Global Edition

THALES
Building a future we can all trust

2022 Thales Cloud Security Study

The Challenges of Data Protection in a Multicloud World

#2022CloudSecurityStudy

cpl.thalesgroup.com

Introduction

Businesses across the globe are accelerating the shift to the cloud in a modern digital world where infrastructure has to be more agile, capable and distributed to support customers and hybrid workforces that are accessing data from anywhere. This shift is driving dramatic increases in multicloud adoption to expand ecosystems of partners and to enable effective and efficient remote work. Along with this shift, security challenges have changed and increased and are top of mind for IT teams and security professionals.

As more data is stored across multiple cloud providers, surveyed companies continue to report issues with cloud data breaches and failed audits. Attacks targeting cloud resources are also on the rise, and enterprises need help understanding what threats to be concerned about and how to protect against them. New types of security platforms and cloud-native security services have emerged, and enterprises need help understanding which ones they should consider adopting for various cloud security use cases, especially as they apply to sensitive data and workloads.

This report presents findings from a global survey of almost 2,800 respondents, spread across 17 countries and a broad range of industries, organization sizes and job functions. The Methodology section covers the specifics of the survey in more detail. The purpose of this research paper is to help enterprise IT and security teams understand the cloud and security challenges faced by their peers, and to help guide cloud security strategy and budgets.

451 Research

S&P Global
Market Intelligence

Source: 2022 Cloud Security custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Contents

Key Findings

This global survey asked enterprises about topics such as multicloud, cloud complexity and cloud security technologies, specifically authentication, data encryption and key management. This report highlights the survey results and provides analysis to help enterprises understand those results and their implications. Key findings include:

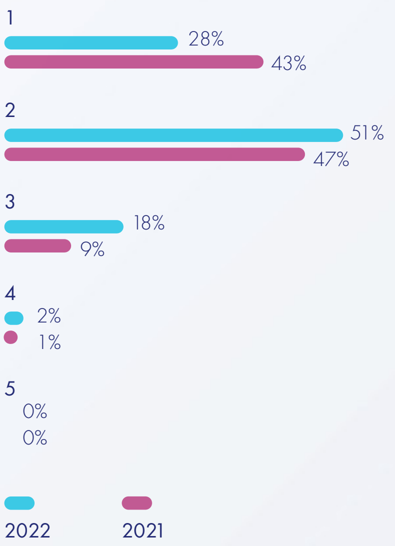
- **Multicloud adoption is growing dramatically.** Respondents report significant expansion in the use of multiple IaaS providers. When contrasted with progress in operational patterns, this could be causing complexity for security teams.
- **Multicloud complexity is creating security challenges.** Complexity is the enemy of effective and efficient security, and respondents report multicloud challenges.
- **There is more sensitive data in the cloud, and it is raising concerns.** The move to cloud has to come with expanded data protections such as encryption, but many are falling short.
- **Security teams are driving cloud policies.** Some level of consolidated management can be useful, but the increasing pace of multicloud adoption can be a burden on security teams if they don't become efficient.
- **Cloud data breaches and failed audits are common.** Dealing with multicloud complexity can be challenging for security teams.
- **Increasing attacks present a greater risk to cloud applications and data.** Respondents are concerned about increased attack surface and effective mitigations.
- **Enterprises see encryption as important to protect their cloud environments.** This is a useful understanding, but it has to translate into implementation, which is at worryingly low levels.
- **Encryption key management is a challenge for enterprises.** This is a historical issue with the cloud and has become more acute as multicloud operations become the norm.
- **Enterprises are embracing zero trust and investing accordingly.** There has been improvement in reported adoption, and there is still room to grow.
- **Understanding of authentication is maturing.** Organizations are improving their understanding of how they can put better authentication and access management to work.
- **Modern authentication techniques are being applied more broadly.** Enterprises are now using modern authentication across both on- and off-premises environments in larger percentages.

> “
>
> **No organization is immune from data security threats, with 45% of global respondents experiencing a data breach at some point.”**

Multicloud Adoption Is Growing

There is a notable increase in the use of multiple IaaS providers. In the 2022 survey, 72% of respondents reported using multiple IaaS providers, compared with 57% the year before. More striking still, the number of respondents using three or more IaaS providers doubled to 20% from 10%. Enterprises surveyed reported using an average of 53 SaaS applications (weighted average).

Number of IaaS Providers Reported



Source: 451 Research's 2021 and 2022 Cloud Security custom surveys

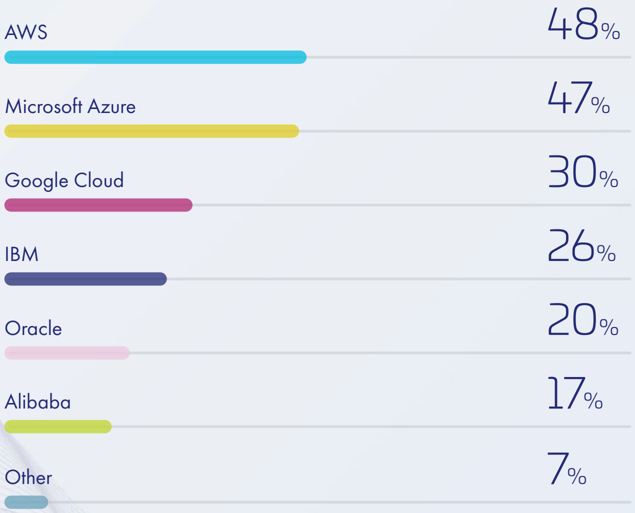
20%

of respondents using three or more IaaS providers doubled to 20% from 10% compared to the previous year.

The journey to the cloud is becoming more complex. For IaaS and PaaS, customers said they're doing a mix of lift-and-shift, repurchase-and-shift, and rearchitecting when migrating applications to the cloud. That mix is changing, with the percentage intending to lift-and-shift, the simplest of migration tactics, dropping from 55% to 24% this year. That could indicate that organizations are moving complex applications to the cloud, which requires complex operational support.

IaaS Providers Used in a Production Capacity

WHICH IAAS PROVIDERS DOES YOUR ORGANIZATION USE IN A PRODUCTION CAPACITY?



Source: 451 Research's 2022 Cloud Security custom survey

Multicloud Complexity Creates Security Challenges

Alongside growing multicloud use, overall cloud use by enterprises is also growing compared to last year's results. When asked what percentage of their organization's workloads and data resides in the cloud (external cloud providers), only 24% said more than 60%, and only 8% said more than 80%. This indicates that most customers are using a mix of venues – on-premises, data center, private cloud, etc. – in addition to external cloud providers.

Cloud security tool sprawl may also be an issue, especially for complex multicloud environments, judging by the wide variety of systems that enterprises are using to secure remote cloud access and cloud environments. Respondents mentioned encryption, key management, hardware security modules, zero trust network access, single sign-on, a virtual private network and multi-factor authentication as key systems for securing access to data in the cloud. Respondents also mentioned using cloud workload protection, cloud security posture management and DevOps to secure cloud-based applications. In addition, many are using multiple key management platforms to manage encryption across cloud environments. The large number and wide variety of platforms is a further indication of the complexity of managing multicloud environments.

Sensitive Data in Cloud

Respondents reported that sensitive data is being stored across multicloud environments, and data storage and classification are major concerns. Enterprises are storing some sensitive data in cloud providers, but not exclusively. Most respondents (66%) store 21-60% of their sensitive data in the cloud. Only 22% store more than half (61-100%) of their data in the cloud. This suggests that many enterprises still store a significant amount of sensitive data outside of cloud environments, likely on-premises or in privately hosted infrastructure.

More than half (51%) of respondents agree that managing privacy and data protection in a cloud (multicloud or hybrid) environment is more complex than on-premises. This is a notable change from 46% agreeing the year before, indicating a sustained increase in this concern alongside the reported increase in the use of multiple cloud providers. If organizations are trying to secure cloud environments individually rather than through a shared management platform, it will increase the burden of coverage on security teams. Results that we will discuss later indicate that organizations tend to use native cloud controls for tasks such as encryption management, and this trend contributes to complexity.

Enterprises also reported that data storage and classification are major concerns. Only 19% of respondents said they know where all of their data is stored. Twenty-two percent were able to classify very little (to none) of their data, and only 25% could fully classify their data. This discrepancy is likely due to complex multicloud environments for data storage that span across cloud providers, on-premises infrastructure, applications and teams.

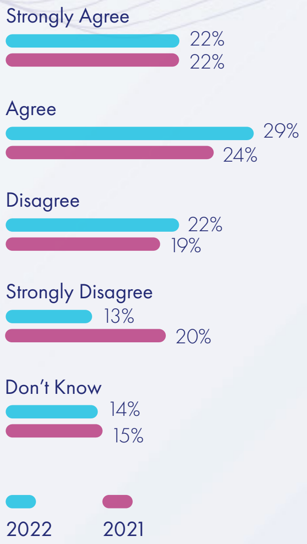
Only

19%

of respondents said they know where all of their data is stored.

Cloud Management Complexity

TO WHAT EXTENT DO YOU AGREE WITH THE FOLLOWING STATEMENT: IT IS MORE COMPLEX TO MANAGE PRIVACY AND DATA PROTECTION REGULATIONS IN A CLOUD (MULTICLOUD/HYBRID) ENVIRONMENT THAN ON-PREMISES NETWORKS WITHIN MY ORGANIZATION?



Source: 451 Research's 2021 and 2022 Cloud Security custom surveys

Security Teams Drive Policy and Standards

Security teams play a major role in deciding and enforcing policies and standards. Eighty-four percent of respondents said security teams define policy. That encompasses 37% who indicated that security teams manage both policy and standards, and 48% who said that security teams set policy but that setting and enforcing technical standards is left to cloud delivery teams. Only 16% said they leave policies, standards and enforcement to cloud delivery teams. The increase in cloud operations' speed and scale, especially considering the expanded use of multicloud environments, will strain security teams. To increase efficiency, organizations need to establish guidelines for consumers of cloud infrastructure that will allow them to build secure environments without direct intervention from security teams.

Security teams can be far more efficient if they can set policy at a level of abstraction that can translate to the specific controls available from individual cloud providers. Security platforms extending across multiple cloud providers can be instrumental in managing multicloud complexity and reducing the work required to onboard a new cloud provider.

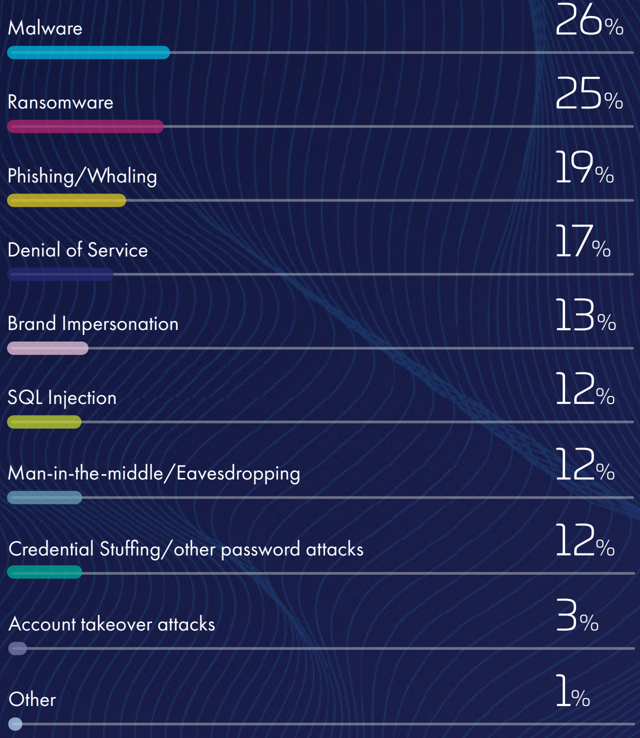
Cloud Data Breaches and Failed Audits Are Common

A significant percentage of respondents have suffered from cloud data breaches or failed audits. Forty-five percent of respondents said they have experienced a data breach or failed an audit involving data and applications that reside in the cloud, an increase from 40% in 2021. Thirty-five percent said they have experienced a data breach or failed an audit involving data and applications that reside in the cloud in the last year. Thirty-two percent of respondents reported having to issue a breach notification to a government agency, customers, partners or employees. Breach notifications are a cause for concern among enterprises with sensitive data, particularly in highly regulated industries.

> **"Thirty-five percent said they have experienced a data breach or failed an audit involving data and applications that reside in the cloud in the last year."**

Types of Cyberattacks Increasing

WHAT TYPES OF ATTACKS/THREATS HAVE YOU SEEN AN INCREASE?



Source: 451 Research's 2022 Cloud Security custom survey

Increasing Attack Risk for Cloud Assets

Cloud assets topped respondents' list of the biggest targets for cyberattacks. Enterprises specifically mentioned web applications, cloud-delivered applications (SaaS), cloud-hosted applications (IaaS, PaaS) and cloud-based storage as top targets for attack. A significant volume of sensitive data resides in the cloud and could be targeted by such attacks. A large majority (85%) said at least 20% of their data in cloud is sensitive. More than half (58%) said at least 40% of their data in the cloud is sensitive.

Respondents also reported that attacks are increasing and present a greater risk to cloud applications and data. Twenty-six percent of respondents experienced an increase in malware attacks, 25% saw an increase in ransomware and 19% experienced more phishing or whaling. These three categories present significant risks to cloud applications and data. Cloud-based storage and cloud databases are leading targets of attack. Respondents also identified web applications, cloud-delivered applications (SaaS) and cloud-hosted applications (IaaS, PaaS) as particular targets for attack.

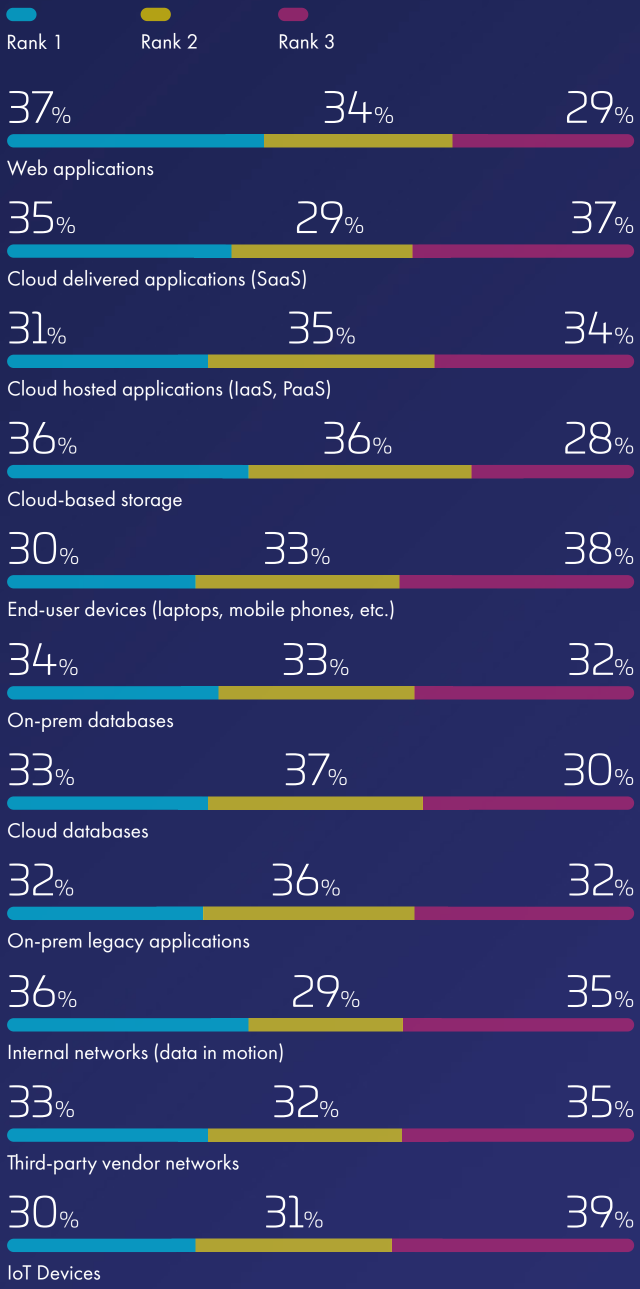
26%

of respondents experienced an increase in malware attacks

Primary Perceived Targets for Cyberattacks

IN GENERAL, HOW DO YOU RANK THE FOLLOWING AS TARGETS FOR CYBERATTACKS?

RANK 3 IN ORDER OF PRIORITY



Source: 451 Research's 2022 Cloud Security custom survey

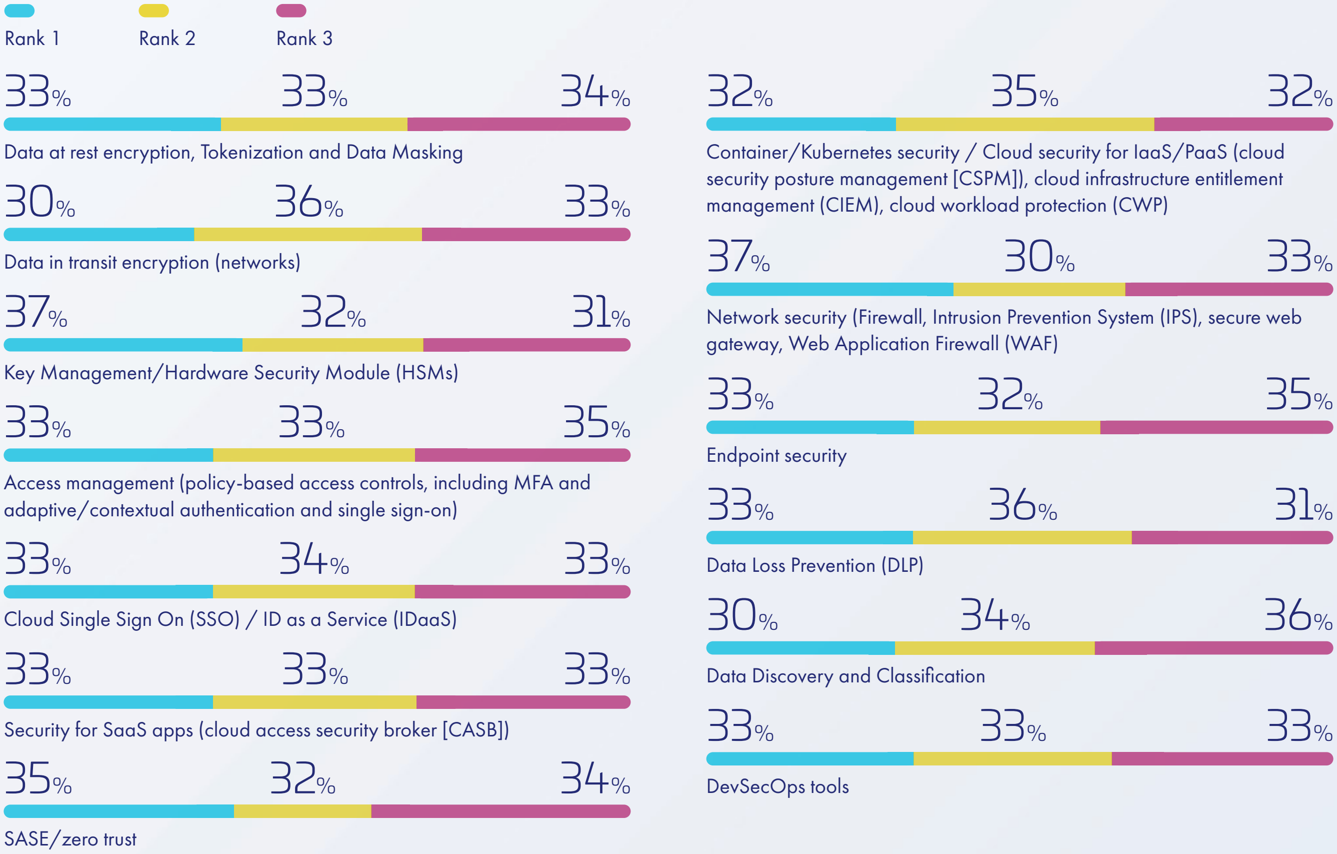
Cloud Protection Strategies

Customers view encryption, key management, remote access security technologies and zero trust as effective ways to reduce cloud risks. These technologies are currently in use, and they are also prioritized for future budgets/investments. There is broad interest across the full set of controls in the survey, which indicates that respondents are drawing on all the tools at their disposal but also speaks to the complexity of addressing a diverse set of risks in the cloud.

Survey respondents see encryption as a key technology to prevent sensitive data from a cyberattack. Respondents cited data-at-rest encryption, tokenization and data masking; data-in-transit encryption; and key management/hardware security modules as top choices. When asked about the primary driver for decisions on where and how encryption is used in the cloud, 46% of respondents said internal security architecture decisions, 39% said regulatory compliance requirements, and 12% said customer or partner requirements. Encryption and key management topped the list (59% and 52% of respondents, respectively) as critical to protecting sensitive data in the cloud.

Technologies Considered Most Effective for Protecting Sensitive Data

HOW DO YOU RANK THE FOLLOWING SECURITY TECHNOLOGIES IN TERMS OF EFFECTIVENESS IN PROTECTING SENSITIVE DATA FROM CYBERATTACKS? RANK 3 IN ORDER OF PRIORITY

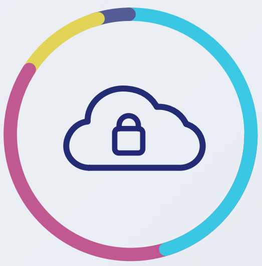


Source: 451 Research's 2022 Cloud Security custom survey

Cloud Protection Strategies (continued)

Primary Drivers for Cloud Encryption Decision-Making

WHAT IS THE PRIMARY DRIVER FOR DECISIONS ON WHERE AND HOW ENCRYPTION IS USED IN CLOUD?

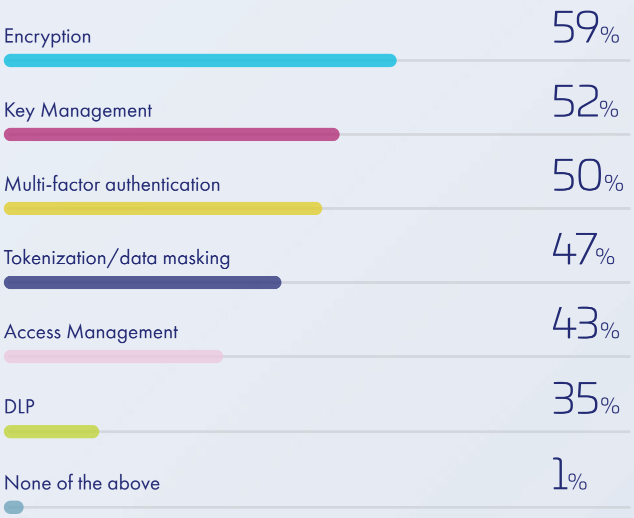


● Internal security architecture decisions	46%
● Regulatory compliance requirements	39%
● Customer or partner requirements	12%
● Other requirements	3%

Source: 451 Research's 2022 Cloud Security custom survey

Security Technologies in Use To Protect Sensitive Data in the Cloud

WHICH SECURITY TECHNOLOGIES IS YOUR ORGANIZATION USING TO PROTECT SENSITIVE DATA IN THE CLOUD?



Source: 451 Research's 2022 Cloud Security custom survey

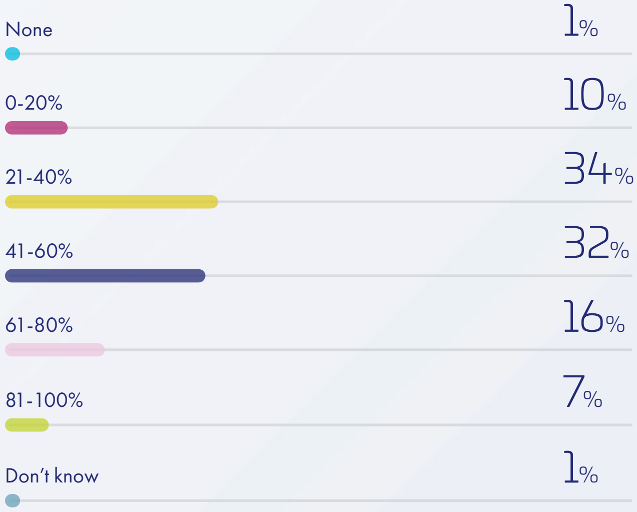
Cloud Protection Strategies (continued)

Enterprises see encryption as important to protecting their cloud environments. Survey data suggests that enterprises are encrypting more sensitive data in the cloud than last year. However, many still have lots of sensitive data in the cloud that is not yet encrypted. When asked what percentage of their sensitive data in the cloud is encrypted, only 11% of respondents said 81-100% is encrypted. The remaining 89% said less than 80% is encrypted. Many respondents also have issues classifying data and have sensitive data stored outside of cloud environments. This indicates an opportunity for enterprises to reduce risk by using platforms that help discover, protect and control their data using a single platform that works across multicloud environments.

When asked how enterprises manage encryption in IaaS/PaaS environments, they reported using a mix of cloud provider platforms and their own platforms. This area was, unfortunately, largely unchanged from last year. Far too many said they rely on cloud providers for encryption and key management. While only 17% use cloud provider encryption exclusively, 39% said more than half of their applications use cloud provider encryption. Only 21% said more than half of their applications bring their own encryption, and just 13% bring their own encryption exclusively. Bringing one's own encryption has the dual benefit of mitigating the risk of third-party exposure and simplifying operations in a multicloud environment. Bringing your own encryption is a cloud security model wherein customers of cloud providers use their own encryption software and manage their own encryption keys. On a positive note, more respondents reported having complete control of encryption keys – moving from 12% last year to 15% this year. It's a small but important shift, and one that could be accelerated with the use of encryption management systems that can manage across multiple cloud providers.

Percentage of Workloads and Data Residing in the Cloud

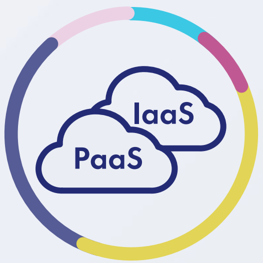
WHAT PERCENTAGE OF YOUR ORGANIZATION'S WORKLOADS AND DATA RESIDES IN THE CLOUD (EXTERNAL CLOUD PROVIDER/S)?



Source: 451 Research's 2022 Cloud Security custom survey

Current Methods of Data Encryption in IaaS/PaaS Environments

HOW DOES YOUR ORGANIZATION ENCRYPT DATA IN IAAS/PAAS ENVIRONMENTS?



●	We use cloud provider encryption only	17%
●	We bring our own encryption only	13%
●	More than half of our applications use cloud provider encryption	39%
●	For more than half of our applications, we bring our own encryption	21%
●	We bring our own encryption for select workloads, use provider encryption otherwise	10%

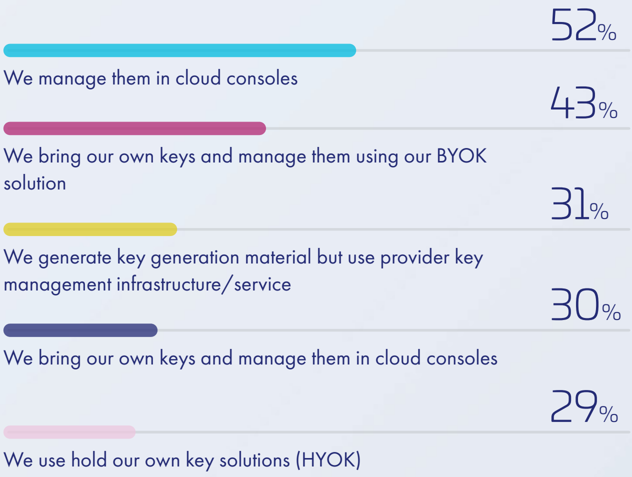
Source: 451 Research's 2022 Cloud Security custom survey

Challenges of Key Management in the Cloud

Encryption key management is a challenge for enterprises. When asked who controls their encryption keys, survey results showed a mix of customers and cloud providers controlling all keys and an understanding of shared responsibility. Shared responsibility refers to sharing the security obligations and accountability between the cloud provider and its users. Regarding how enterprises control encryption keys, results showed a mix: managing them in cloud consoles; bring your own keys (BYOK) and managing them using their own platform; generating key material but using cloud provider key management; bringing their own keys and managing them in cloud consoles; and using hold-your-own-key (HYOK) platforms.

Methods of Controlling Encryption Keys

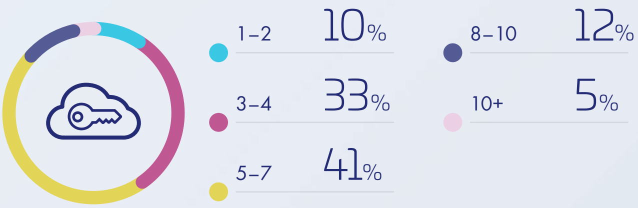
HOW DOES YOUR ORGANIZATION SPECIFICALLY CONTROL ENCRYPTION KEYS?



Source: 451 Research's 2022 Cloud Security custom survey

Number of Key Management Solutions in Use

HOW MANY DIFFERENT KEY MANAGEMENT SOLUTIONS DOES YOUR ORGANIZATION HAVE? INCLUDE ENTERPRISE KEY MANAGER VENDORS, CLOUD PROVIDER KEY MANAGER, ETC.



Source: 451 Research's 2022 Cloud Security custom survey

Survey results also showed that key management platform sprawl may be an issue for enterprises. Only 10% of respondents use one to two platforms, 90% use three or more, and 17% use eight or more platforms.

In summary, the survey results show enterprises using a mix of encryption platforms (their own and cloud providers'), mixed strategies for controlling encryption keys, and a sprawl of key management platforms. This indicates an opportunity for enterprises to consolidate and centralize on independent third-party platforms that reduce complexity and provide coverage across multicloud environments.

Zero Trust

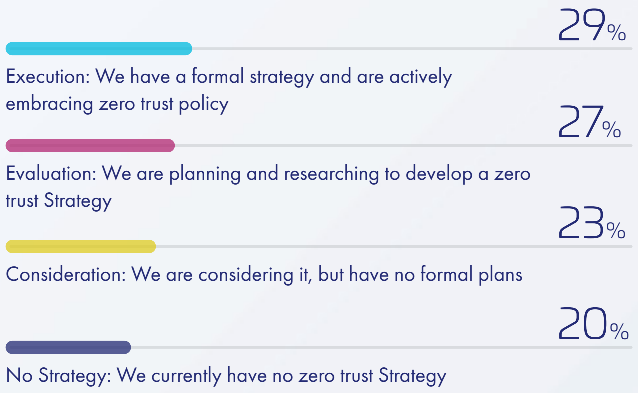
Enterprises are embracing zero trust and investing accordingly. When asked where they are on their zero trust journey, 29% said they are already executing a zero trust strategy, 27% said they are evaluating/planning, 23% said they are considering it and only 20% said they have no plans. That's a notable increase from last year when 52% indicated that they were in execution or evaluation of zero trust. Effective security in a more complex, multicloud world requires a strong authentication and access foundation. Responses also indicate a maturing understanding of the role that modern authentication plays in zero trust. Almost half of the respondents (47%) indicated that it plays a key role in zero trust, an increase from the previous year.

29%

of respondents said they are already executing a zero trust strategy.

Stage of Zero Trust Journey

WHERE ARE YOU ON YOUR ZERO TRUST JOURNEY?



Source: 451 Research's 2022 Cloud Security custom survey

Another area where understanding is maturing is in access management. When asked if an agnostic access management offering (third-party solution versus cloud provider solution) can best protect multicloud environments, 54% said they agree, up from 51% last year. Another small gain, but one that's trending in a direction that can improve enterprises' ability to manage securely in a multicloud environment.

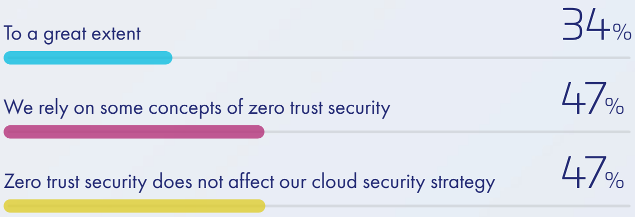
We asked respondents what percentage of employees use modern authentication (more than password only) for access in cloud and SaaS applications, and results were mixed. While enterprises see the value of modern authentication, adoption is still not as widespread as expected, which may indicate an opportunity for providers to drive improved adoption.

Zero Trust (continued)

When asked to what extent zero trust shapes their cloud security policy, 34% said to a great extent, 47% said they rely on some concepts of zero trust, and only 19% said zero trust does not affect their cloud security strategy, down from 24% in 2021. While the differences from last year are not large, they're moving in the right direction.

Extent of Zero Trust's Influence on Cloud Security Strategy

TO WHAT EXTENT DOES ZERO TRUST SECURITY SHAPE YOUR CLOUD SECURITY STRATEGY?

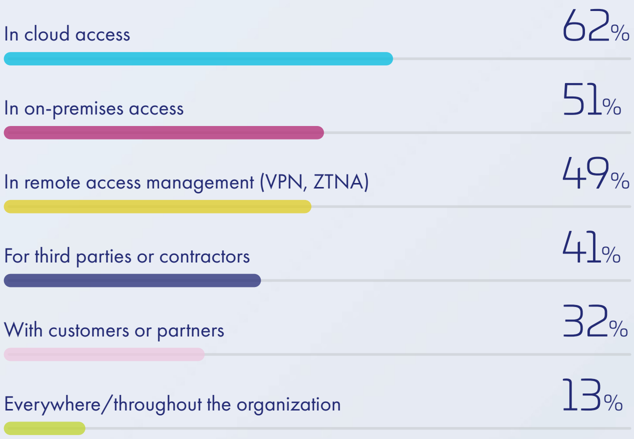


Source: 451 Research's 2022 Cloud Security custom survey

When asked where they plan to apply zero trust, 62% said "in cloud access," which was the leading response. Organizations are maturing in their expectations of where they'll put modern authentication to work: In last year's study, there was a strong preference to apply these technologies in externally facing use cases. The significant growth in the percentage of respondents who expect to apply zero trust to on-premises applications indicates a growing awareness that modern authentication has to be applied across all forms of access.

Venues Where Zero Trust Principles Will Be Used

WHERE DO YOU EXPECT TO USE ZERO TRUST PRINCIPLES?



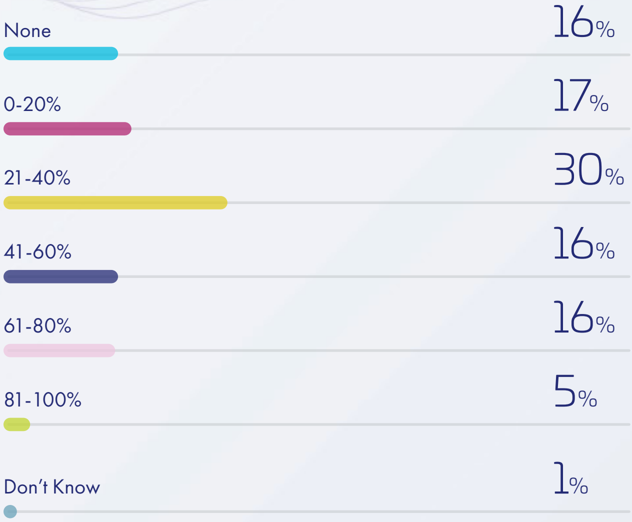
Source: 451 Research's 2022 Cloud Security custom survey

Zero Trust (continued)

Zero trust is an increasingly important security framework for enterprises. Enterprises are embracing zero trust principles, developing strategies to implement zero trust policies, and allocating a budget to invest in zero trust solutions. This is particularly important for cloud access, as the survey responses show. One of the key principles of zero trust is end-to-end encryption of sensitive data, including encryption for data at rest and encryption for data in transit. This strongly suggests that there is an opportunity for enterprises to reduce risk and improve security by investing in platforms that enable effective encryption and authentication management across their organizations. To manage security effectively at a cloud scale and across multicloud environments, organizations have to become much more efficient in the way they operate their security infrastructure.

Percentage of Employees Using Modern Authentication for Cloud/SaaS

WHAT PERCENTAGE OF EMPLOYEES USE MODERN AUTHENTICATION (MORE THAN PASSWORD ONLY) FOR CLOUD APPLICATIONS/SAAS APPLICATIONS?



Source: 451 Research's 2022 Cloud Security custom survey

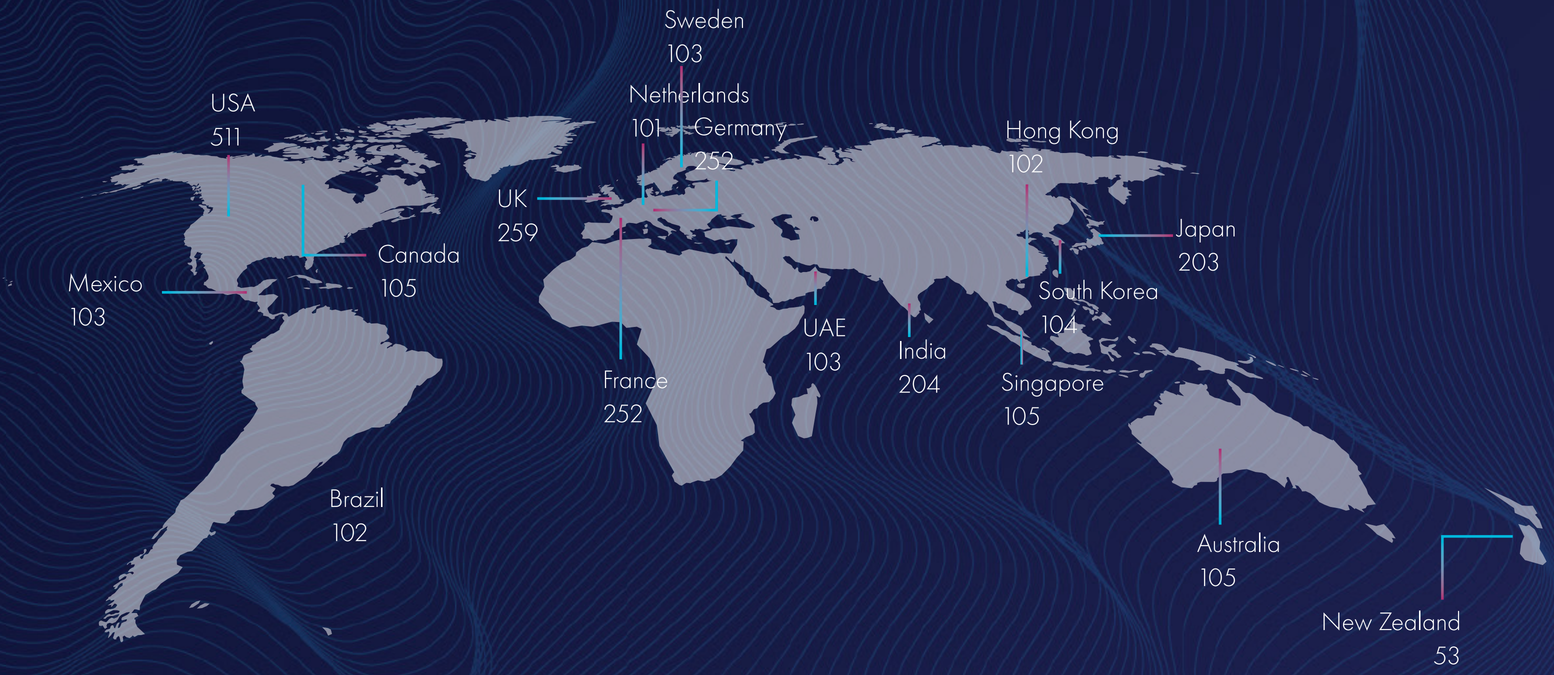
Conclusion

The shift to modern, multicloud infrastructure is in full swing, and organizations have to build security capabilities that will support it. Enterprises are undergoing an accelerated shift to empower an expanding ecosystem of partners, more digital customers and a hybrid workforce, and they see cloud technologies as a solution. Multicloud adoption is soaring, and organizations not only have to expect this to be the normal operating mode, but they also need to be ready for expansion. They must plan accordingly since the complexity of managing multicloud environments creates security challenges. For example, sensitive data is stored across multicloud environments, and data storage and classification are major concerns. Failed audits and cloud data breaches are common, and enterprises are trying to determine what new threats to be concerned about and how they should respond. With increasing multicloud use, security teams need tools and capabilities that can make them more efficient in securing multicloud environments with centralized control of their multicloud security operations. While there has been an improvement in enterprises using encryption to secure sensitive data in the cloud, this remains an area where continuous improvement and consolidation are necessary.

Enterprises see encryption and key management as important security controls in the cloud. They are experiencing challenges with key management solution sprawl and have varying strategies on how to control encryption keys, which may indicate an opportunity to centralize and consolidate solutions. Enterprises are also embracing zero trust, especially for cloud access, and investing accordingly. The combination of these capabilities is helping enterprises to secure complex multicloud environments and enabling cloud transformation to support a remote or hybrid workforce in whatever conditions the future holds for them.

About This Study

As organizations step beyond the urgent actions of the last two years, they're grappling with securing the more complex environments in which they now operate. The global edition of the 2022 Thales Cloud Security Study looked at various aspects of those impacts in a wide-ranging survey of security professionals and executive leadership that touched on issues including accelerated digital transformation, cloud migration, and the complexities of managing security in a multicloud world. The 2022 Thales Cloud Security Study is based on data from a survey of almost 2,800 security professionals and executive leaders. This research was conducted as an observational study and makes no causal claims.



Industry Sector

Manufacturing	157
Retail	154
Technology	127
Financial Services	120
Healthcare	115
Public Sector	109
Consumer Products	107
Computers/ Electronics/Software	106
Engineering	104
Federal Government	103

Revenue

$100 million to $249.9 million	162
$250 million to $499.9 million	802
$500 million to $749.9 million	865
$750 million to $999.9 million	458
$1 billion to $1.49 billion	254
$1.5 billion to $1.99 billion	58
$2 billion or more	168

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