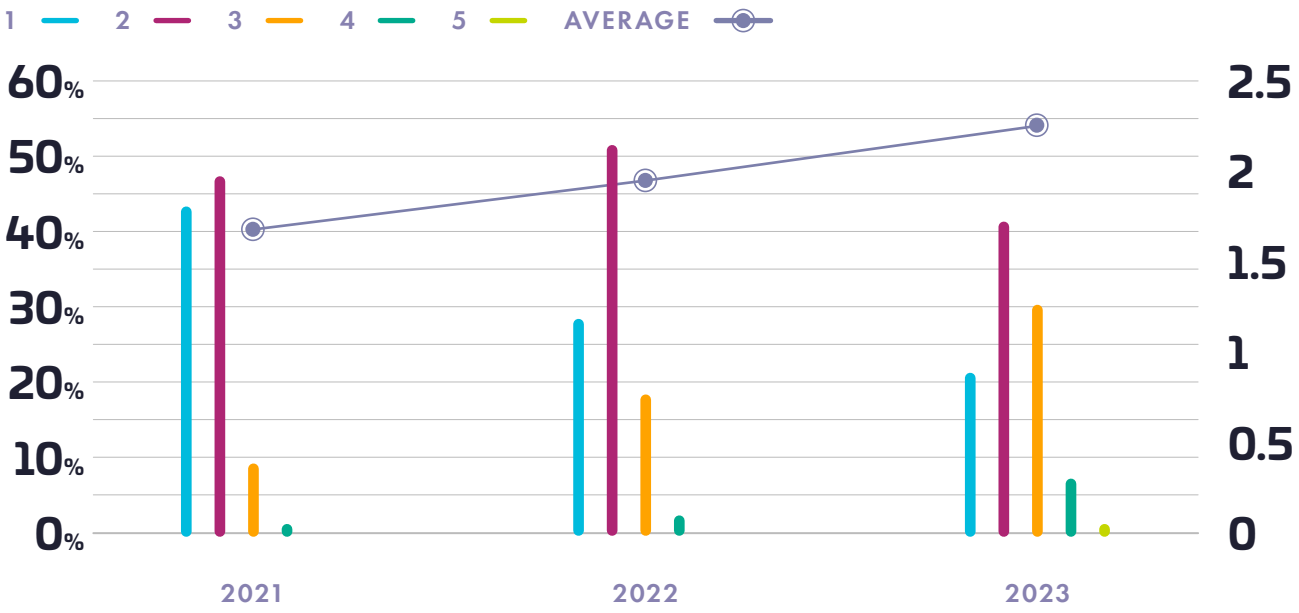
83% are concerned about impacts of sovereignty on cloud deployments.

It's a multicloud world

There are many reasons that could be pushing enterprises into expanding their portfolio of cloud providers. An interest in additional functionality, a move to diversify operations for greater resilience, partnerships, service availability and especially mergers and acquisitions are all possible causes that may be behind the increasing numbers, but the study results are clear – multicloud use continues to grow. Average number of cloud infrastructure providers (IaaS and PaaS) is up 35% over two years (from 1.68 to 2.26). With each additional cloud provider, there are new security controls and data protection models to understand and implement. Cloud users have to extend their existing operating processes further, while understanding the constraints of the new environment.

Multicloud is the rule, not the exception

Of the following cloud Infrastructure as a Service (IaaS) providers, which does your organization use or plan to use in a production capacity?



Source: S&P Global Market Intelligence's 2021-2023 Cloud Security custom surveys

35%

Growth in the number of cloud providers reported over the last two years

While cloud usage is growing for infrastructure, SaaS use is growing as well. More respondents are using SaaS applications to replace on-premises application functionality. In 2021, 16% of respondents reported their enterprises using 51-100 SaaS applications. That number increased to 22% for 2023 respondents. That translates into a shift in the mean number of applications reported in use from 69 in 2021 to 97 in 2023, a 41% increase, growing faster than regular cloud infrastructure.

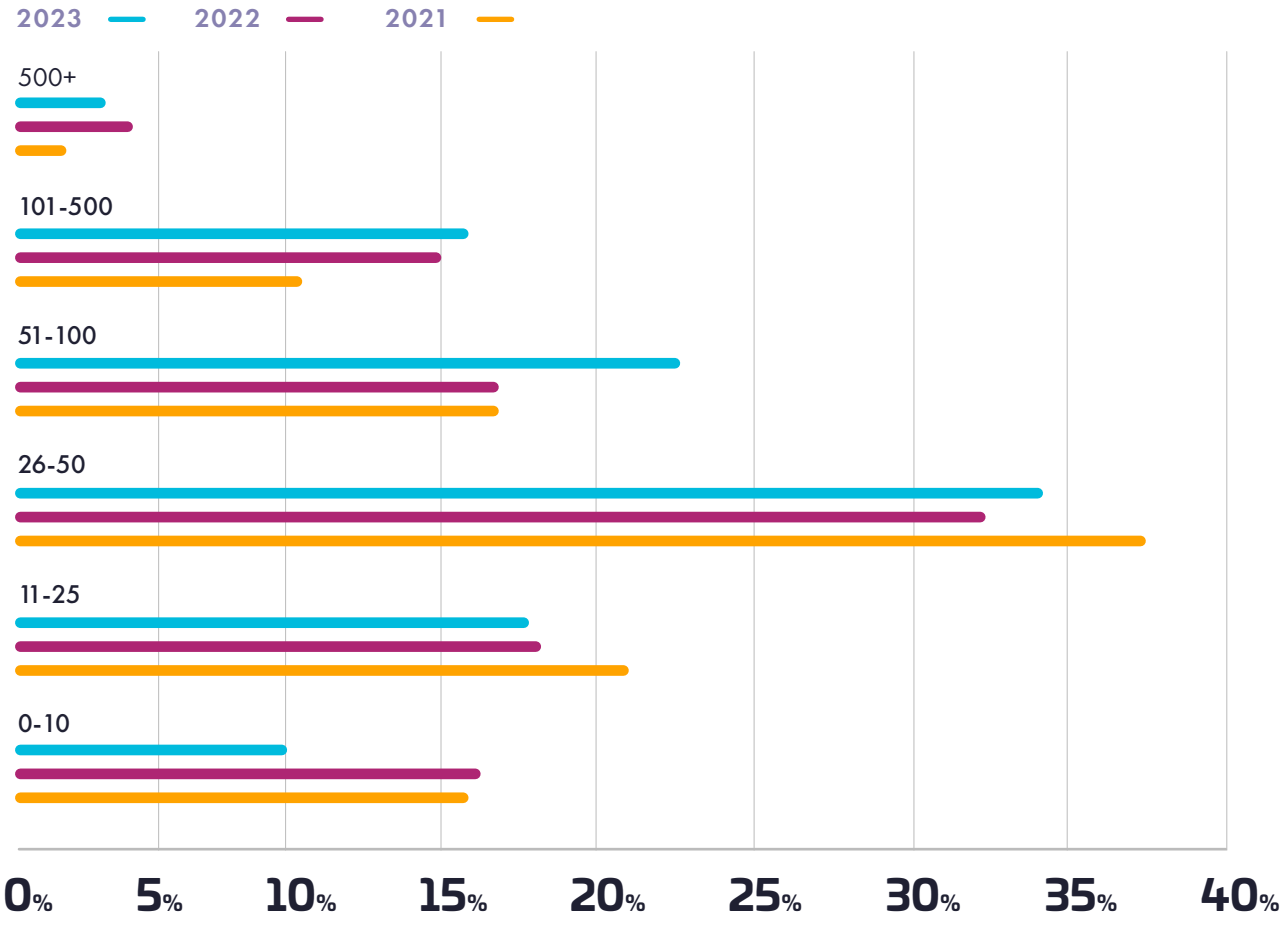
All of this expansion means that there is more to manage and secure, and that sensitive data is distributed to more locations. A majority of respondents (55%) note that they find it more complex to secure data in the cloud, and the increasing number of cloud providers could be driving that issue.

41%

Growth reported in the mean number of SaaS applications

SaaS diversity is trending higher

How many Software as a Service (SaaS) applications does your organization use?



Source: S&P Global Market Intelligence's 2021-2023 Cloud Security custom surveys

The threat landscape for the cloud

With the increasing use of cloud-based resources, it's important to understand perceptions of the threat landscape and the experiences that respondents have had in defending cloud resources. The study asked respondents to rank a set of attack targets by likelihood of attack. Garnering the most votes, more than a third (38%) of respondents say SaaS apps are the top target for cyberattacks, with 36% identifying cloud storage. It's an indication of the level of concern that exists for cloud-based resources. And it's not a concern that is unfounded.

Organizations identify the potential exposure of applications and data stored in the cloud as a risk. In fact, about half (46%) say they have experienced a data breach in their cloud environment. The number experiencing a data breach in the last year is up 4 percentage points (from 35% to 39%) from last year's report. As attackers target cloud-based resources, there's a greater need for organizations to improve their security posture. As the data indicates, that task is all the more difficult when there are more cloud providers to secure, which could be contributing to the reported increase in successful attacks.

38%

rank SaaS apps as the top target for cyberattacks

With a larger number of platforms to secure, the opportunity for operational errors grows, increasing the attack surface with each error. Organizations either have to dedicate separate teams to specialize in each platform or expect their security teams to become well-versed in multiple platforms at the same time. Respondents say that human error is the leading cause of cloud data breaches, which might be an indication that the strategy they're using for platform management is not working well enough.

As organizations are embracing cloud, the attacker community is increasing its presence and skill level in those same environments. That means that the threat landscape in the cloud will continue to become more hostile and require increasing effort to secure. This pressure, combined with increasing cloud environments, puts a greater emphasis on the ability of security teams to become more efficient in security operations.

39%

of respondents experienced a data breach in the last year

Cloud data concerns

The study results confirm that there are more workloads and data residing in the cloud, with those with 60% or more of their workloads and data in the cloud increasing from 23% to 27% in the last year. That mirrors larger industry trends as cloud becomes a more common path for new applications. There is a bigger story around sensitive data.

The study looked both at the amount of an organization's sensitive data that is stored in the cloud and the amount of data in the cloud that is sensitive. There is a notable increase in both areas. There has been a dramatic increase in the amount of an organization's sensitive data in the cloud. In 2022, 52% of respondents reported that more than 40% of their sensitive data was in the cloud. This year, this amount dramatically increased to 64%. That's most likely due to larger numbers of core applications running in the cloud, applications that are bringing the critical data that they handle with them.

The number of respondents saying that 40% or more of their data in the cloud is sensitive increased in a similar fashion – moving from 49% in 2021 up to 75% in 2023. That increase of more than 50%, combined with an increase in the number of cloud platforms, could be another factor leading to challenges in managing cloud data security. Point data protection controls alone cannot keep up with the volume and diversity of sensitive data growth.

75%

report that 40% or more of their data in the cloud is sensitive

Even though more data is in the cloud and more of that data is considered sensitive, there is still much that is not encrypted. More sensitive data is being encrypted, but levels are still low. Only 22% of respondents report that more than 60% of their sensitive data in the cloud is encrypted, with the average being 45% of data being encrypted. This is a marked improvement from previous years. In 2021, only 17% reported that more than 50% of sensitive data was encrypted. This year, that number is 40%. Only 2% report 100% encryption of sensitive data in the cloud this year.

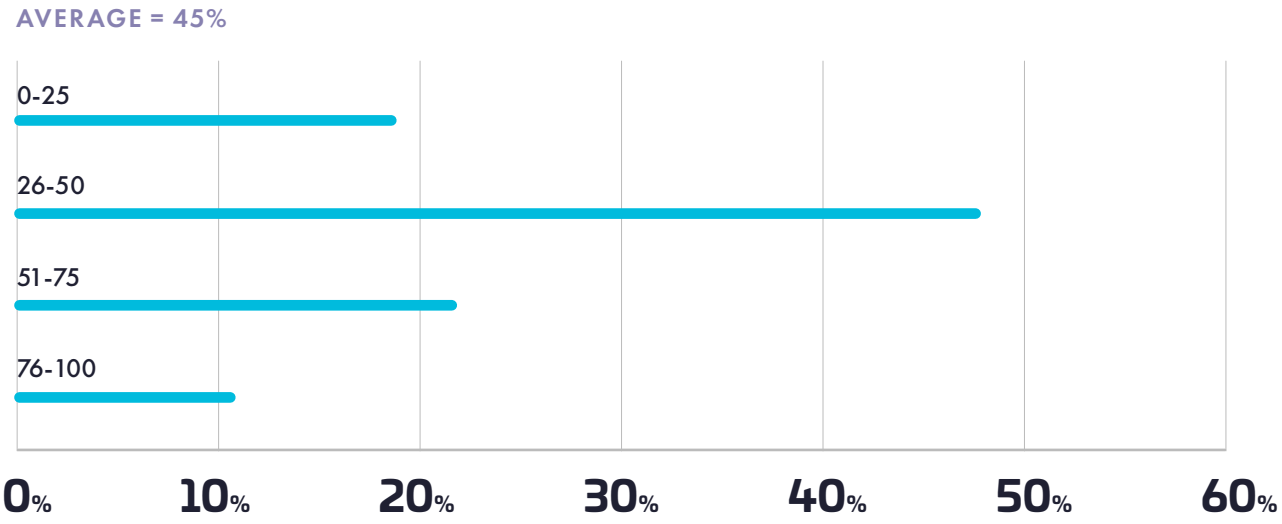
ONLY

2%

report 100% encryption of sensitive data in the cloud

Significant amounts of sensitive data are unencrypted

What percentage of your organization's sensitive data in the cloud is encrypted?



Source: S&P Global Market Intelligence's 2023 Cloud Security custom survey

There are clearly many factors at work that limit the use of encryption to these levels, but it raises serious questions about approaches to data security when such significant volumes of data identified as sensitive aren't encrypted. A lack of understanding of specific cloud encryption operations might be a contributor because cloud environments typically operate differently than traditional on-premises systems. Concerns about limiting developer productivity might weigh on some organizations. It could also be that organizations are carrying the traditional practice of relying on application-based data protection into clouds, where it is clearly not sufficient to address third-party risk. Whatever the cause, organizations need to do more, especially in light of regulatory requirements that are taking on a larger role in data protection.

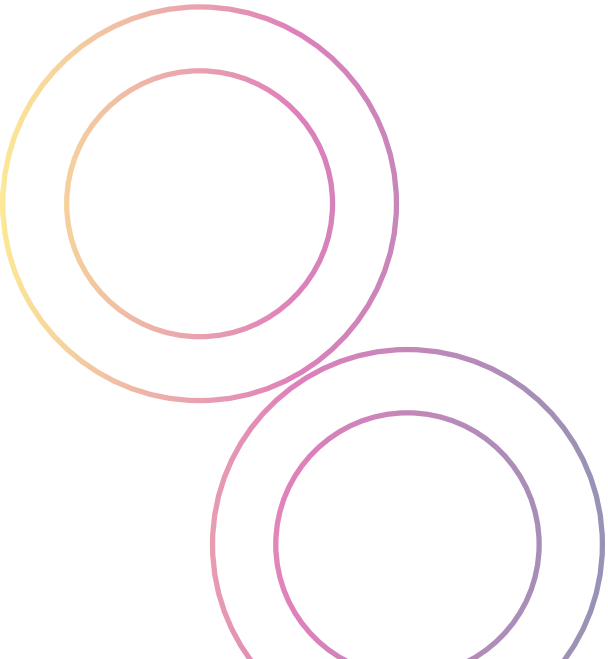
22%

report that more than 60% of their sensitive data in the cloud is encrypted

Impacts of data sovereignty

Digital sovereignty is a global strategic initiative, and privacy compliance represents opportunities for enterprises to mature their data management capabilities. It's a critical functionality because concerns about digital sovereignty can hinder digital transformation if organizations can't effectively manage the data that fuels their businesses. It can present challenges with requirements to control and manage where data is stored and used and who has access to it. When asked about digital sovereignty, 83% of respondents worldwide say they are "somewhat" or "very" concerned about impacts on cloud deployments.

The foundation of digital sovereignty is not the cloud provider but the data management capability of the infrastructure that supports the workloads and applications under the data custodian's control. The use of cloud-based resources introduces a third party that legacy data management strategies may not have addressed. Those leveraging cloud need to ensure not only that the data being secured is protected from disclosure but also that it is delivered only to those environments where it should be used. Multicloud environments can help address digital sovereignty requirements as organizations leverage different cloud environments for regional coverage. However, that potential benefit could add complexity if organizations aren't able to simplify the way they manage the various clouds that make up their infrastructure.

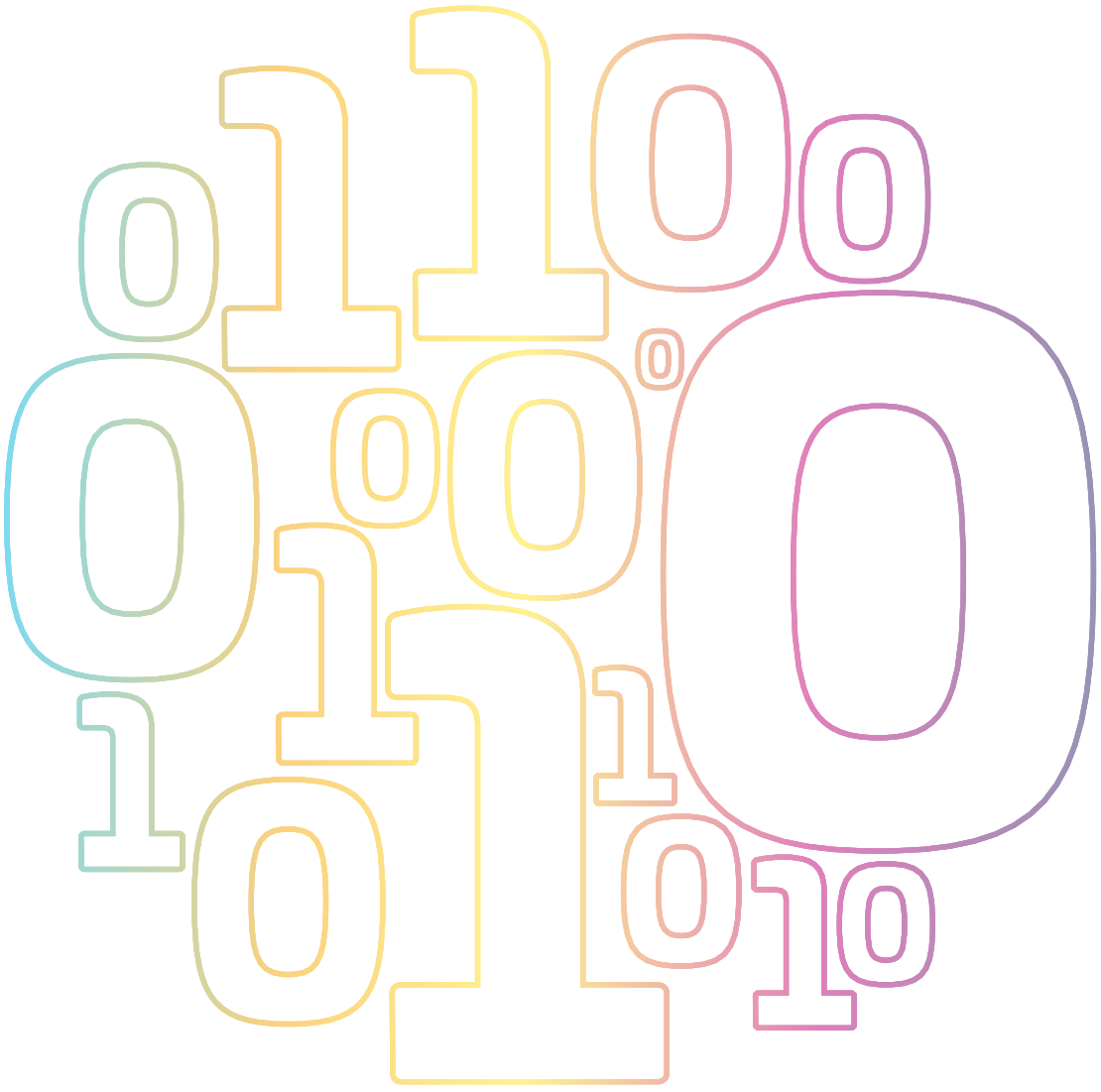


83%

say they're concerned about digital sovereignty impacts on cloud deployments

Regarding expectations for meeting digital sovereignty requirements, 96% of respondents believe that designating or changing the location and jurisdiction or the use of full data encryption are acceptable measures to achieve various levels of digital sovereignty. Only the remaining 4% are not concerned about the location of data with respect to sovereignty mandates. More than a third (35%) believe that location is important for all workloads. This reflects both the concern about regulations that use the physical location of data as a means of protection and the growing interest in cryptographic protections as a sufficient means of protection. With the latter, data encryption provides the isolation required and ensures that no matter where the data is located, it is protected from disclosure to unauthorized parties. It's an approach that has many advantages and is under active exploration by a number of regulatory bodies.

Organizations need to understand that the core elements of digital sovereignty will become a requirement for all. While it may seem that those operating within a single region could remain exempt, providing highly available digital customer experiences will eventually require the same level of data protection. By building in better data protection capabilities today, they'll be prepared for whatever requirements regulators, either local or global, put forward in the future.



Operational complexity in the cloud

The operational realities of multicloud environments have raised concerns for many organizations. More than half (55%) of study respondents indicate that it is more complex to manage data in the cloud than it is in on-premises environments. While most have been honing their operational capabilities in the cloud, it's still seen as an operational concern. Growing numbers of cloud providers could certainly be adding to this complexity.

The study looked at operational aspects of data protection and management in the cloud, and the results offer some insights into what may be driving the complexity. Only 14% of respondents say that they control all of their encryption keys in their cloud environments. This means that most organizations are working with multiple cloud environments, and they manage their data encryption keys in different ways across those environments.

55%

say that it's more complex to manage data in the cloud

A further confirmation of the complexity in data protection management comes from a question on the number of key management systems in use. Almost two-thirds (62%) say they have five or more key management systems in place across their operational infrastructure. That means that there are independent realms in which data protection must be managed. More than a quarter of respondents (27%) say their cloud provider controls all of their keys. As with other aspects of multicloud security management, organizations will either have to have dedicated teams for each cloud or expect their teams to be skilled in key management operations for all of their providers at the same time. With this situation, it's not surprising that respondents report human error as the leading cause of cloud data breaches (55%), well ahead of the second cause, exploitation of vulnerabilities (21%). Complex operational environments are all too susceptible to human failings. This is another area where organizations have to simplify their security management to become more effective.

ONLY

14%

of respondents say that they control all of their encryption keys in their cloud environments

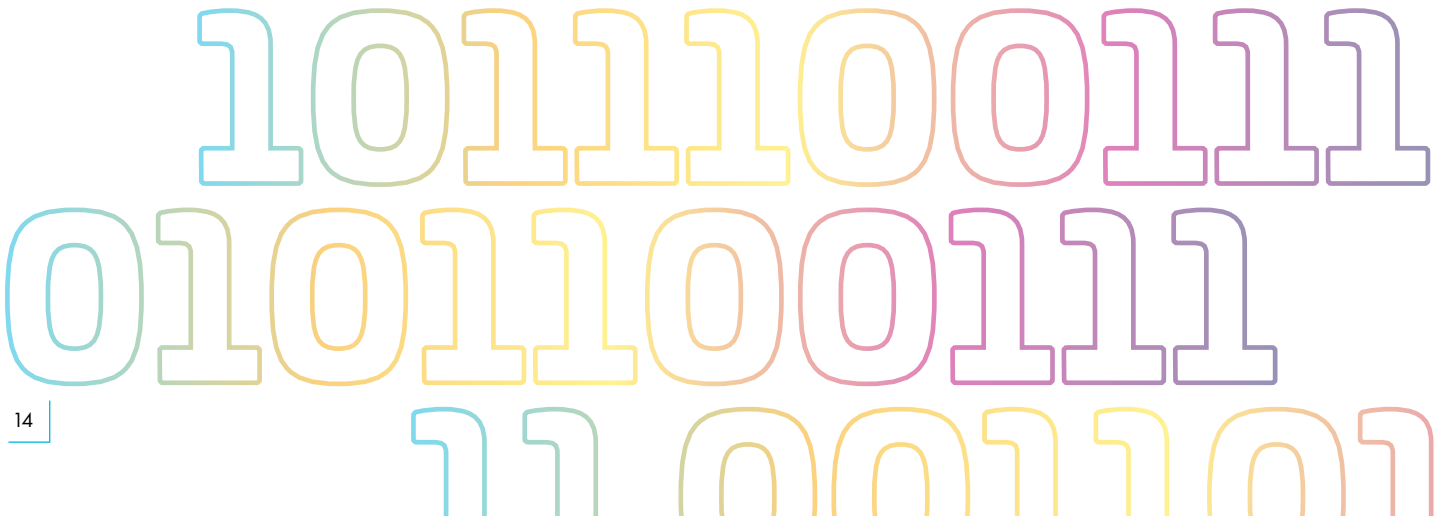
Pathways to better cloud security

The study results clearly illustrate the challenges faced by organizations as they work to secure their cloud-based infrastructure, but they also offer some indications of pathways to improving cloud security. Identity and access management has been identified as a top mitigating control for data breaches, and there has been progress from previous study results. Strong MFA adoption increased to 65%, but that's still not good enough. With a third of respondents yet to implement this important control, there is significant cloud infrastructure at risk

Another key point taken from the study results is that data security has to be improved. Centralizing encryption management is mandatory. In a multicloud world, organizations have to be able to centrally manage keys that are used across their infrastructure — on premises as well as in the cloud. That management skill not only reduces operational complexity but can also give organizations the flexibility to secure new environments as business needs dictate, whether that's to take on a new partnership or merge businesses.

65%

report deploying MFA to secure cloud data access

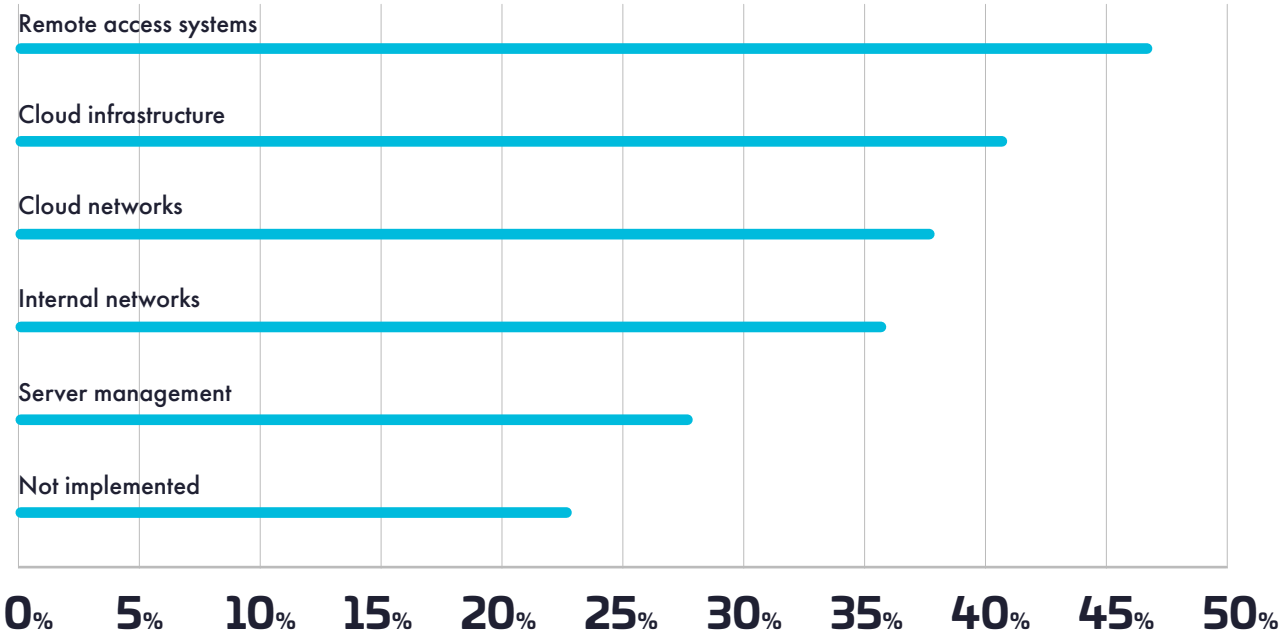


It's also an improvement that can address the leading cause of cloud data breaches: human error. Making security operations more efficient can make them more effective. Building security management systems that can leverage automation and span the full range of an organization's infrastructure is a critical goal.

Improving operational architectures is another area to improve security posture. Getting to a zero-trust footing in the cloud can build a better foundation for operational security. Only 41% have zero-trust controls on cloud infrastructure, and even fewer (38%) use zero-trust controls in cloud networks.

Zero trust use is improving, but more needed

How does your organization use zero trust practices?



Source: S&P Global Market Intelligence's 2023 Cloud Security custom survey

Moving ahead

The study results point to a set of challenges that organizations are facing in securing data in the cloud environments. They're living in a multicloud world and need to be able to secure it effectively and efficiently. They need to overcome the complexity that working across cloud infrastructure and SaaS environments presents. Data protection in the cloud must become simpler to manage to overcome issues with human error and misconfiguration. The results of the study indicate specific areas that need improvement.

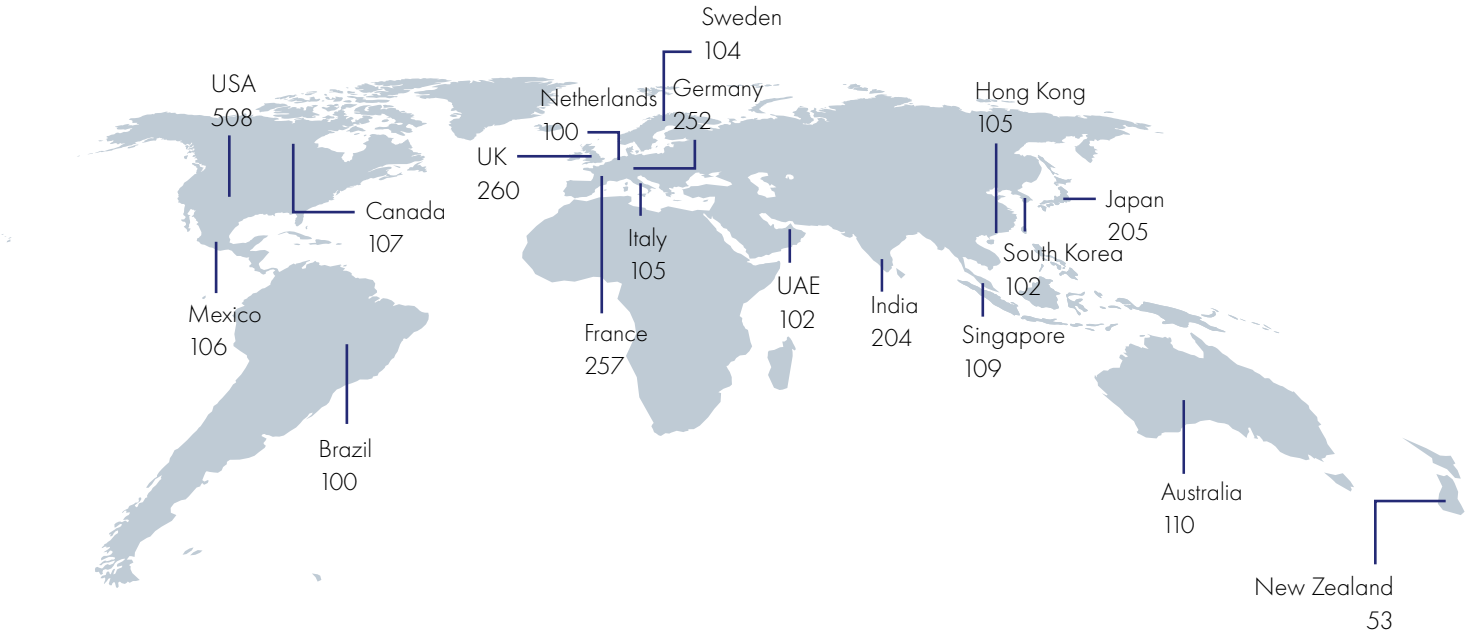
- **Key management consolidation.**
- **Greater use of data encryption.**
- **Gaining control of encryption keys.**
- **Achieving great efficiency through security automation.**

Key management environments need to be consolidated. Doing so can deliver the operational control that's needed to scale up the use of encryption in ways existing security teams can handle. At the same time, organizations need to take advantage of the force-multiplying power of automation. It is underutilized in security, more so than in other technological disciplines, and is another tool to reduce the risk of human error alongside the efficiency gains it provides. These improvements can also bolster digital sovereignty compliance efforts with the necessary controls to ensure data is where it needs to be and is well protected.

The most effective way to improve cloud data security is to ensure that cloud environments can be treated as an extension of existing infrastructure, not a special case. That's a mandate for technologies that can span the multiple environments that organizations find themselves in with a common security management environment. It's a pathway to making all of an organization's data protections more effective and efficient.

About this study

This research was based on a global survey of 2,889 respondents that was fielded in November and December 2022 via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about the level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated an 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

$100m to $249.9m	**91**
$250m to $499.9m	**749**
$500m to $749.9m	**796**
$750m to $999.9m	**748**
$1Bn to $1.49Bn	**229**
$1.5Bn to $1.99Bn	**134**
$2Bn or more	**142**

Industry Sector

Retail	**158**
Manufacturing	**148**
Financial services	**140**
Healthcare	**139**
Federal government	**125**
Public sector	**122**
Technology	**117**
Automotive	**114**
Pharmaceuticals	**108**
Telecommunications	**101**

THALES

Building a future we can all trust

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/cloud-security-research