GLOBAL EDITION

THALES
Building a future we can all trust

2021 Thales Cloud Security Study

The Challenges of Cloud Data Protection and Access Management in a Hybrid and Multicloud World

#2021CloudSecurity

cpl.thalesgroup.com

Contents

About this study

The COVID-19 pandemic has accelerated what has been a long-term broad adoption of cloud environments, including multicloud and hybrid deployments. The benefits of cloud come with significant new security challenges for organizations. The 2021 Thales Cloud Security Study, based on data from a global survey of more than 2,600 IT and security professionals, delves into cloud security trends so that readers can align the research findings to their own practices as they consider their cloud migration and implementation efforts.

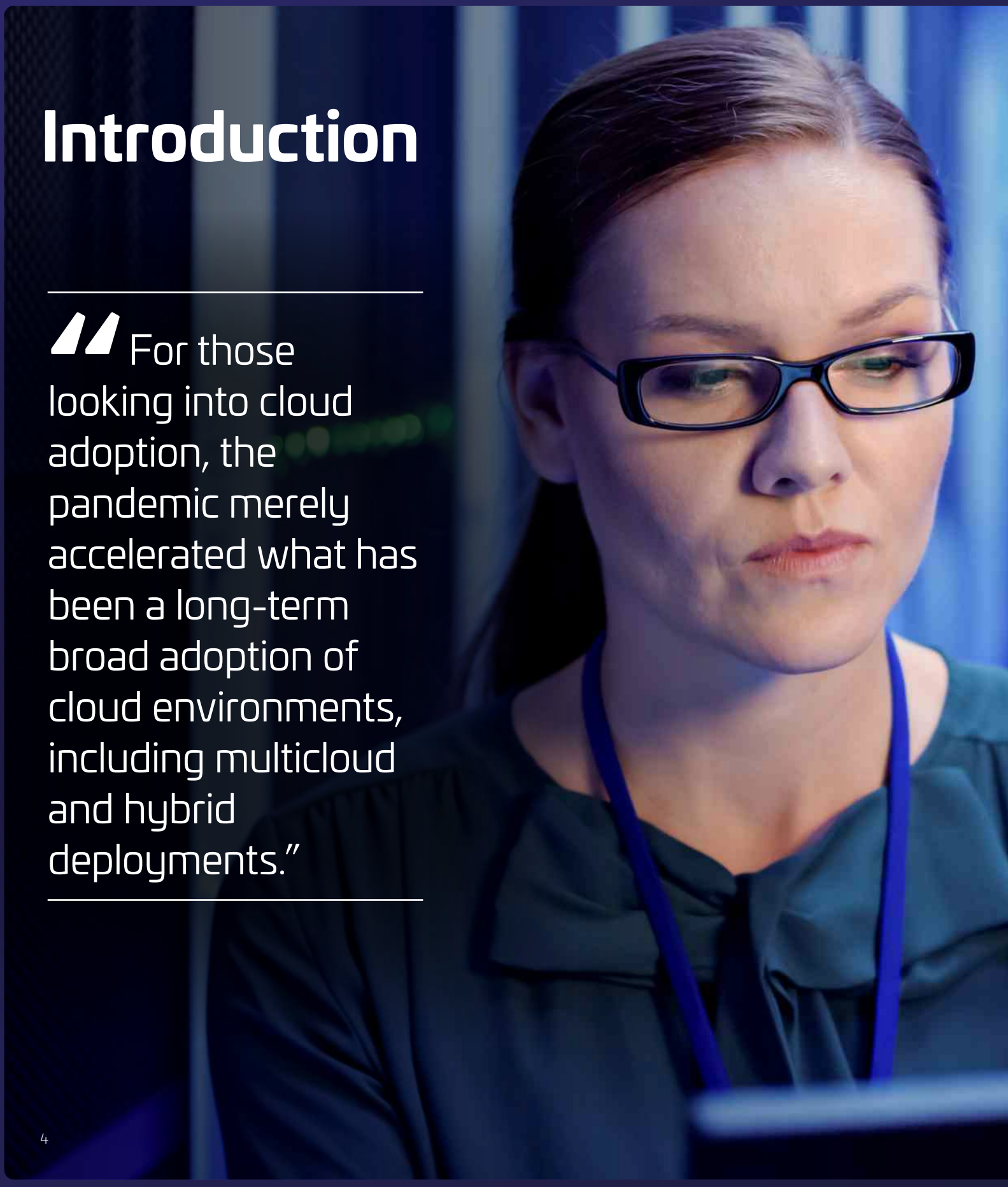
451 Research

S&P Global
Market Intelligence

Source: 2021 Cloud Security custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Our sponsors are:

Introduction



"For those looking into cloud adoption, the pandemic merely accelerated what has been a long-term broad adoption of cloud environments, including multicloud and hybrid deployments."

As the world continues to grapple with the COVID-19 pandemic, it's clear that the technology sector in general – and cloud adoption in particular – has been instrumental in helping the world cope with the enormity of the task. It has provided the advanced medical research at various stages; helped instrument public health, officials, and the general public, and provided the foundation of ongoing commerce, communication and entertainment.

For those looking into cloud adoption, the pandemic merely accelerated what has been a long-term broad adoption of cloud environments, including multicloud and hybrid deployments. There are numerous benefits to this adoption: faster time to value and time to market, as well as the ability to experiment and quickly leverage elasticity and resiliency. That said, the benefits of cloud come with significant new security challenges for organizations. They need to understand how responsibilities are shared between provider and customer, how the threat models change, how internal stakeholders respond to cloud, and much more.

Throughout all this, it's useful to get a sense of how others are handling these issues. Just how widespread is multicloud? What are the operational challenges of managing security across multiple clouds? Is all this cloud transformation as hard as it seems? How do I secure data in cloud? This report delves into these and other trends in cloud security. The report presents findings that come from a global survey of more than 2,600 respondents, spread across industries, organization sizes and job functions. Please refer to the Methodology section for more detail.

The intent is for readers of this report to benefit from aligning the research findings to their own practices as they consider their cloud migration and implementation efforts.

Key Findings

This report covers topics such as multicloud, cloud complexity and security technologies for cloud, specifically authentication, data encryption and key management. It includes numerous findings broken down across regions, organization size, vertical market, job title, etc. Some of the highlights are:

Multicloud adoption is widespread. On a global basis, 57% of respondents indicated that they use two or more from a select group of six large cloud providers for infrastructure as a service/platform as a service (IaaS/PaaS). Regionally, respondents in the Middle East and North America were slightly below this average. As expected, the proportion of multicloud usage grows with organization size and complexity: Nearly 70% of those in organizations with more than US$2bn in revenue indicated multicloud usage. Those in healthcare represented the largest proportion of multicloud usage, while transportation and media/entertainment the lowest. Finally, senior managers and staff have different perspectives on multicloud use – a higher proportion of senior manager respondents indicated they use multicloud than others.

82%

of respondents indicated that security teams are responsible for defining cloud security policies

> **"While 57% of respondents overall have adopted multicloud, the data shows differences in terms of geography."**

Software as a service (SaaS) usage is even more pervasive. The survey showed that the use of SaaS applications is widespread across all geographies, verticals and company sizes, with a calculated weighted global average of about 60 applications. Some of the regional nuances indicate that Latin America and the Middle East are below this average. Not surprisingly, respondents from larger organizations indicated they use, in aggregate, a larger number of applications than smaller organizations. Looking at data from specific sectors, respondents from telecommunications, manufacturing and financial services use a larger number of SaaS applications.

Security teams have a key role in defining security policies for clouds. While there are nuances on how cloud security controls ultimately get implemented, 82% of respondents indicated that security teams are responsible for defining cloud security policies. There is broad consensus on the topic across geographies, company size and verticals. Notably, there is an apparent distinction within organizations: Those in senior leadership positions – identified either via title or via their role in the purchasing process – lean toward concentrating more responsibilities on security teams, while staff indicated there is a bigger role to be played by cloud engineering teams.

> "The survey showed that the use of SaaS applications is widespread across all geographies, verticals and company sizes, with a calculated weighted global average of about 60 applications."

Cloud complexity is a common concern. Nearly half (46%) of global respondents (the majority of those with an opinion on this topic) agreed or strongly agreed with a statement indicating that 'within their organizations, it is more complex to manage privacy and data protection regulations in a cloud environment than on-premises.' The proportion of 'Agree' responses from those in smaller organizations and in large (but not the largest) organizations was noticeably higher, likely reflecting internal organizational pressures. Respondents from the manufacturing and telecommunications sectors also indicated a higher level of agreement with the statement. Those working in multicloud environments indicated a higher level of agreement (50% versus 46% globally) as well.

Many choose 'lift & shift' for their cloud migrations. While not all organizations move to cloud – many adopt hybrid models, for example – those that are migrating some of their workloads indicated – at 55% globally – some preference for lift & shift versus re-architecting applications. Regionally, both Latin America and the Middle East indicated a higher response rate of lift & shift over re-architecting. There's a noticeable gap in perception between respondents given their organizational roles: those associated with more approval over processes indicated there's a bigger proportion of re-architecture over lift & shift. On a sector basis, respondents in the 'tech' sector also indicated a higher proportion of lift & shift (64%). Finally, respondents not pursuing multicloud also indicated a slightly higher proportion of lift & shift (at 58%).

A few common technologies emerge when considering how to secure cloud deployments. When asked to rank which technologies they consider key for securing cloud environments, the top choices ranked first, second or third by respondents were cloud security tools (cloud security posture management, cloud workload protection, cloud identity and access management); data loss prevention; encryption; and multi-factor authentication (MFA) at 38%, 38%, 37% and 33%, respectively. Smaller organizations favored the use of cloud security tools and encryption. Those in sectors such as financial services, media and transportation highlighted encryption as the most popular option, while MFA was listed first by technology respondents.

> **"Only 17% of respondents indicated that they encrypt more than 50% of sensitive data that they host on cloud environments."**

Encryption in the cloud is not widespread. According to survey results, only 17% of respondents indicated that they encrypt more than 50% of sensitive data that they host on cloud environments. In other words, it is uncommon for companies to encrypt most of their sensitive cloud data. Sectors such as financial services, transportation, and media and entertainment are only marginally better at 21% saying they encrypt more than half of their sensitive data. There may be a correlation between encryption and the effort of maintaining a multicloud presence. According to global survey results, the proportion of respondents who have adopted multicloud and encrypt more than 50% of their sensitive data in cloud drops to 15%. Finally, the use of encryption is also split between those using their own encryption capabilities (at 35%) and those using encryption offered by the cloud provider (at 55%).

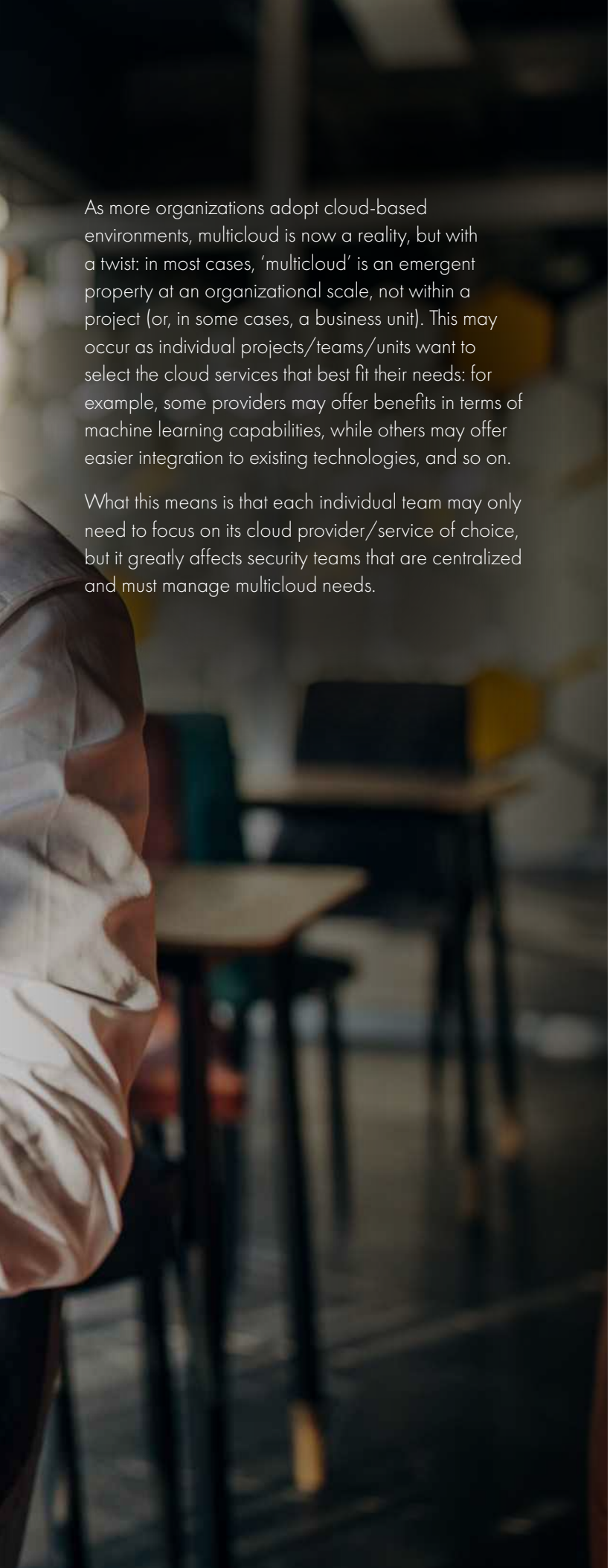
While some organizations retain control, many leave key ownership to providers. The survey indicates that, at a global level, only about 34% of respondents use their own encryption keys, with an additional 6% maintaining control over key-generation material, with others leaving that to the cloud providers. Some nuances on use of provider-owner keys include more respondents from the Middle East and from healthcare reporting higher use of provider keys, with Latin American and manufacturing respondents indicating higher usage of their own encryption keys.

Reports of breaches and audit issues in cloud environments are common, but unevenly distributed. Globally, 40% of respondents indicated that their organization has had to deal with a breach in their cloud environments. From a geographical perspective, Latin America and Asia-Pacific indicated lower rates of breach, and industries such as healthcare, consumer staples and telecommunications reported lower rates of breaches. Interestingly, those that indicated they've adopted multicloud reported a lower incidence of breaches as well. Similarly, at a global level, 43% indicated they had either experienced a breach or an audit issue on their cloud environments in the past 12 months. The dynamics of breach/audit issues are similar to breaches.

Multicloud Adoption – IaaS and PaaS

For this research, we asked respondents to select from a list of six representative cloud providers: Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Cloud, Oracle Cloud and Alibaba Cloud. Those who indicated they used more than one of these providers were classified as 'multicloud.'

The global numbers (see Figure 1) are not identical but are similar to additional data from 451 Research, which showed that 70% of respondents use two or more cloud providers.



As more organizations adopt cloud-based environments, multicloud is now a reality, but with a twist: in most cases, 'multicloud' is an emergent property at an organizational scale, not within a project (or, in some cases, a business unit). This may occur as individual projects/teams/units want to select the cloud services that best fit their needs: for example, some providers may offer benefits in terms of machine learning capabilities, while others may offer easier integration to existing technologies, and so on.

What this means is that each individual team may only need to focus on its cloud provider/service of choice, but it greatly affects security teams that are centralized and must manage multicloud needs.

FIGURE 1

Multicloud Adoption

Number of IaaS Providers

Source: 451 Research's 2021 Cloud Security custom survey

Regional Nuances Arise

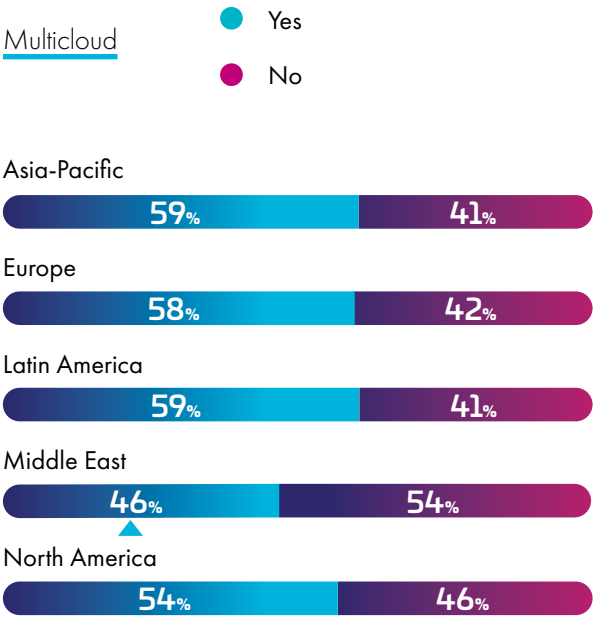
While 57% of respondents overall have adopted multicloud, the data shows differences in terms of geography. For example, respondents from the Middle East were noticeably behind the global average in terms of multicloud support (see Figure 2). This is understandable, given that public cloud providers currently have limited footprint in the region, although many indicated plans for growth. Until full provider regions are made available in the Middle East, many cloud providers are recommending the use of hybrid architectures using on-premises equipment attached to cloud management planes.

North American respondents also trail the global average slightly. While this research doesn't delve into specifics or causation, it is possible that because North American cloud presence usually supports a greater number of services, customers may have fewer reasons to consider multicloud approaches.

> **"While 57% of respondents overall have adopted multicloud, the data shows differences in terms of geography."**

FIGURE 2

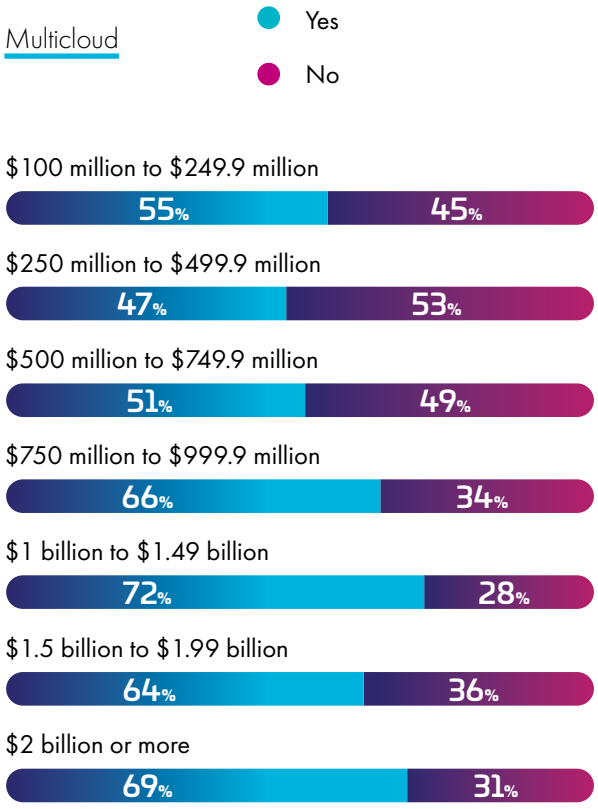
Multicloud Adoption by Geography



Source: 451 Research's 2021 Cloud Security custom survey

FIGURE 3

Multicloud Adoption by Company Size (Revenue)



Source: 451 Research's 2021 Cloud Security custom survey

Organization Size Matters for Multicloud

The research shows that there is an approximate correlation between organization size (as measured in revenue) and adoption of multicloud. While we can attribute the use of multicloud in larger organizations, as above, to it being an emergent property, the relative higher use in very small organizations might be attributed to lack of existing governance.

Internal Organizational Aspects Show Disconnect

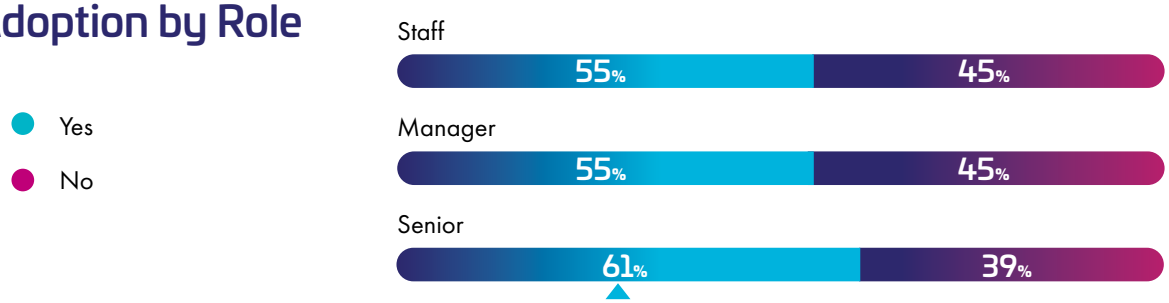
Throughout our research and, in many cases, across multiple aspects of cybersecurity, we often observe a divergence in responses between respondents in senior leadership roles and those in more operational or staff roles. This is important because the lack of alignment between these stakeholders can lead to deficiencies in security planning, management and operations.

In this study, those in senior leadership positions indicated that their organizations have adopted multicloud at a higher proportion than those in staff or management positions (See Figure 4). This lack of agreement on key technology aspects of the organization's cloud footprint can potentially cause friction in operating and evolving this footprint.

> **"In this study, those in senior leadership positions indicated that their organizations have adopted multicloud at a higher proportion than those in staff or management positions ."**

FIGURE 4

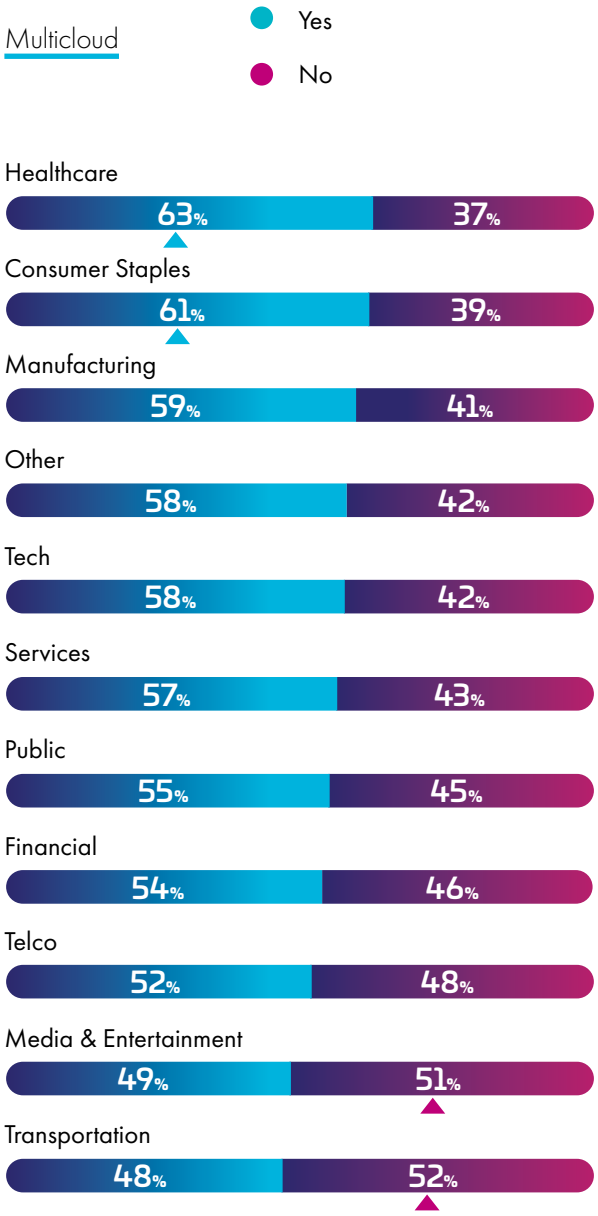
Multicloud Adoption by Role



Source: 451 Research's 2021 Cloud Security custom survey

FIGURE 5

Multicloud Adoption by Industry Sector



Source: 451 Research's 2021 Cloud Security custom survey

Sector Differences in Multicloud

Breaking down responses to multicloud usage across sectors indicates significant differences, likely tied to the broad set of use cases associated with each sector. Healthcare and consumer staples responded notably above the 57% global average (at 63% and 61%, respectively), while transportation and media & entertainment were well below that average, at 48% and 49%, respectively.

This result teases out that in some industries, organizations may be more tied to the broader set of services from one cloud provider because of the specific requirements of their use cases. Indeed, when considering the set of services offered by providers, many include specialized services aimed at media management (transcoding, transmissions, content distribution), as well as services aimed at supporting IoT use cases that include 'edge' elements.

PaaS Adoption, in Contrast, Is a Lot More Stable

Compared to the variance in use of multicloud, respondents are remarkably more consistent in their use of PaaS platforms. Across the many demographic characteristics of this research, the number of PaaS offerings was about two.

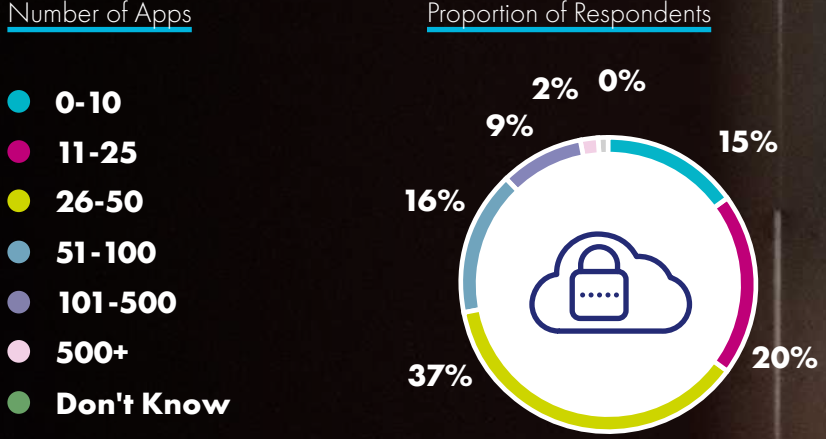
Software as a Service Usage

While it's easy to focus discussions of cloud security on the nuances of IaaS and PaaS, the reality is that the use of SaaS applications is widespread across all industries, and those tasked with securing organizational resources in cloud should have SaaS applications in their scope, even if handled by different technologies than IaaS and PaaS use cases.

To analyze SaaS results in this research, we asked respondents about the approximate number of SaaS applications in use at their organizations, which we then converted to an estimated weighted average number using the midpoint of each range. For those indicating they use 100-500 SaaS apps, the midrange was arbitrarily set at 200 to account for inaccuracies (such as respondents overestimating the number of applications). For those with more than 500 SaaS applications, the midpoint was arbitrarily set at 600 for similar reasons.

FIGURE 6

SaaS Usage



Source: 451 Research's 2021 Cloud Security custom survey

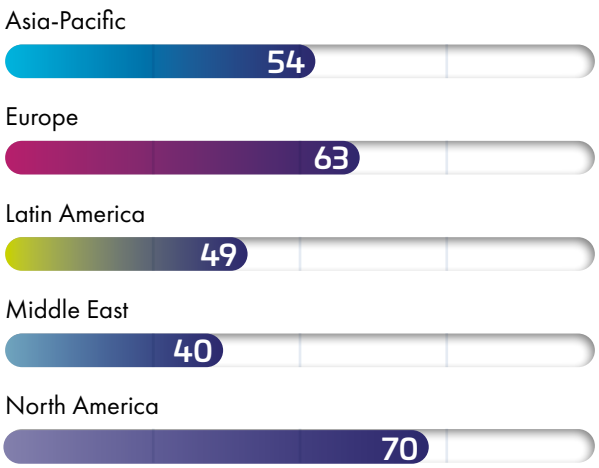
Regional Averages Differ Significantly

As Figure 7 shows, the regional numbers vary significantly, with North American having the highest average at 70 applications and the Middle East the lowest at 40, followed by Latin America with 49. This range is likely explained by the relative maturity and penetration of cloud-native SaaS offerings in each region, coupled with local factors such as telecommunications costs and local taxation of services.

FIGURE 7

SaaS Usage by Geography

Average Number of Applications



Source: 451 Research's 2021 Cloud Security custom survey

Number of SaaS Applications Grow with Organization Size

When looking at global usage of SaaS applications by size of organization, the numbers follow a predictable pattern: Larger organizations use more SaaS applications. This is expected, because one of the key characteristics of SaaS applications is that they can be deeply aligned to specific use cases and easy consumption, which means the inherent complexity of larger organizations can yield a large number of possible use cases for SaaS applications.

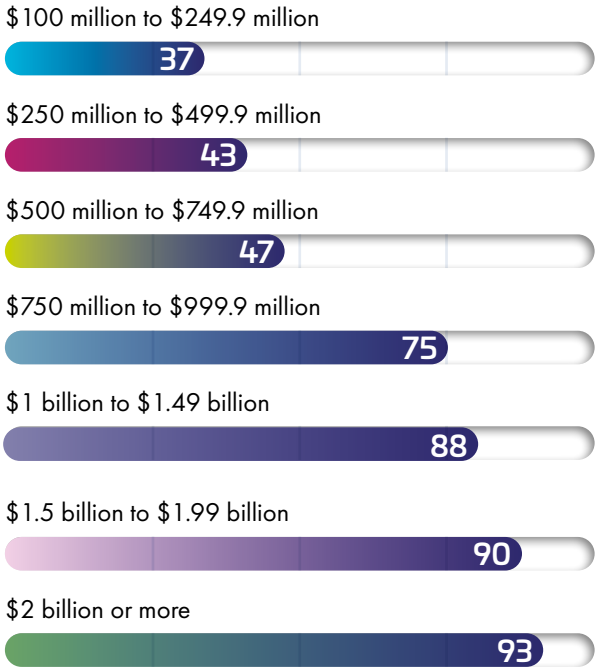
From a security perspective, it is important to note that this multitude of use cases – and use of a greater number of SaaS applications – translates to a complex usage pattern: the potential for sensitive corporate data to be present and used at multiple locations outside direct organizational control.

"When looking at global usage of SaaS applications by size of organization, the numbers follow a predictable pattern: larger organizations use more SaaS applications."

FIGURE 8

SaaS Usage by Company Size

Average Number of Applications

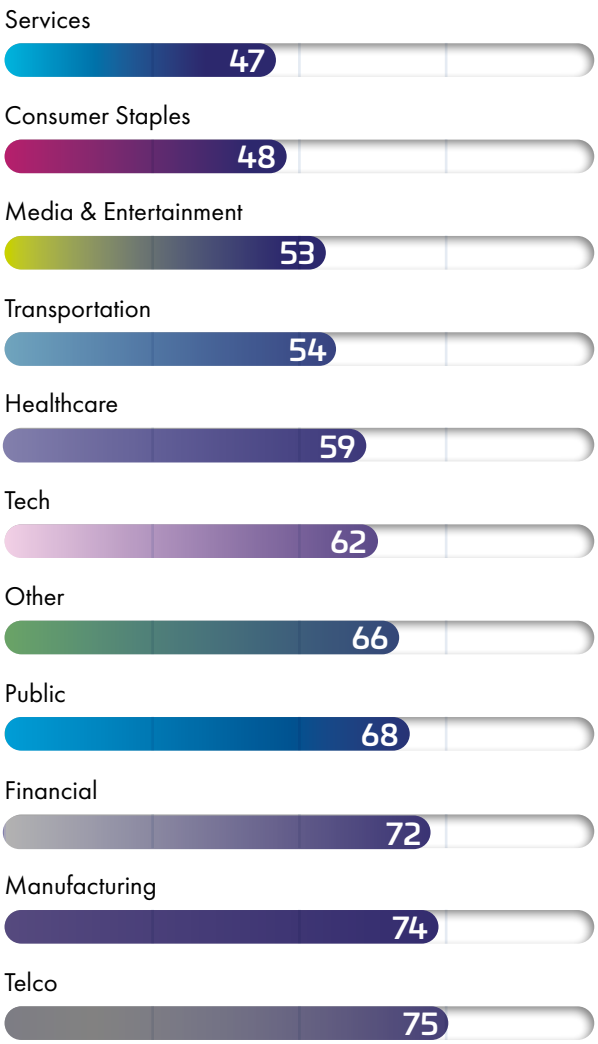


Source: 451 Research's 2021 Cloud Security custom survey

FIGURE 9

SaaS Usage by Industry Sector

Average Number of Applications



Source: 451 Research's 2021 Cloud Security custom survey

Sector Variance in SaaS Applications

The global results for SaaS applications, broken down by industry sector, indicate that telecommunications, manufacturing and financial organizations have the highest average number of SaaS applications, while services and consumer staples have the lowest. For those industries with a large number of SaaS applications, these results likely stem from the inherent complexity of more specific use cases in these domains, possibly coupled with an inherent effect from these companies potentially being larger, in which the case the size effect as mentioned above would be a confounding factor.

Managing Cloud Security

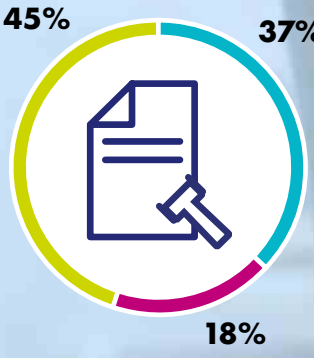
One of the most differentiating aspects of cloud adoption is that the cloud model is not merely a technology refresh; it is forcing organizations of all sizes to take a deeper look at their internal organizational structure. Compared to previous technology cycles, cloud adoption brings about a broader set of internal stakeholders and demands, from faster time to value to accelerated project schedules. In the case of IaaS and PaaS services, cloud engineering departments, groups or centers of excellence have arisen. For SaaS, business units ask for specific offerings. How is security being managed in these scenarios?

This research focused on this question by asking how organizations are structuring two key elements of cloud governance: policy definition and policy enforcement.

At a global level, there's a broad acceptance that yes, security teams are tightly involved with policy definition (at 82%), but an almost even split (37% to 45%) in relation to enforcement.

FIGURE 10

Responsibility for Policy Definition and Enforcement



- Policies and standards are defined centrally by the security team and enforced by the security team using tooling of their choice.
- Policies and standards are designed by the individual cloud delivery teams and enforced by the cloud delivery teams.
- Policies are defined centrally by the security team, but defining technical standards and enforcing them is up to individual cloud delivery teams.

Source: 451 Research's 2021 Cloud Security custom survey

Different Views Between Management and Staff

As mentioned elsewhere in this research, there's sometimes a discrepancy between management and staff in how they envision a particular issue. As Figure 11 shows, those in senior management have a higher perception that security teams are responsible for both policy definition and enforcement, compared to staff. (39% to 32%). Conversely, staff respondents primarily indicated that security teams are responsible for policy definition, but enforcement is up to others (50% to 41%). This has the potential to create confusion and a lack of coordination between teams both during incidents and during strategic planning for security activities.

Figure 12 illustrates this dynamic from a slightly different perspective. Here, management/staff alignment is associated with role in the decision-making process.

FIGURE 11

Perception of Who is Responsible for Policy Definition and Enforcement by Role

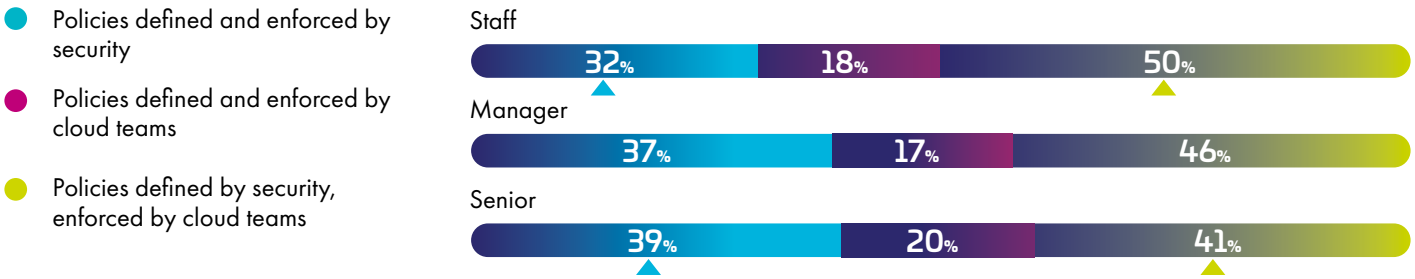
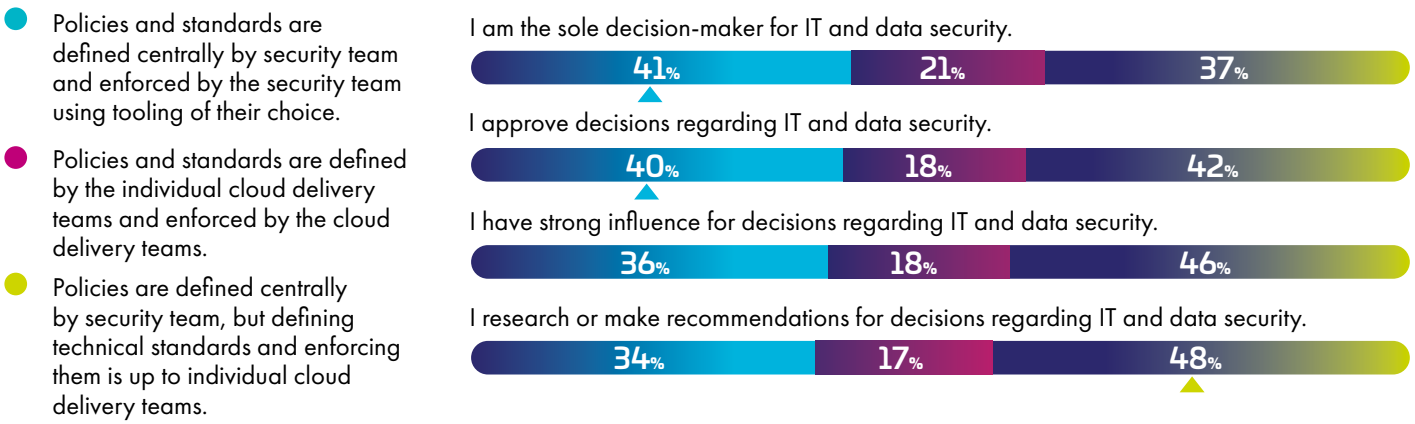


FIGURE 12

Perception of Who is Responsible for Policy Definition and Enforcement by Role in Decision-Making Process



Source: 451 Research's 2021 Cloud Security custom survey

Cloud Complexity

The road to cloud is ongoing, with many organizations and individuals still adapting to running cloud environments. With that in mind, this research asked respondents how they feel about the difference in managing cloud environments compared to on-premises. Specifically, the question posed: 'To what extent do you agree with the following statement: It is more complex to manage privacy and data protection regulations in a cloud environment than on-premises networks within my organization.'

Results were aggregated into agree/disagree/don't know, with global averages as follows:

> "The road to cloud is ongoing, with many organizations and individuals still adapting to running cloud environments."

FIGURE 13

Complexity of Cloud vs. On-Premises Environments

To what extent do you agree with the following statement: It is more complex to manage privacy and data protection regulations in a cloud environment than on-premises networks within my organization.

- **46%** Agree
- **39%** Disagree
- **15%** Don't know

Source: 451 Research's 2021 Cloud Security custom survey

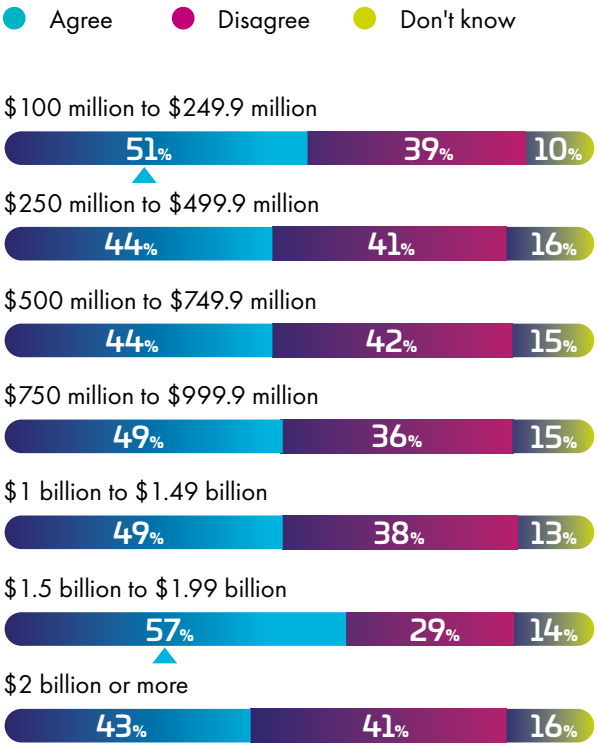
Is Complexity Related to Growing Pains?

The data from this research indicates that, given an organization's size, agreement about the complexity of managing cloud spikes twice: in the smallest companies and in those organizations just shy of being in the largest category. This likely derives from two distinct phenomena: For the smallest companies, the challenge of managing cloud is likely relatively new when compared to on-premises, or the company itself is potentially new and still evolving its governance structure. For the larger category, we theorize it may be related to a shift in governance because increased complexity needs to be handled with newer organizational structures and responsibilities. For those in the $2bn and more group, cloud complexity appears to subside as it becomes one more operational environment to manage.

> **"For those in the $2bn and more group, cloud complexity appears to subside as it becomes one more operational environment to manage."**

FIGURE 14

Complexity of Cloud vs. On-Premises Environments by Organization Size



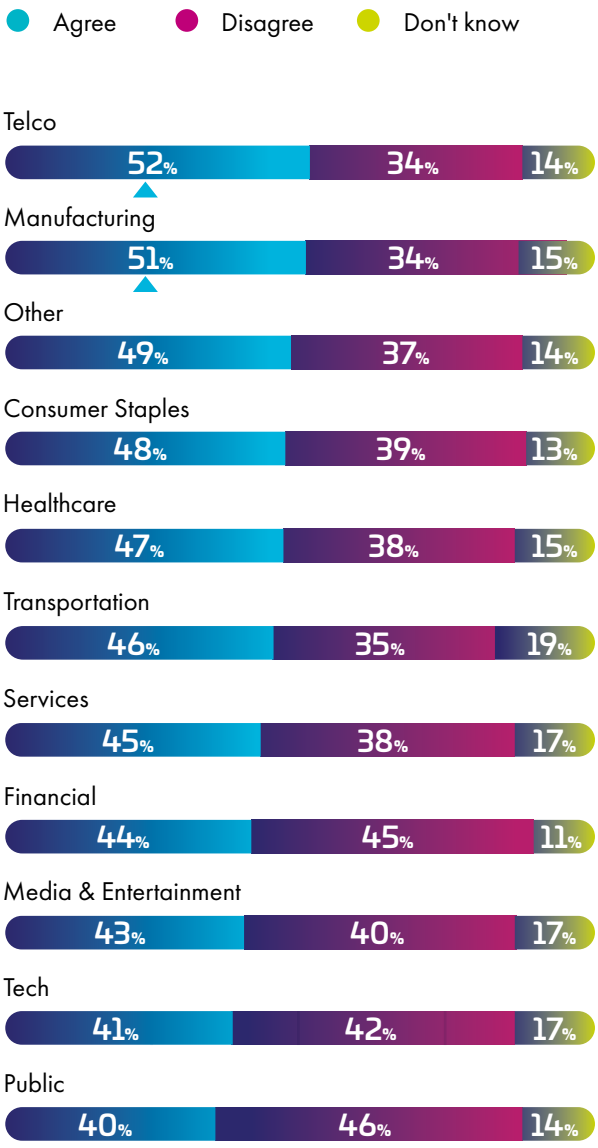
Source: 451 Research's 2021 Cloud Security custom survey

Some Sectors Indicate More of a Struggle

As the data below shows, sectors such as telecommunications and manufacturing indicated a higher level of agreement with the complexity of managing cloud as opposed to on-premises environments. In this scenario, we expect that these sectors addressed the inherent complexity of on-premises deployments via strong operational practices, which now must be revisited considering cloud migrations.

FIGURE 15

Complexity of Cloud vs. On-Premises Environments by Industry Sector



Source: 451 Research's 2021 Cloud Security custom survey

52%

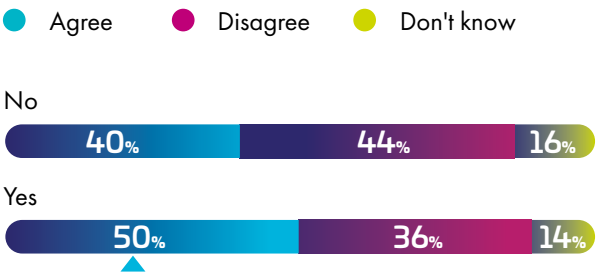
of telecommunications indicated a higher level of agreement with the complexity of managing cloud as opposed to on-premises environments

Multicloud May Exacerbate Complexity

Interestingly, the data shows an increased level of agreement of cloud complexity from those practitioners who indicated they come from organizations that have adopted multicloud. This likely reflects the challenge facing centralized teams such as security, which, as mentioned before, must deal with the complexities of multiple cloud environments, even if specific project teams may only need to be focused on a single cloud provider.

FIGURE 16

Complexity of Cloud vs. On-Premises Environments by Multicloud Adoption



Source: 451 Research's 2021 Cloud Security custom survey

Cloud Migrations

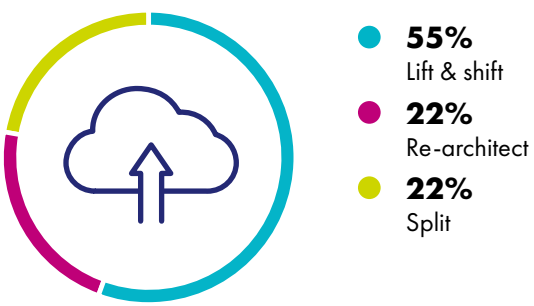
For all the activity around cloud adoption across the board, two key aspects need to be raised: first, virtually all organizations still have a part of their footprint 'on-premises,' which is then tied to cloud resources in what is usually accepted as a 'hybrid' environment; second, there are multiple ways for workloads to be migrated to cloud.

In broad terms, workloads can be 'lifted & shifted' to the cloud (traditionally maintain the use of virtual machines and application architecture, but they are now hosted on a cloud environment) or 're-architected' to incorporate newer concepts such as containerization and serverless function execution. There are some nuances – separate 451 Research indicates there's a sizable proportion of organizations that choose to re-architect but maintain on-premises – but the two broad approaches are 'lift & shift' and 're-architect.' Each has benefits and drawbacks, from potential faster time to value to better use of cloud paradigms and resources.

This research polled participants on their preference for lift & shift or re-architecture. The global results indicate a broad preference for lift & shift.

FIGURE 17

Preferred Method for Migration to Cloud



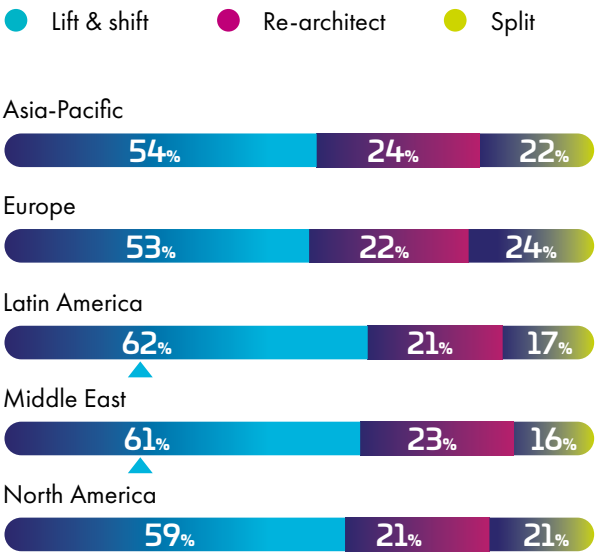
Source: 451 Research's 2021 Cloud Security custom survey

Geographic Preferences Vary

The data shows that Latin America and the Middle East were over the global average for use of lift & shift (62% and 61%, respectively). The research did not inquire about rationale, but these regions also indicated less adoption of multicloud, which also correlates with a preference for lift & shift (see below).

FIGURE 18

Preferred Method for Migration to Cloud by Geography



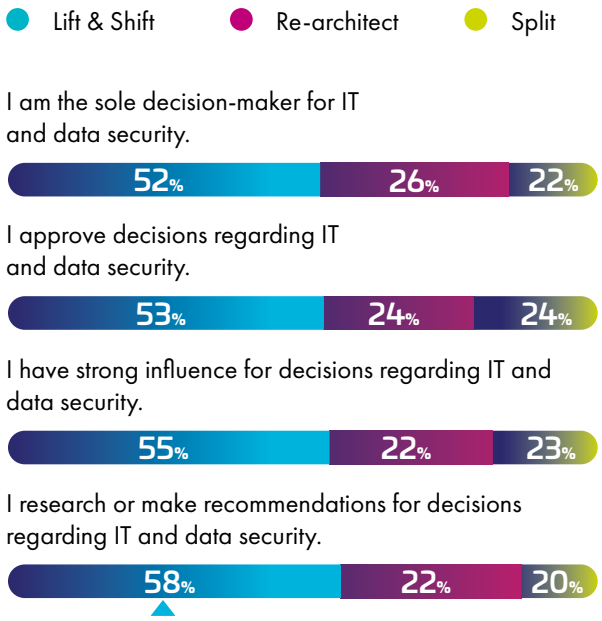
Source: 451 Research's 2021 Cloud Security custom survey

Discrepancy Along Organizational Lines, Again

Once again, there is a discrepancy between staff and senior management regarding lift & shift vs. re-architecture. This time, though, the evidence is stronger when looking at roles related to the purchasing process (as opposed to self-appointed titles). In Figure 19 below, those associated with what typically are staff functions (research and recommendations) favored lift & shift more than the global average. Those with activities related to management have a slight preference for re-architecture.

FIGURE 19

Preferred Method for Migration to Cloud by Role Related to Purchasing Process



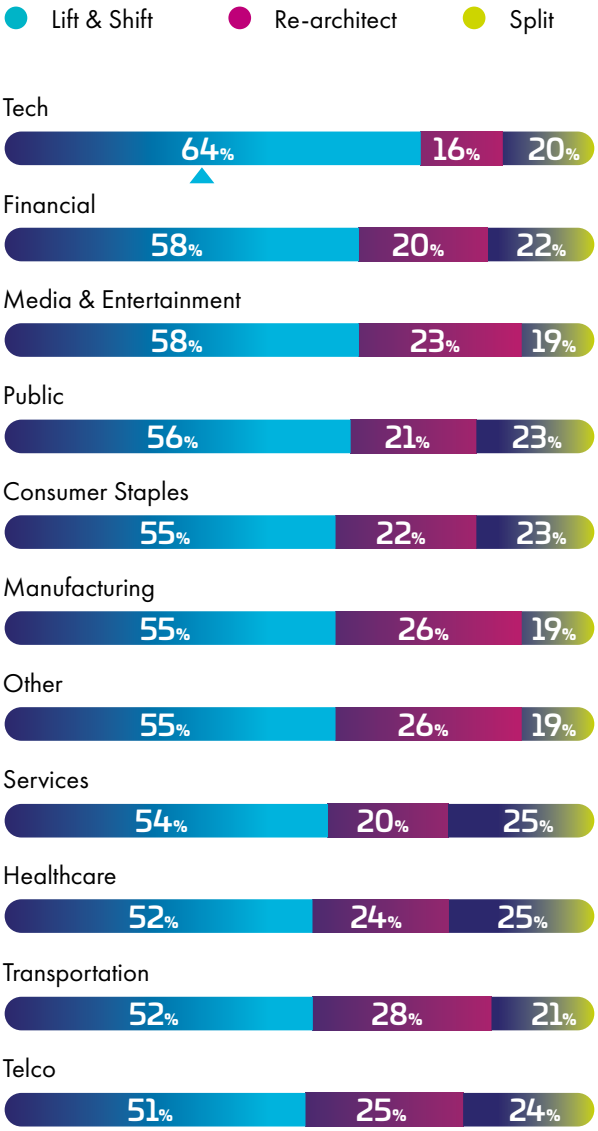
Source: 451 Research's 2021 Cloud Security custom survey

Sector Results Indicate a Mild Surprise

Looking at the same question from the perspective of the various industry sectors shows a somewhat surprising result: those in the technology sector indicated a higher preference for lift & shift (at 64%, well above the 55% global average). While the research didn't cover specific reasoning, it is possible to assume that technology organizations are well positioned to have a more modern technology estate that can be more easily moved to cloud via lift & shift, as opposed to other industries for which the migration effort may be too onerous. Alternatively, technology organizations may have a more nuanced view of the actual benefits of moving to cloud environments and may be able to achieve these benefits with less disruption to their application architectures.

FIGURE 20

Preferred Method for Migration to Cloud by Industry Sector



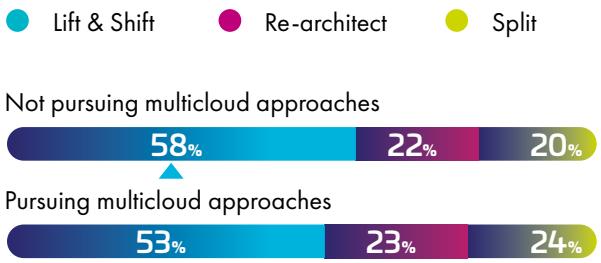
Source: 451 Research's 2021 Cloud Security custom survey

Correlation to Multicloud

Finally, the data indicates that, at a global level, there's a slight preference for the lift & shift approach (above and beyond the global average) by those who self-identified as not pursuing multicloud approaches. As mentioned in the introduction to this section, there are benefits and drawbacks to both approaches, so this should not be taken as a value judgement.

FIGURE 21

Preferred Method for Migration to Cloud by Multicloud Adoption



Source: 451 Research's 2021 Cloud Security custom survey

> “At a global level, there's a slight preference for the lift & shift approach (above and beyond the global average).”

Securing Cloud Environments

As organizations secure cloud environments, they realize they have a host of tools at their disposal, each addressing key aspects of their threat models. This research asked about the key technologies being used to secure cloud deployments.

The evolution of the threat landscape – be it the rise of ransomware or the challenges around post-breach credential-stuffing attacks – is driving increasing awareness and adoption of multi-factor authentication (MFA) as a common, if not best, practice in access management: use of MFA may be the difference between a remote attacker taking over corporate resources or a diligent end-user quickly notifying Security that something is amiss.

With that in mind, the research data shows that organizations still have a long way to go for MFA to be broadly adopted. According to survey results, only approximately 16% of global respondents indicate they use MFA to secure more than half of the cloud services they use. Worryingly, the equivalent proportion of those using MFA for more than half of their on-premises applications falls, at a global level, to just 11%.

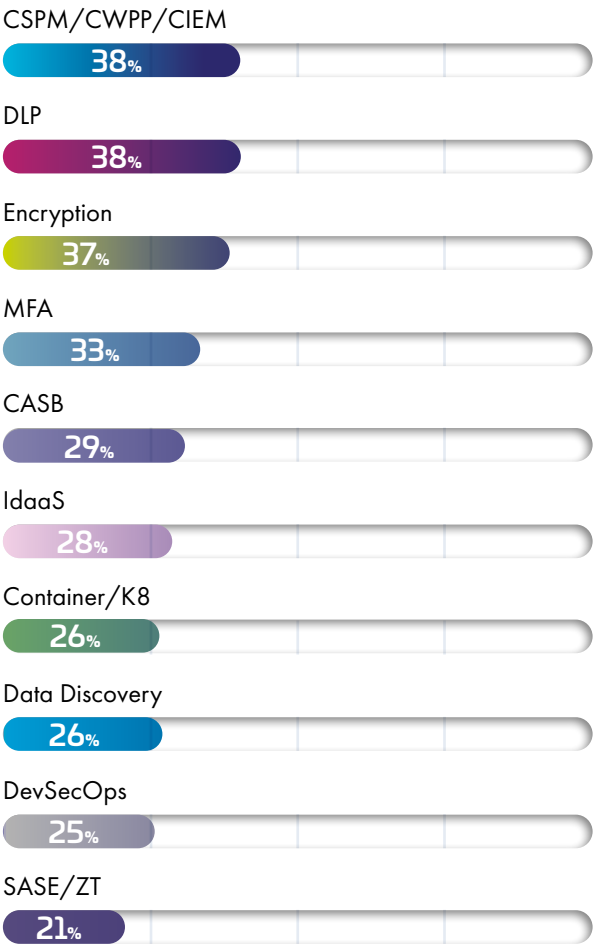
The complexity facing those looking to secure modern environments – which are often a hybrid of on-premises and cloud – also shows up as a key access management challenge: according to global respondents, 66% of them consider securing the combination of on-premises and cloud either "challenging" or "very challenging".

We asked respondents to rank their top three choices from a list of options. The results below aggregate these answers by indicating how often the option came up as one of the top three choices.

The global results are as follows:

FIGURE 22

Key Technologies Being Used to Secure Cloud Deployments



Source: 451 Research's 2021 Cloud Security custom survey

> **“Senior managers indicated a higher response rate for cloud tools (42%) than staff respondents (34%).”**

When aggregating responses globally, cloud-specific tools (cloud security posture management, cloud workload protection, cloud identity and access management), data loss prevention (DLP), encryption, and multi-factor authentication (MFA) were consistently the top ranked choices as tools for securing data in cloud environments.

These top results hold broadly across multiple lenses such as geography, firm size, sector and title, with some outliers. Some of the notable exceptions include:

- Smaller organizations (100-249m in revenue) responded particularly high to cloud tools (47%) and encryption (42%) but relatively low on MFA (25%).
- Respondents from the Middle East indicated a preference for cloud tools (42%) and increased preference for containers/Kubernetes and DLP, but a notably lower response for CASB (22%), which correlates with lower SaaS apps numbers as reported elsewhere in this research.
- North American vendors followed the general trend, with a slight uptick in choosing SASE/Zero Trust (although still only at 24%).
- Senior managers indicated a higher response rate for cloud tools (42%) than staff respondents (34%).
- Financial sector respondents indicated high support for encryption (42%) and higher than usual support for IDaaS (38%).
- Technology sector respondents had a strong preference for MFA (45%).
- Public sector respondents indicated support for cloud security tools (42%).
- Respondents in the transportation sector had a high level of support for encryption (42%).

Interestingly, there were no material differences in responses between those that self-identified as having multicloud within their organizations or not.

Encryption and Key Management in the Cloud

As the previous section showed, encryption is one of the key technologies that respondents have chosen to address cloud security needs. Delving into use of encryption requires addressing two aspects: deploying encryption capabilities to data residing in cloud, and managing the keys used for encryption. There's also the matter of just how much data should be encrypted. Normally, we would expect all or most sensitive data in the cloud to be encrypted. However, research results point to a different result.

We asked respondents what percentage of their sensitive data in cloud is encrypted (Figure 23). To calculate an approximate proportion of sensitive data being encrypted, we calculated the midpoint of each interval for an average number (used 75% as midpoint for 50%+).

The result is that the global average is just 41%.

While some organizations indicated that they encrypt more than 50% of their sensitive data in cloud, that proportion on a global level is merely 17%.

FIGURE 23

Percentage of Sensitive Data in Cloud that is Encrypted

- **2%** 0-10%
- **9%** 11-20%
- **18%** 21-30%
- **26%** 31-40%
- **28%** 41-50%
- **17%** >50%
- **0%** Don't Know

Source: 451 Research's 2021 Cloud Security custom survey

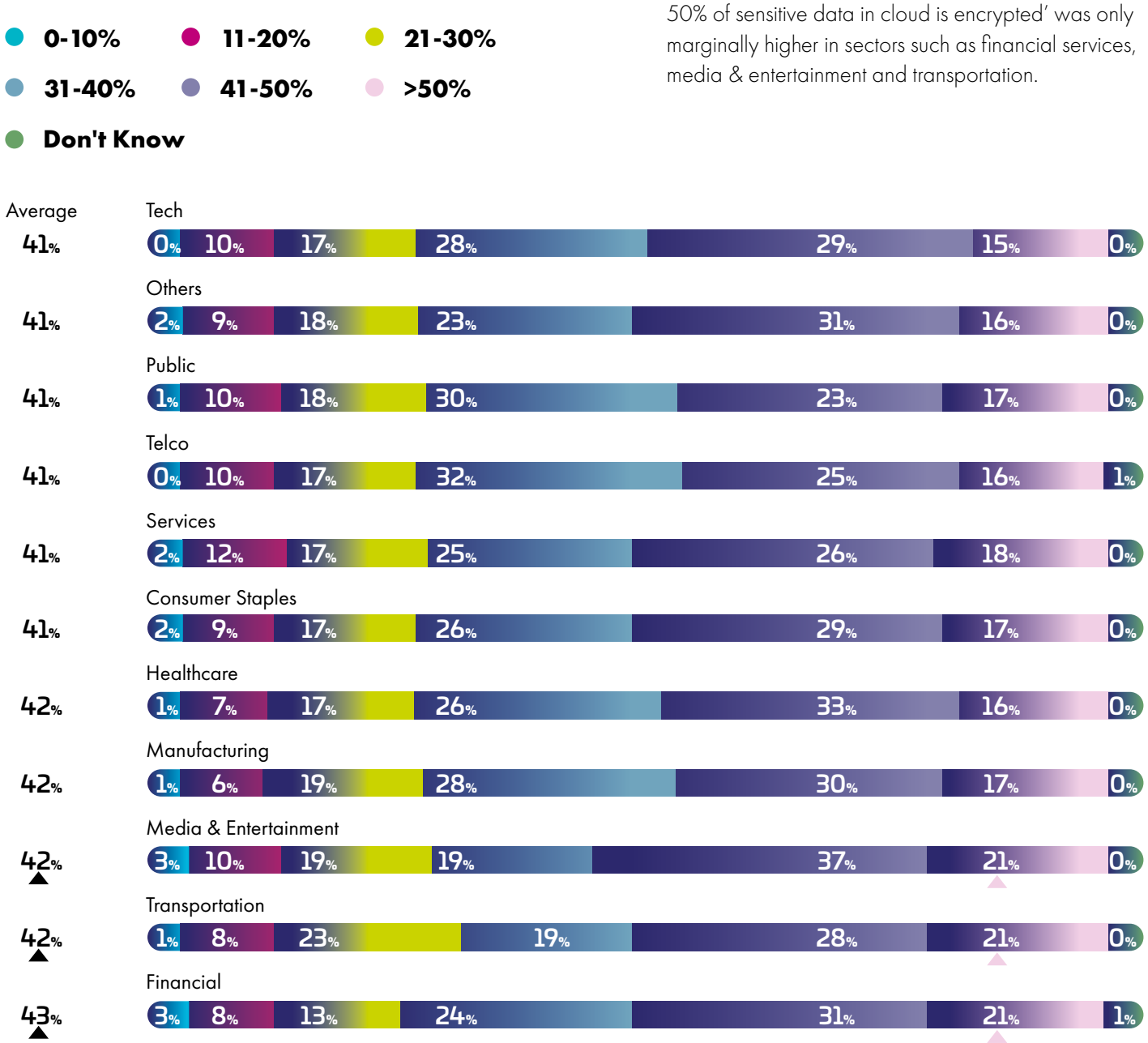
17%

of organizations encrypt more than half their sensitive data.

FIGURE 24

Percentage of Sensitive Data in Cloud that is Encrypted by Industry Sector

Proportion of Encrypted Workloads by Sector



Source: 451 Research's 2021 Cloud Security custom survey

Little Movement Between Sectors

The various industry sectors are about the same regarding the encryption of sensitive data in cloud. The proportion of respondents that picked 'more than 50% of sensitive data in cloud is encrypted' was only marginally higher in sectors such as financial services, media & entertainment and transportation.

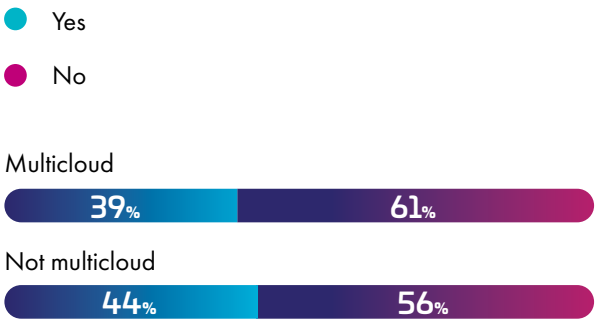
Multicloud Appears to Come at a Cost

Organizations adopting multicloud appear to understand it is not a zero-cost effort and may have shifted their attention away from encryption. This could explain why organizations adopting multicloud indicated slightly lower average encryption usage.

FIGURE 25

Percentage of Sensitive Data in Cloud that is Encrypted by Multicloud Adoption

What percentage of sensitive data is encrypted?



Source: 451 Research's 2021 Cloud Security custom survey

The effect is not huge, but teasing out some of the complexity of multicloud, the proportion of respondents that indicated they have adopted multicloud and encrypt more than 50% of their sensitive data in cloud falls to just 15%.

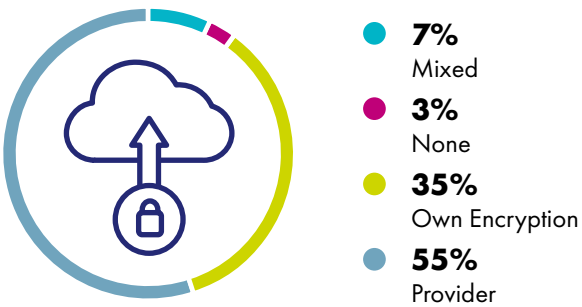
> **"Organizations adopting multicloud appear to understand it is not a zero-cost effort."**

Delivering Encryption Capabilities to Cloud Environments

When considering what kind of encryption capabilities are used to encrypt sensitive data, organizations have the choice of using services from their cloud services provider, rolling out their own third-party encryption capability for handling that data, or using a mixture of both. The worldwide averages for how organizations choose are as follows:

FIGURE 26

Type of Encryption Capabilities Used



Source: 451 Research's 2021 Cloud Security custom survey

Looking at the responses from different perspectives yields similar results. Some of the notable differences include:

- Geographically, there is some slight difference as Latin America has increased use of their own encryption (41%), and the Middle East has greater use of encryption from a provider (63%).
- When considering organization size, there's an increase in use of own encryption (from 26% to mid-high 30s) as organizations grow.
- Respondents in the manufacturing sector indicated more use of own encryption at 42%.

35%

of respondents indicated use of own encryption.

Key Management for Cloud

There's more to protecting sensitive data in cloud with encryption than just deciding how to implement that encryption. Key management becomes a concern, particularly since cloud usage fundamentally means a shared responsibility between the organization and the provider, but not a relinquishing of ultimate responsibility of data protection between the organization and its clients and stakeholders.

Much like the use of encryption technology, there are different approaches to managing keys for cloud environments. The organization may use encryption provided by the cloud service provider but still retain control over how keys are created and managed, or the organization may choose to use provider-managed keys. Put simply, the trade-off is between cost and control.

This research polled respondents on how they approach key management. The global answers are to the right:

> "Much like the use of encryption technology, there are different approaches to managing keys for cloud environments."

FIGURE 27

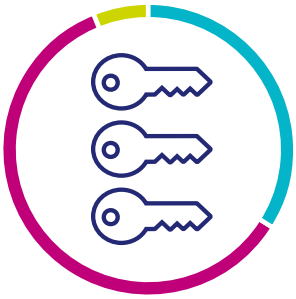
Approach to Key Management

- **34%** All or mostly cloud provider controls encryption keys
- **21%** All or mostly we control encryption keys
- **26%** Cloud provider controls all encryption keys
- **6%** Shared – we control key generation material but provider control keys
- **12%** We control all encryption keys

Source: 451 Research's 2021 Cloud Security custom survey

FIGURE 28

Key Management Subgroups



- **34%** Own control
- **60%** Provider
- **6%** Shared

Source: 451 Research's 2021 Cloud Security custom survey

There's regional nuance in that Latin America has a slightly higher proportion of respondents indicating use of own keys (39%), and Middle East respondents indicated greater use of provider keys (65%).

From a sector perspective, healthcare stands out with 67% of respondents indicating use of provider keys.

Organizations need to balance choices. While some choices such as provider keys may favor more immediate operational simplicity, others are better at supporting strong ownership of data. For those organizations concerned with data access requests from government agents, for example, the use of self-managed keys can possibly offer additional levels of protection. Furthermore, those with specific compliance mandates may also look favorably to maintaining greater control over encryption keys.

62%

of healthcare respondents indicated use of provider keys.

Prevalence of Breaches and Compliance Issues

Ultimately, one of the key goals of security is to protect the organization, supporting its many internal needs, processes, constraints and objectives so it can achieve its desired outcomes while minimizing the cost of securing it and preventing breaches.

This research inquired about the prevalence of breaches and audit issues in cloud environments. Given the observational nature of research surveys, this report makes no claims on causality; rather, it presents data for further discussion.

When asked *'Has your organization ever experienced a data breach involving data and applications that reside in the cloud?'* responses were split worldwide as follows.

FIGURE 29

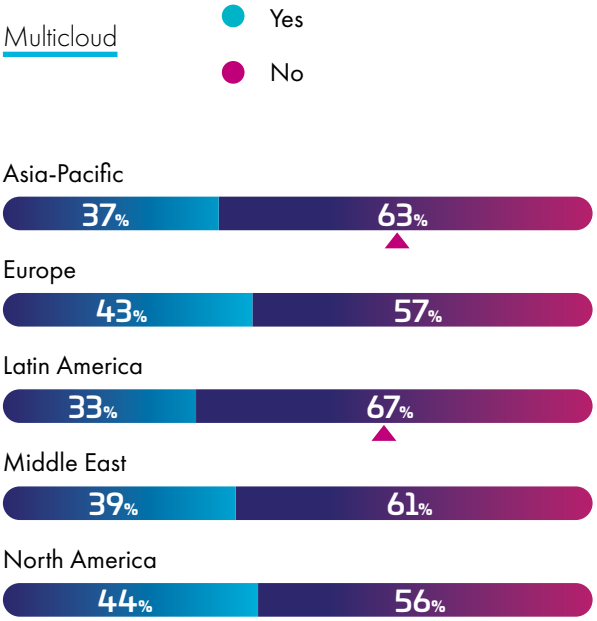
Experienced a Data Breach

Source: 451 Research's 2021 Cloud Security custom survey

When looking for regional nuance, we observe that those in Latin America and Asia-Pacific indicated lower rates of cloud-related breaches.

FIGURE 30

Experienced a Data Breach by Geography

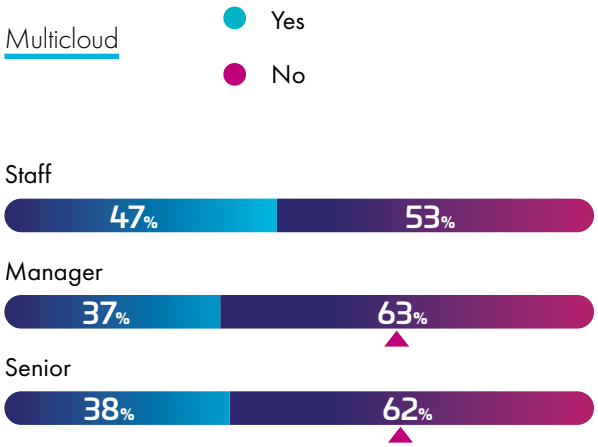


Source: 451 Research's 2021 Cloud Security custom survey

Meanwhile, the split inside organizations is again present. A slightly higher proportion of those in management compared to those in staff positions indicated that they have not had a breach involving their cloud environment or data.

FIGURE 31

Experienced a Data Breach by Role



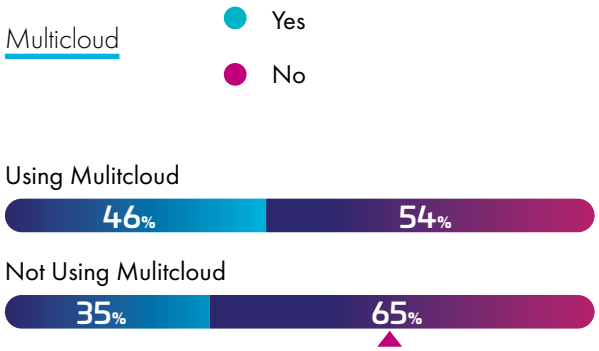
Source: 451 Research's 2021 Cloud Security custom survey

From a sector perspective, healthcare, telecommunications and consumer staples responded more often that they had not experienced breaches in their cloud environments (at 65%, 65% and 64%, respectively).

Interestingly, those who self-identified as multicloud organizations responded that they had not experienced breaches in higher numbers.

FIGURE 32

Experienced a Data Breach by Multicloud Adoption



Source: 451 Research's 2021 Cloud Security custom survey

The slight difference in the response rate for multicloud respondents may indicate that organizations choosing to deploy the necessary resources to improve their cloud expertise (using their multicloud status as a potential marker for this additional experience/expertise) may indeed be able to consume cloud services in a more secure manner.

We asked a similar question about compliance issues – 'Has your organization experienced a breach or failed an audit involving data and applications stored in the cloud this past year?' Results were generally consistent with the breach data as reported above, with a slightly higher number of global respondents indicating that they had an issue – 43% for breach/audit issues compared to 40% for breaches.

Moving Ahead

This research paints a picture that shows variety in how organizations are tackling cloud adoption – the use of multicloud, how cloud governance is shaping up, which controls are being used, etc. Readers are encouraged to review these trends and compare them to how their own organizations are tackling cloud adoption.

In terms of high-level guidance, each organization has its own set of objectives, preferences and constraints, but some key themes have emerged:

- There's a high likelihood that security teams at all organizations – particularly larger ones – will need to account for the need to support multicloud use cases. This will require balancing security features from the cloud provider – or multiple cloud providers – with how to deliver and centrally manage the same security outcomes across multiple providers and organizational environments.
- There's a gap between practitioners and senior management in multiple areas, which, if left unaddressed, may result in friction within the effort to secure cloud adoption. For most organizations, effective security requires alignment both at the operational level and within senior leadership conversations.
- The research data indicates that a large proportion of organizations have had issues involving data residing in cloud. This means organizations will likely need to have strong support for cloud environments in their incident detection and response capabilities.
- To the extent that protecting customer data is a priority, organizations should strongly consider reviewing their strategies and approaches to proactively protect data in cloud, especially sensitive data. This includes understanding the role of specific controls and technologies including authentication, encryption and key management, as well as the shared responsibilities between providers and their customers.
- As data privacy and sovereignty regulations grow across the globe, it will be paramount for end-user organizations to have a clear understanding of how they remain responsible for data security and how they must make clear decisions about just who is in control of and who can access their sensitive data.

Methodology

This research was based on a global survey of 2,625 respondents, fielded in January 2021, 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$100m and with US$100-250m in selected countries.

This research was conducted as an observational study and makes no causal claims.

Demographics

FIGURE 33

Countries

USA	507
Mexico	101
Brazil	100
UK	255
Germany	252
Sweden	101
Netherlands	100
France	251
UAE	101
India	202
Australia	101
New Zealand	51
Japan	201
South Korea	100
Singapore	101
Hong Kong	101

FIGURE 35

Titles

Staff	661
Manager	1146
Senior	818

FIGURE 34

Revenue

$100 million to $249.9 million	120
$250 million to $499.9 million	623
$500 million to $749.9 million	819
$750 million to $999.9 million	624
$1 billion to $1.49 billion	210
$1.5 billion to $1.99 billion	76
$2 billion or more	153

FIGURE 36

Industry Sector

Consumer Staples	429
Services	351
Healthcare	306
Public	301
Manufacturing	232
Tech	205
Other	202
Media & Entertainment	191
Transportation	145
Financial	133
Telco	130

THALES

Building a future we can all trust

Contact us

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

cpl.thalesgroup.com/cloud-security-research