Sensitive Data in the Cloud

cloud security alliance®

Acknowledgments

Lead Authors

Hillary Baron
Josh Buker
Sean Heide
Alex Kaluza
Shamun Mahmud
John Yeoh

Designers

Claire Lehnert

Special Thanks

Kim del Fierro
Bruce Fram
Jenn LeBlanc
Linda Popky

Table of Contents

Acknowledgments 3
Survey Creation and Methodology 5
Goals of the Study 5
Executive Summary 6
Key Finding 1: Most organizations have sensitive data in the cloud 6
Key Finding 2: CSP security controls are effective but organizations still aren't confident in their own ability to protect sensitive data in the cloud 7
Key Finding 3: Over half of organizations have plans to implement data security solutions like homomorphic encryption, and/or confidential computing 8
Cloud Use Overview 9
Security Priorities and Challenges 10
Sensitive Data in the Cloud 12
Current and Future Technologies 14
Familiarity with cloud security technologies 14
Current use and plans to use cloud security technologies 14
Conclusion 15
Demographics 16

Survey Creation and Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA also educates various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

Anjuna commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding sensitive data in the cloud. Anjuna financed the project and co-developed the questionnaire by participating with CSA research analysts. The survey was conducted online by CSA in April 2022 and received 452 responses from IT and security professionals from various organization sizes and locations. CSA's research team performed the data analysis and interpretation for this report.

Goals of the Study

The goal of this survey was to understand the following:

- Cloud use and data security needs
- Security priorities and challenges for the next year
- Approach to hosting sensitive data and workloads in the cloud
- Familiarity with cloud and data security technologies

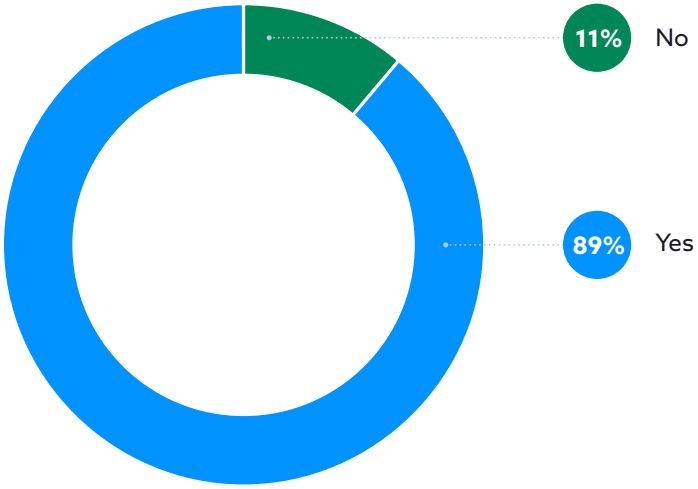
Executive Summary

Key Finding 1:

Most organizations have sensitive data in the cloud

The vast majority of organizations (89%) host sensitive data or workloads in the cloud. Of those organizations, 67% host some sensitive data in the public cloud, and 45% host in the private cloud. With such sensitive data in these cloud environments, it emphasizes the need for proper security of this data with measures like encryption.

Hosting sensitive data in the cloud



About 1 in 10 organizations reported not keeping sensitive data in the cloud. This could cause their organizations to lag behind their counterparts. When asked what was preventing them from doing so, the most common responses were regulatory requirements (23%), concerns about access controls (23%), and concerns about the security of the CSP (21%). While the sample size is too small to draw definitive conclusions from, organizations need to find methods and strategies that address their key concerns and allow them to keep pace with their counterparts.

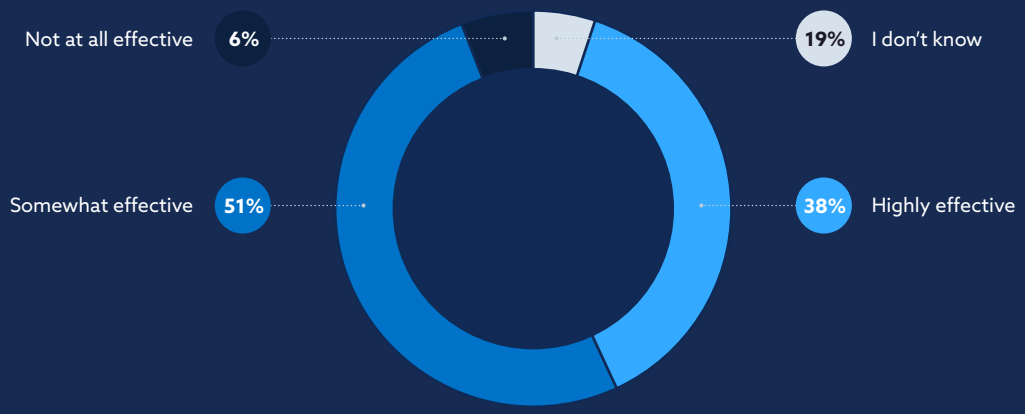
Environments used to host sensitive data

Key Finding 2:

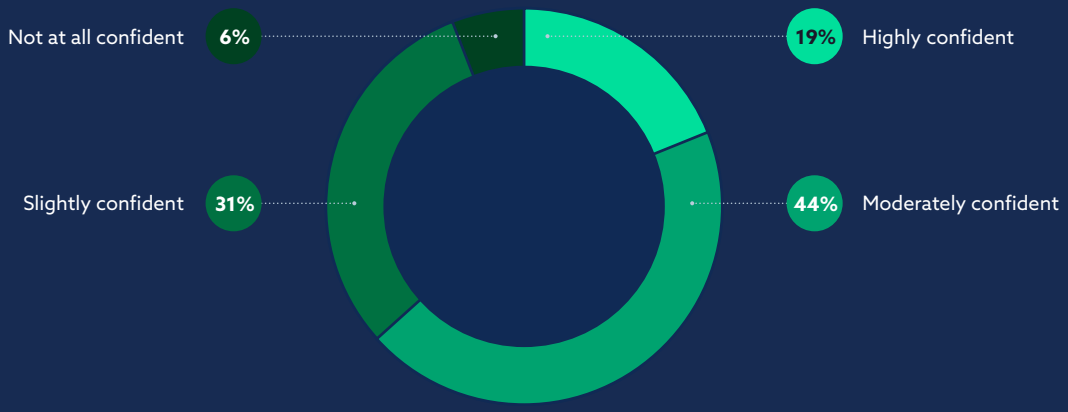
CSP security controls are effective but organizations still aren't confident in their own ability to protect sensitive data in the cloud

Most organizations report that their CSP security controls are highly effective (38%) or somewhat effective (51%). However, organizations feel less confident in their own ability to protect sensitive data in the cloud, slightly (31%) or moderately (44%) confident. Taken together it appears organizations are not as confident in their ability to protect data even though CSPs provide effective security controls. These results could be due to CSPs' greater access to security resources such as knowledgeable staff, budget, and time. All these resources can be dedicated to understanding and addressing the ever-evolving threatscape. But despite organizations' sense of confidence in their CSPs' security controls, they still have reservations about their ability to protect sensitive data in the cloud. Just over a third of organizations were not confident or only slightly confident about their ability to protect sensitive data in a cloud environment and another 44% reported they were only moderately confident. Despite this, 81% of organizations have sensitive data in the cloud. This makes it clear that organizations need to address the protection of the data layer in addition to utilizing their CSP's security controls.

Effectiveness of cloud provider's security controls



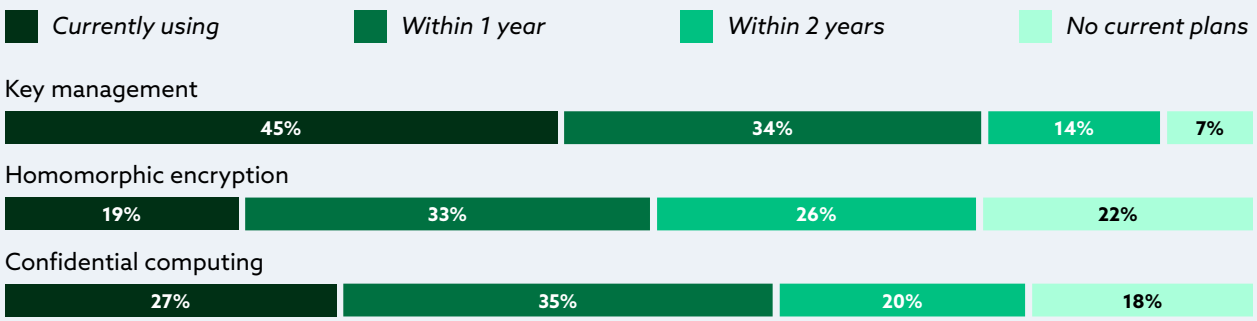
Confidence in organization's ability to protect sensitive data in the cloud



Key Finding 3:

Over half of organizations have plans to implement data security solutions like homomorphic encryption, and/or confidential computing

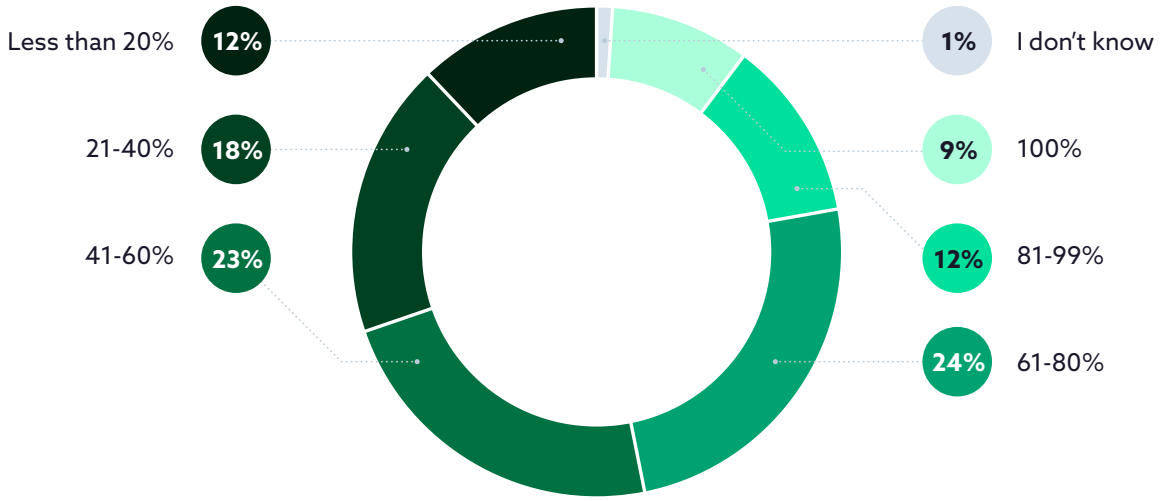
While many organizations may have some current doubts about their ability to protect sensitive data, many organizations plan to address this issue. Over half of organizations plan to implement emerging solutions such as homomorphic encryption (59%), and confidential computing (55%) within the next 1 or 2 years. This trend is quite notable, considering these technologies are newer and indicate a market shift. However, these estimations may be idealized or inflated due to the incorporation of these solutions in other products as well as recent marketing by CSPs about these solutions. Gartner predicts privacy-enhancing computation techniques such as homomorphic encryption and/or confidential computing will be used by 60% of large organizations by 2025. This is the result of organizations' need to process data in the public cloud and share data with multiple parties. All this requires not just securing data-in-use, but also data-at-rest, and data-in-transit.



Cloud Use Overview

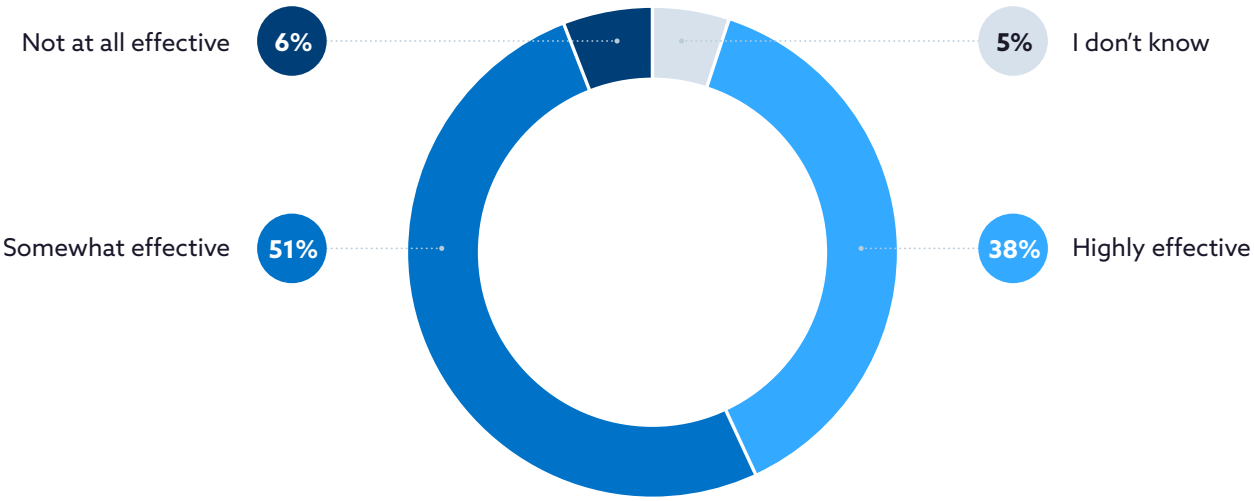
Percentage of workloads in the cloud

Nearly half of the organizations surveyed have between 61-80% (24%) or 41-60% (23%) of their workloads in the cloud. Unsurprisingly over the past few years, organizations have shifted increasingly to the cloud as evidenced by previous surveys[1].



Effectiveness of cloud provider's security controls

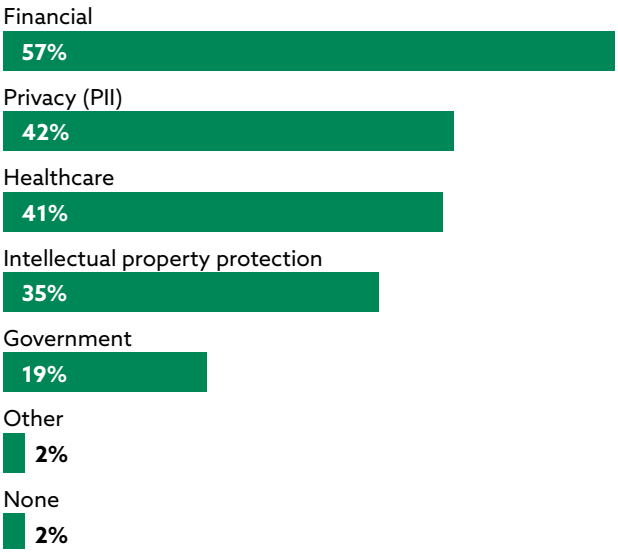
Most organizations find their cloud provider's security controls somewhat effective (51%) or highly effective (38%). Only a tiny percentage (6%) found them to be ineffective.



1 Cloud Security Concerns, Challenges, and Incidents (2020). CSA.

Types of data security compliance requirements

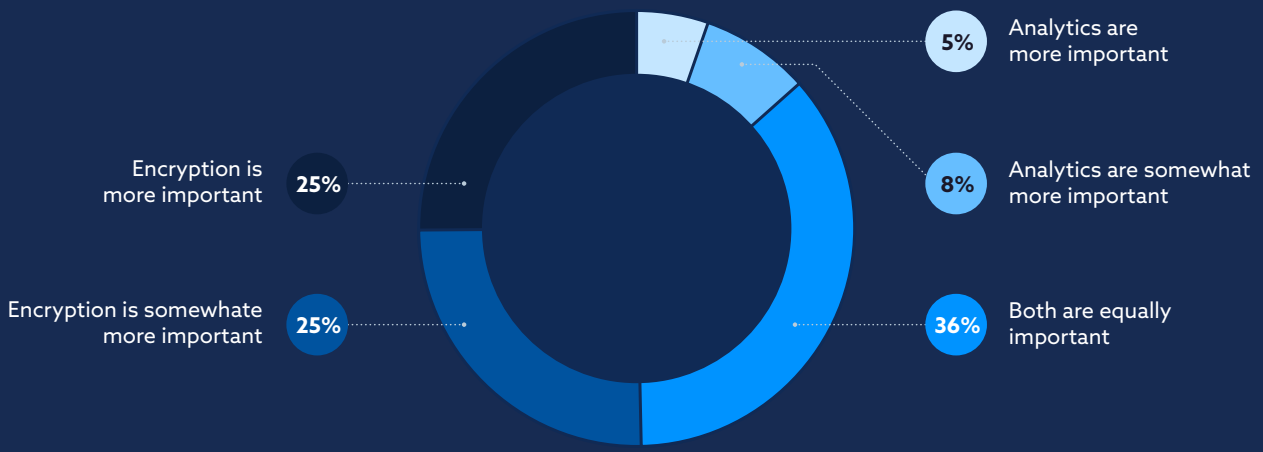
The most common data security requirements organizations need to follow are financial (57%), followed by privacy (42%), and healthcare (41%). Approximately 1/3 follow intellectual property protection requirements, and finally, about 1/5 follow government requirements. Only 2% of respondents reported following no data security requirements.



Security Priorities and Challenges

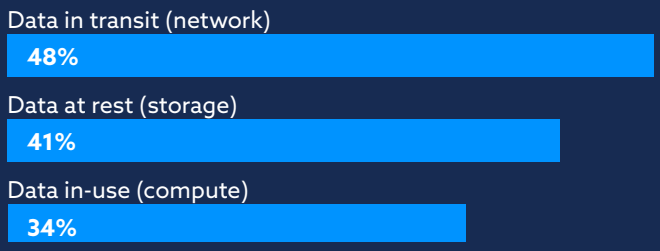
Balancing encryption and analytics

When asked how their organizations balanced encryption and analytics, the most common response was that encryption and analytics are equally important (36%). However, when the scale options favoring encryption are combined, it's clear that organizations value encryption more than analytics (50%). In total, only 13% reported that analytics was more important than encryption.



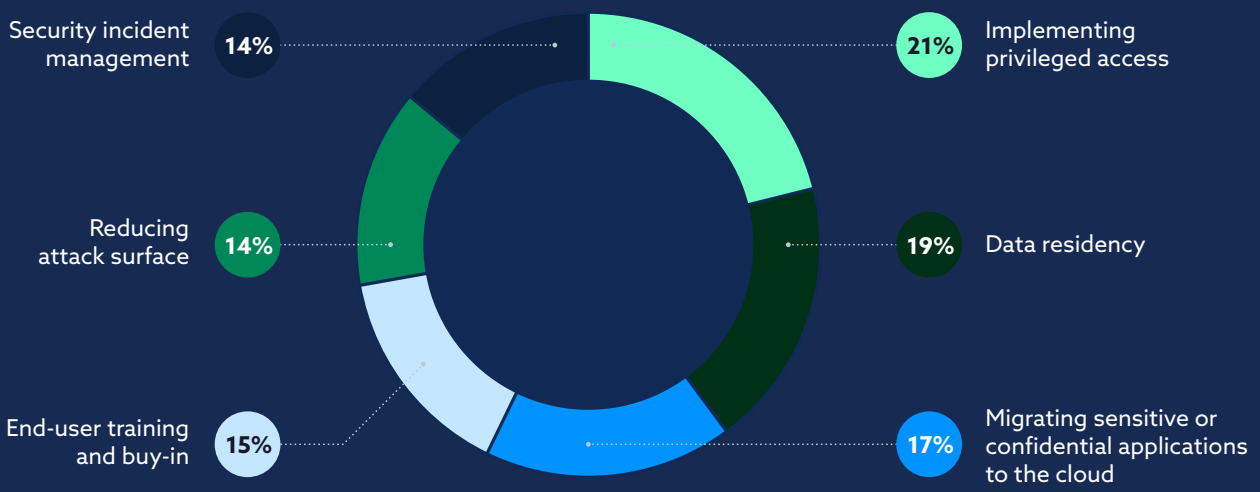
Importance of data encryption

Respondents then rated the importance of three different types of data encryption. About half of organizations report data in transit (network) as highly important (48%). This could be due to the high number of attacks targeting data in this state. Data at rest (storage) and data in use (compute) were rated as "highly important" slightly less frequently at 41% and 34%, respectively.



Most difficult areas to manage for organizations

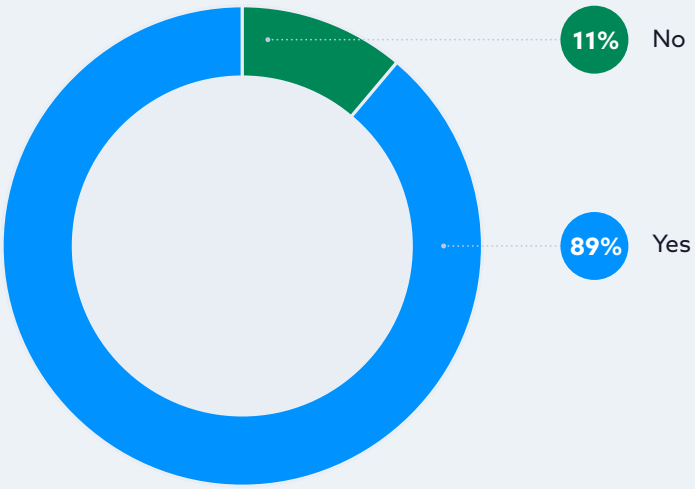
The category most frequently ranked as most difficult was implementing privileged access (21%), followed by data residency (19%), and migrating sensitive or confidential applications to the cloud (17%). The last three received an approximately equal percentage of votes, end-user training and buy-in (15%), reducing attack surface (14%), and security incident management (14%).



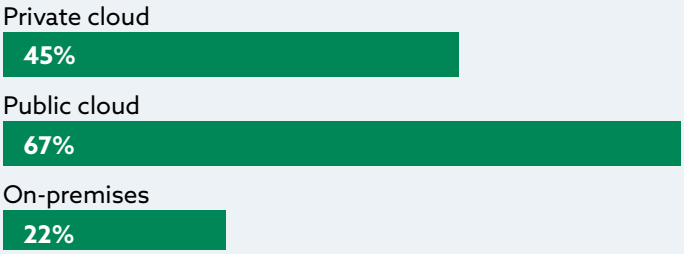
Sensitive Data in the Cloud

Hosting sensitive data in the cloud

Most organizations are hosting sensitive data or workloads in the cloud (89%). Only 11% reported they do not host sensitive data.



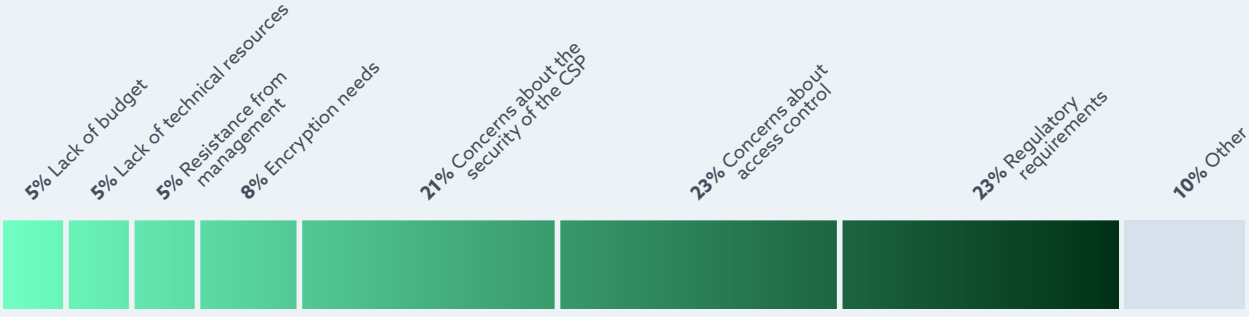
Environments used to host sensitive data



As a follow-up to those who responded that they had sensitive data in the cloud (89% of respondents), respondents reported which environments they use. The most common response was public cloud (67%), private cloud (45%), and on-premises (22%).

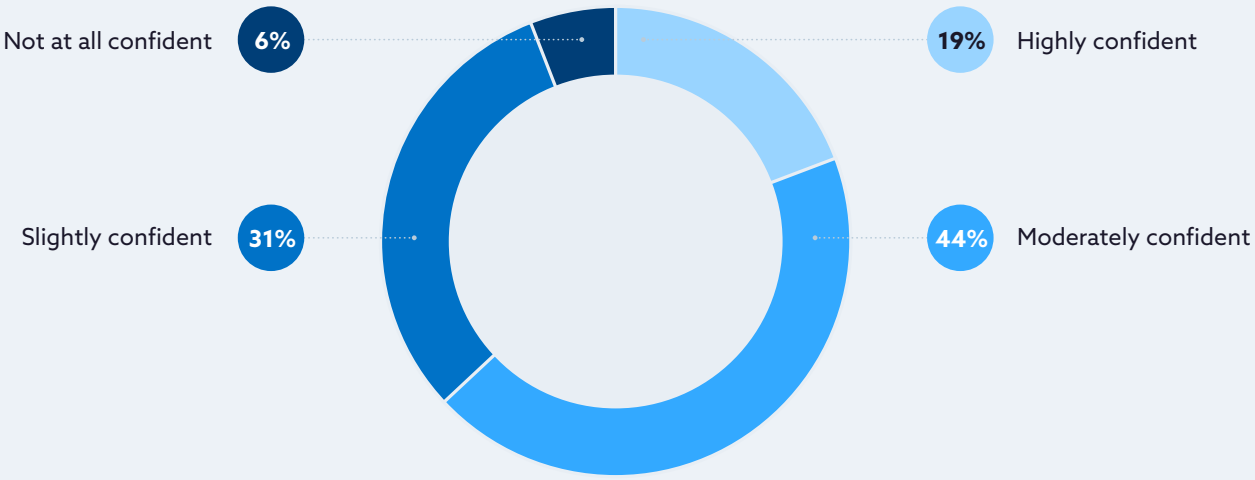
The top barrier preventing organizations from hosting sensitive data in the cloud

A follow-up question was also posed to those who indicated they did not have sensitive data in the cloud (10% of the respondents). The top barriers preventing organizations from hosting sensitive data in the cloud were regulatory requirements (23%), concerns about access control (23%), and concerns about the security of cloud service providers (21%). However, there were so few responses, so no definitive conclusions should be drawn from this data.



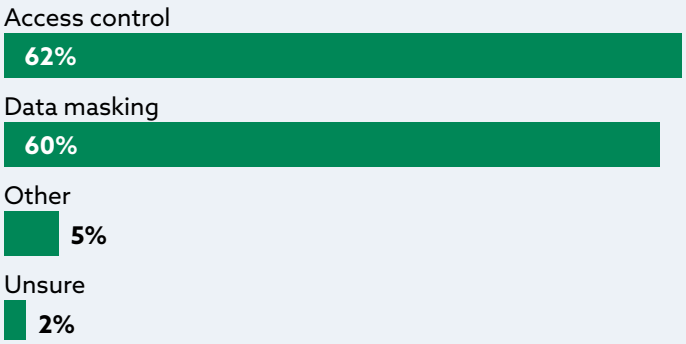
Confidence in an organization's ability to protect sensitive data in the cloud

Organizations are slightly (31%) to moderately confident (44%) in their ability to protect sensitive data in the cloud. Earlier respondents were asked about how effective they believe their cloud provider's security controls are. This yielded more positive results, with 51% indicating somewhat effective and 38% indicating highly effective. Taken together, this seems to suggest that organizations seem to have more apprehension about the portions of cloud security they are responsible for, particularly when it comes to sensitive data.



Methods for secure access to sensitive data

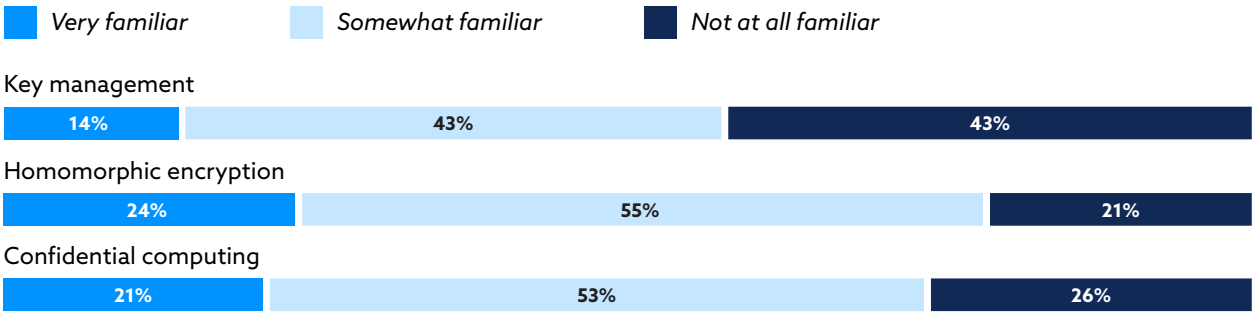
The methods that organizations currently use to ensure only authorized users have access to sensitive data are primarily one or both of the following: access control (62%) and data masking (60%). Many of the responses for those who selected "other" also fit into those two categories, indicating that the rates of use for access control and data masking could be even higher.



Current and Future Technologies

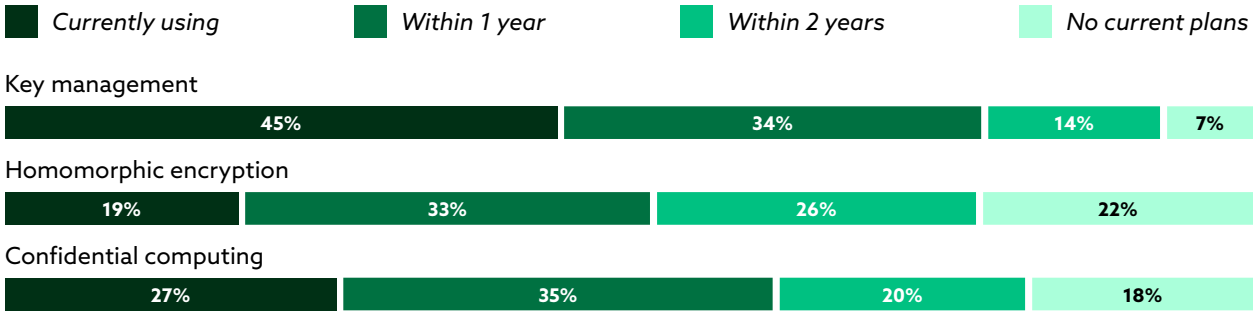
Familiarity with cloud security technologies

Respondents were asked about their familiarity with a few cloud security technologies. Respondents were most familiar with the key management (43% - very familiar). This is unsurprising since it is a more mature technology than the others listed. The remaining two received relatively similar results. Since these remaining technologies are newer than key management, it was surprising to see that roughly a quarter of respondents reported they are very familiar.



Current use and plans to use cloud security technologies

The familiarity ratings appear to correspond with the percentage of respondents currently using each of the respective technologies: key management - 45%, homomorphic encryption - 19%, confidential computing - 27%. It also appears that over half of organizations plan to implement homomorphic encryption, and confidential computing within the next 1 or 2 years. However, in an article from Gartner, the author notes that homomorphic encryption is still likely 3 - 6 years out from coming to market. Regardless of the exact timeline for the market, it's clear that the industry is excited about these technologies and their potential.



Conclusion

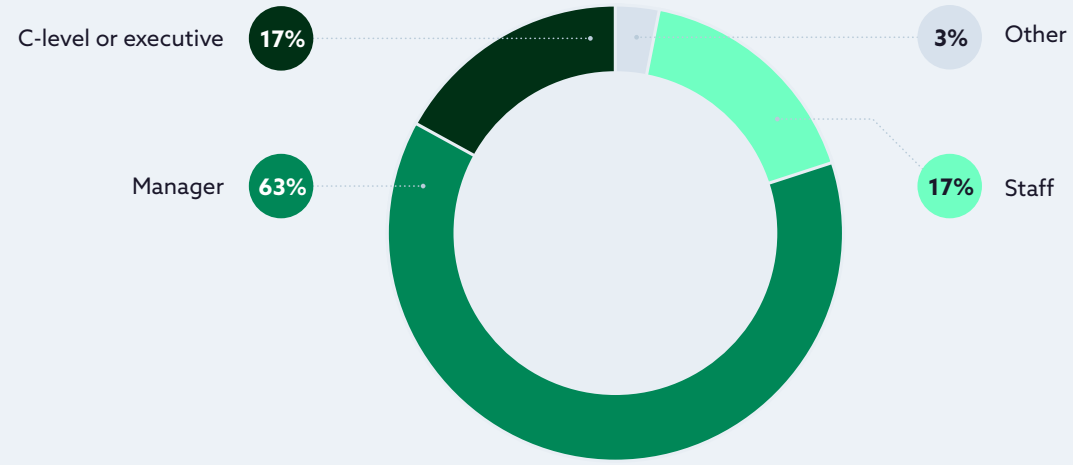
The vast majority of organizations host sensitive data or workloads in the cloud. This can in part be attributed to organizations' confidence in cloud security. More specifically the effectiveness of the security controls offered by CSPs, have at least in part encouraged organizations to store their sensitive data in public and private cloud environments at greater rates than on-premises. Taken together it appears that many organizations have overcome any initial apprehension around the cloud and the initially perceived insufficiencies of its security. Major CSPs for some time now have had greater access to security resources such as knowledgeable staff, budget, and time to dedicate solely to improving security and addressing changes in the threatscape.

Despite this confidence in cloud security and CSPs security controls, organizations still have reservations about their own ability to protect their sensitive data in the cloud. This gap between the perceived effectiveness of CSP security controls and confidence in organizations' abilities to protect sensitive data in the cloud could be due to the difference in security resources when comparing CSP and cloud users. Equally, it points to organizations' need for additional security measures beyond CSPs' built-in security features. This is further evidenced by the clear interest in implementing additional emerging security solutions such as homomorphic encryption, and confidential computing. In fact, several larger companies and CSPs have promoted the use of these technologies in recent months which has likely spurred on this trend and interest. Regardless of the reason, it has produced a major shift in the market which should not go unnoticed.

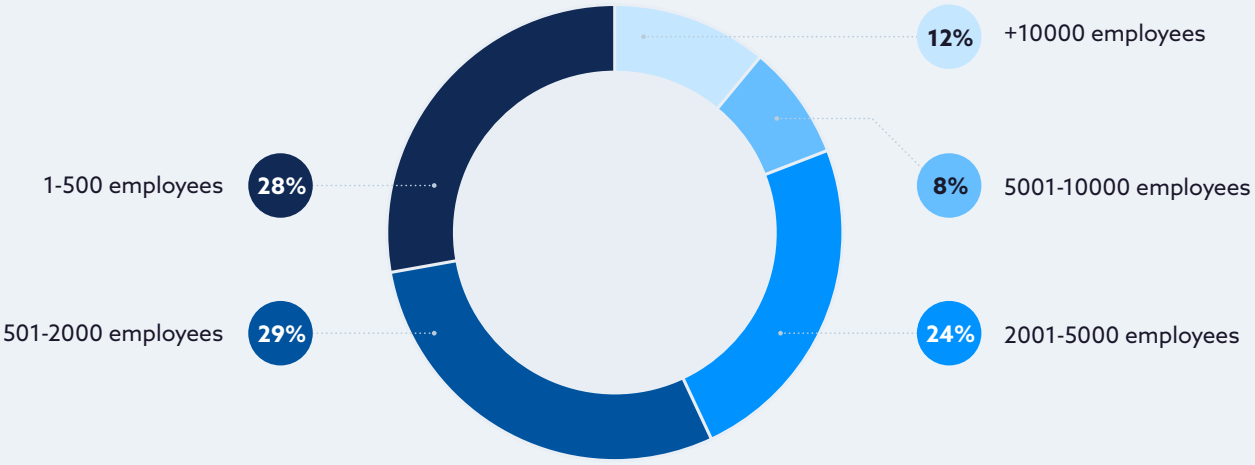
Demographics

This survey was conducted in April 2022 and gathered 452 responses from IT and security professionals from various organization sizes, industries, locations, and roles.

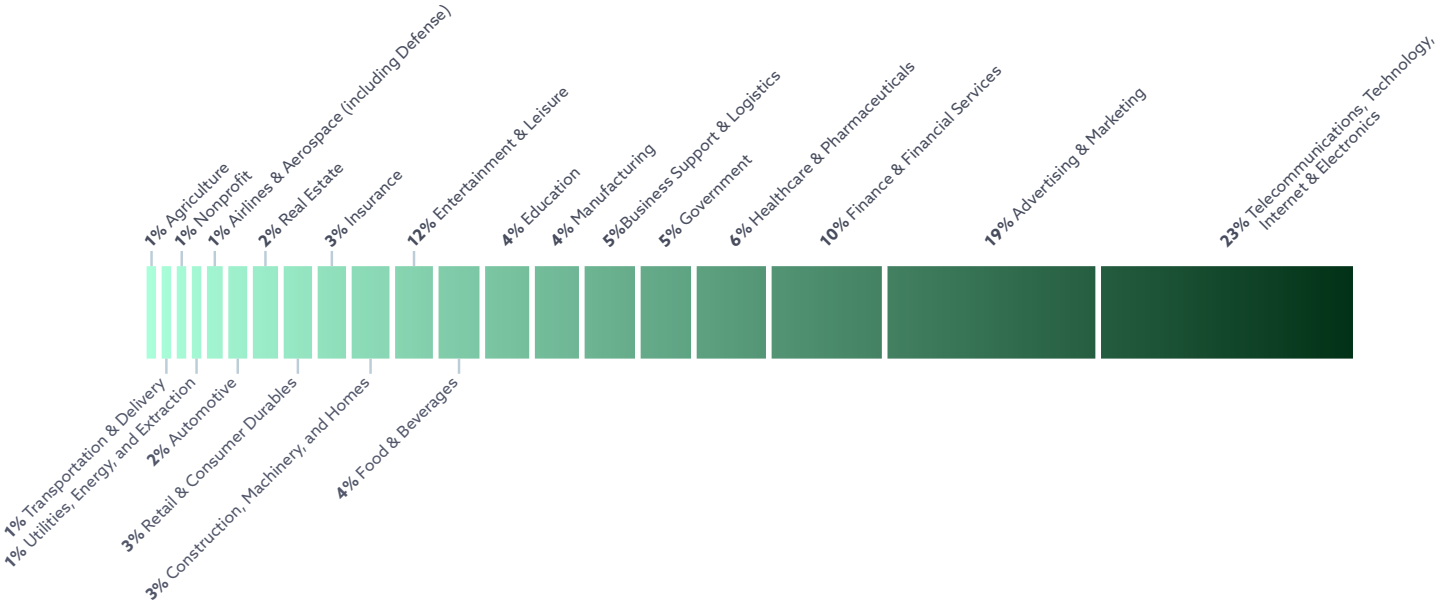
Which of these best describes your current job level?



What size is your organization?



Which of the following best describes the principal industry of your organization?



What region of the world are you located in?