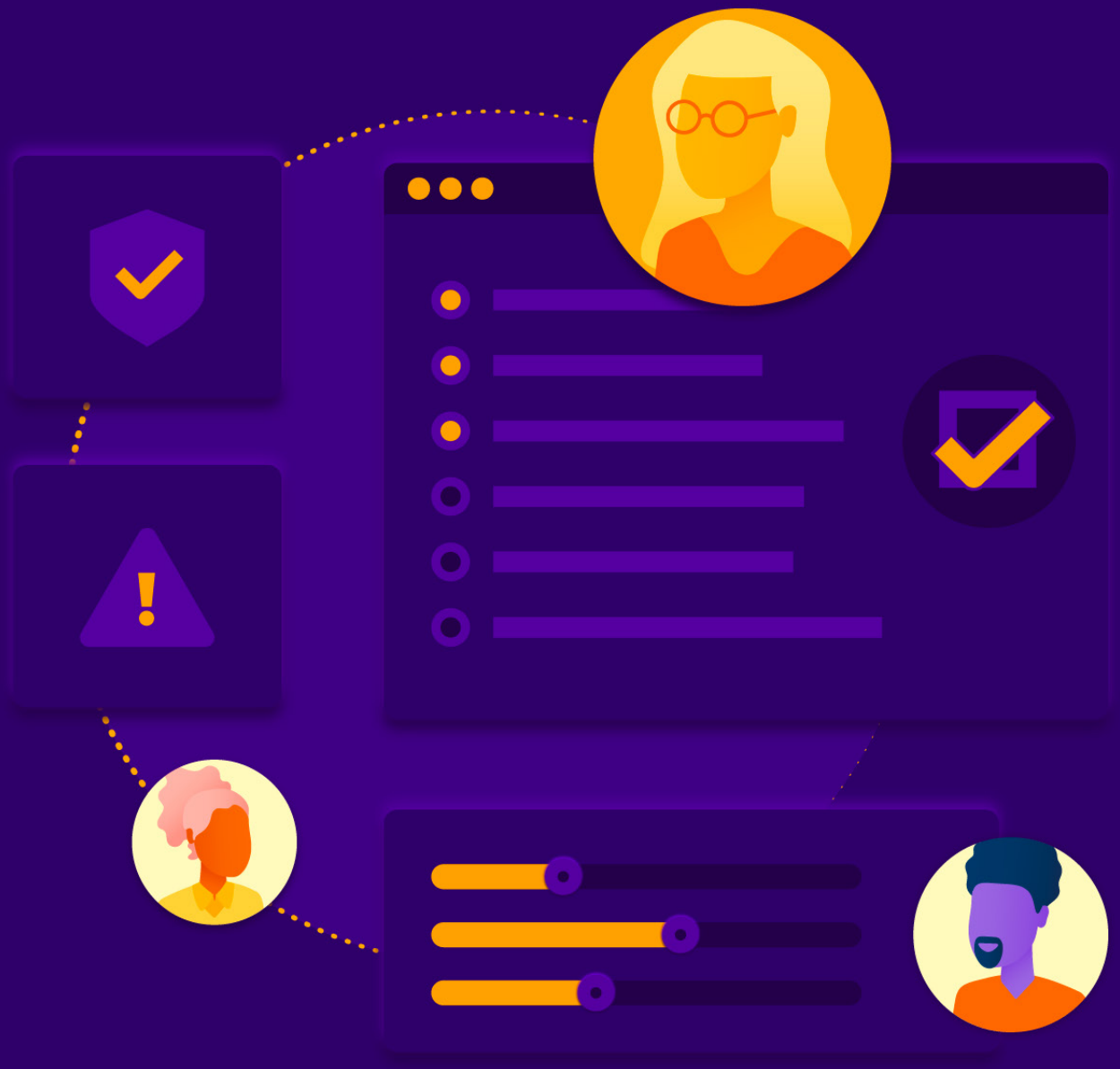
Understanding Cloud Data Security and Priorities in 2022



cloud security alliance®

© 2022 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Lead Author

Hillary Baron

Contributors

Josh Buker
Sean Heide
Alex Kaluza
John Yeoh

Designer

Claire Lehnert

Special Thanks

Neil Patel

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Table of Contents

© Copyright 2022, Cloud Security Alliance. All rights reserved.

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 cybersecurity 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.

BigID commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding data security in the cloud. BigID financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in July 2022 and received 1663 responses from IT and security professionals from organizations of various sizes and locations. CSA's research analysts performed the data analysis and interpretation for this report.

Goals of the Study

The goals of this study were to understand the following:

- Approaches to cloud data security
- Priorities for cloud data security
- The current state of sensitive and dark data
- Concerns about data breaches
- Difficulties of regulatory compliance

© Copyright 2022, Cloud Security Alliance. All rights reserved.

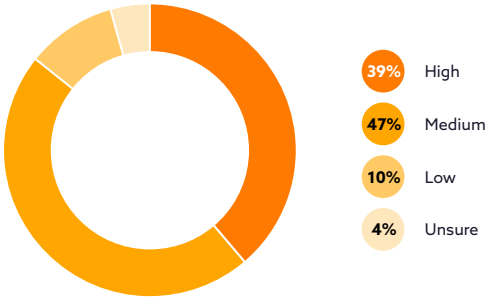
Key Findings

Key Finding 1:

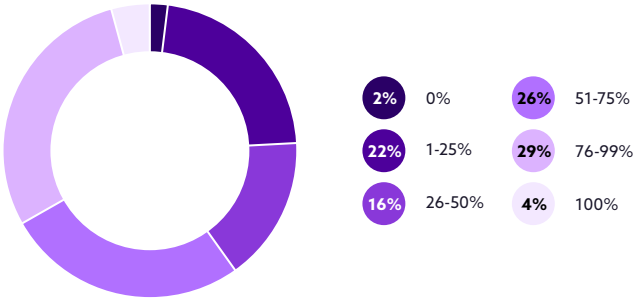
Organizations are struggling with securing and tracking sensitive data in the cloud

In general, organizations are lacking confidence in their ability to secure data in the cloud, with 39% reporting high confidence levels. Over half of the organizations (57%) report medium to low levels of confidence. This lack of confidence becomes even more evident when discussing sensitive data. Forty percent of organizations indicate that 50% or less of their sensitive data in the cloud has sufficient security. Only 4% report sufficient security for 100% of their data in the cloud. This finding suggests that organizations may generally have some confidence in their ability to secure data, but are struggling when it comes to sensitive data.

Level of confidence in organization's ability to secure data in the cloud



In your opinion, what percentage of your organization's sensitive data in the cloud is sufficiently secured?



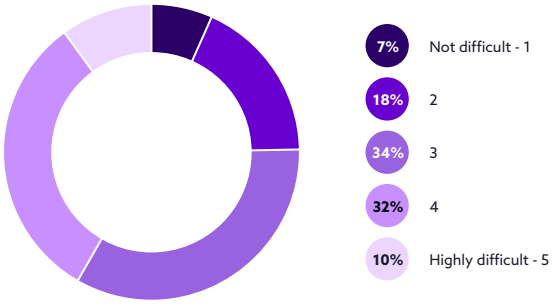
In addition to struggling with securing sensitive data, organizations are struggling with tracking data in the cloud. Over a quarter of organizations aren't tracking regulated data, nearly a third aren't tracking confidential or internal data, and 45% aren't tracking unclassified data. This suggests that organizations' current methods of classifying data aren't sufficient for their needs.

Regarding SaaS platforms, 76% of organizations rate tracking data as moderately to highly difficult. Only 7% of organizations report that tracking data isn't an issue at all. The difficulty of data tracking is particularly concerning when considering the amount of sensitive data that organizations have in SaaS platforms.

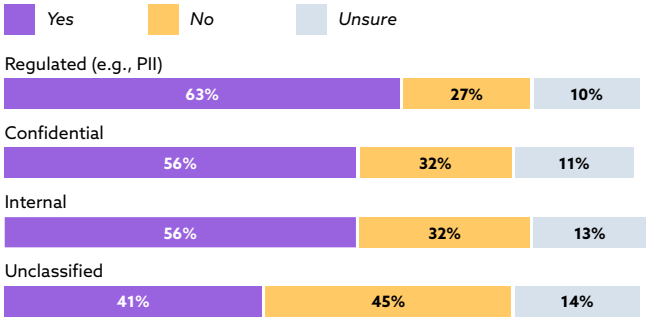
These data tracking struggles may tie back to the lack of use of data classification and discovery mechanisms, with only 9% of organizations using these features. This lack of use may be tied to lack of capabilities (52%) and lack of cross-platform support (41%), as these were cited as the reasons for selecting third-party cloud data security vendors. Regardless, use of data classification and discovery mechanisms would allow organizations to better track their data.

© Copyright 2022, Cloud Security Alliance. All rights reserved.

Level of difficulty tracking data in SaaS platforms poses



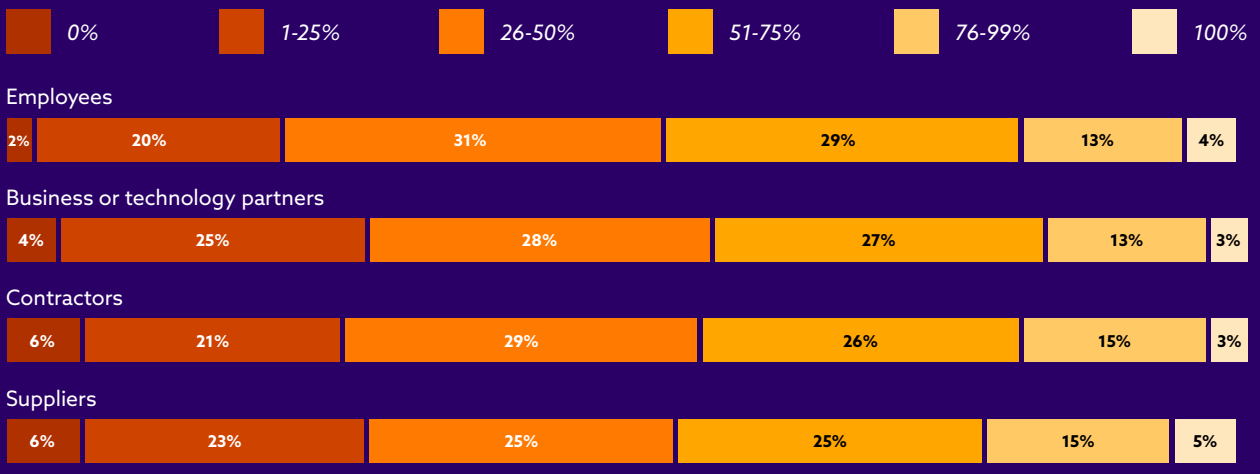
Data tracked in the cloud



Key Finding 2:

Third parties and suppliers have similar access to sensitive data compared to employees

Organizations appear to give nearly identical levels of access to sensitive data in their organization to employees, contractors, partners, and suppliers. This finding indicates that third parties and suppliers may have too much access to organizations' sensitive data, particularly in light of the recent newsworthy supply chain attacks. In a recent CSA survey report on cloud and web attacks, third parties, contractors, and partners were found to be the most commonly targeted group in attacks (58%). In addition, according to a study by Colorado State University, 2/3 of breaches are the result of vulnerabilities from suppliers and third parties. Considering the enormity of these implications, organizations need to understand who has access to their sensitive data and also lock down access, in particular to third parties.

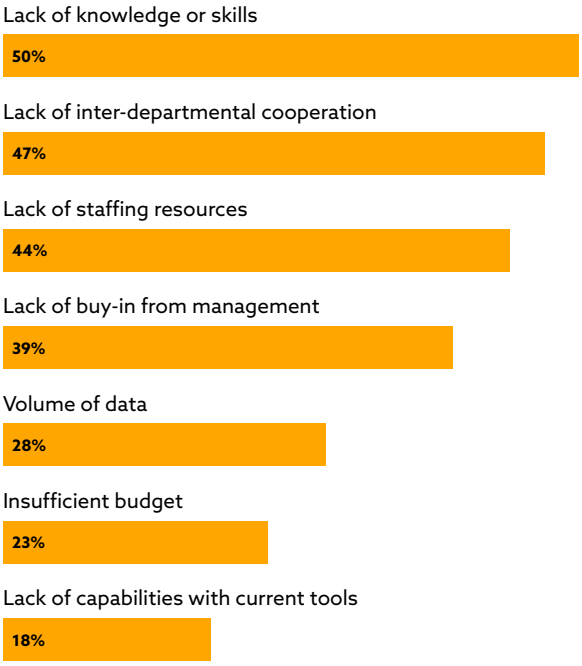


© Copyright 2022, Cloud Security Alliance. All rights reserved.

Key Finding 3:

Dark data issues stem from staffing issues and interdepartmental conflict

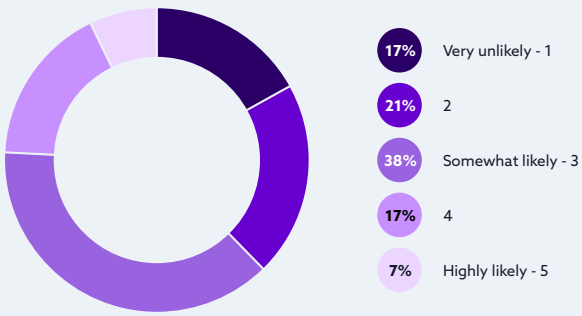
Over half of organizations (79%) have moderate to high levels of concern around the proliferation of dark data in their organization, but are unsure about how to approach the issue.
The top three barriers for organizations capturing dark data are related to staffing issues: lack of skills/knowledge (50%), lack of interdepartmental cooperation (47%), and lack of staff resources (44%). Organizations will need to dedicate themselves to educating their staff and prioritizing technologies that can support staffing gaps. In addition, organizations need to define a unified approach to tackling dark data to avoid competing priorities in siloed departments. Establishing a single source such as a data inventory can provide disparate departments with the base knowledge they need to work more cohesively.



Key Finding 4:

The majority of security professionals believe their enterprise will experience a data breach in the next year

Sixty-two percent of organizations report that they are somewhat to highly likely to experience a cloud data breach in the next year. Given the high number of organizations who report experiencing a cloud data breach in the past 12 months, it makes sense that there is more concern about an attempted breach in the upcoming 12 months. For organizations that hadn't experienced a breach in the past 12 months, 22% indicated that a breach in the next 12 months is very unlikely. Organizations that had experienced a breach believe a data breach is more likely to happen, with only 8% reporting a data breach in the next 12 months to be very unlikely. One key step will be for organizations to lock down third-party access to sensitive data. Organizations also need to continue to prioritize cross-platform support for their complex cloud environments (e.g., multi-cloud and hybrid cloud) to ensure security across all environments.

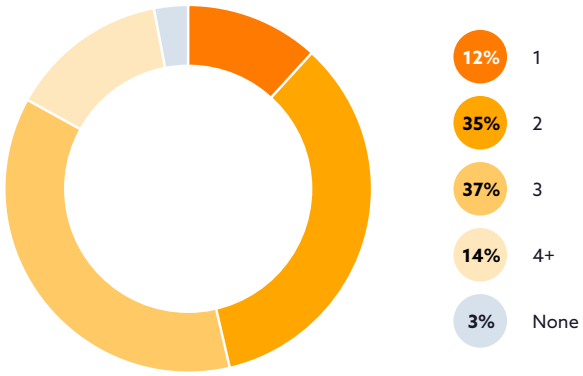


© Copyright 2022, Cloud Security Alliance. All rights reserved.

Overview

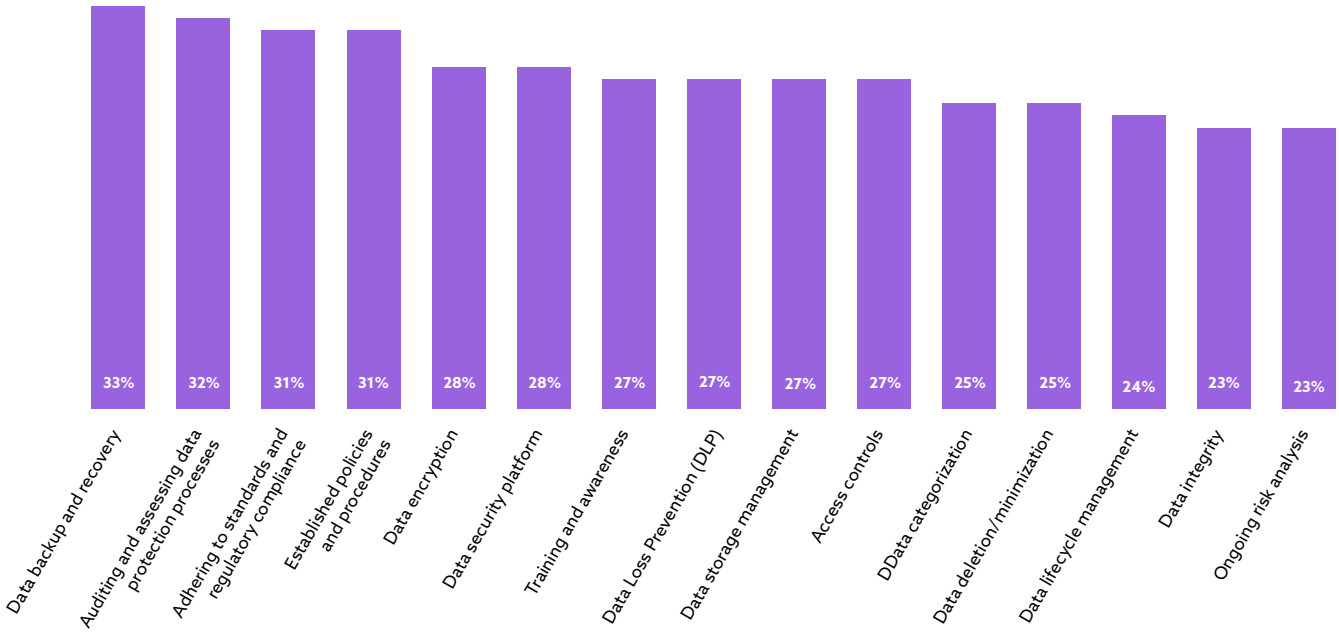
Number of IaaS and PaaS platforms used for data storage

The vast majority of organizations utilize multiple cloud platforms to store their data (86%). Most organizations utilize 2 (35%) or 3 (37%) cloud IaaS and PaaS platforms to store data. Only 12% report utilizing 1 platform.



Data protection strategy

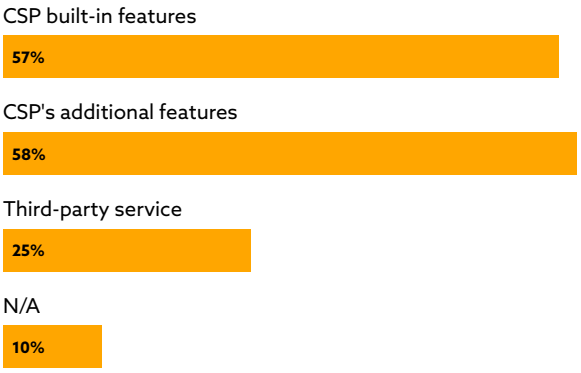
Organizations utilize between 4 and 5 different components for their data protection strategy. Some of the most common components include data backup and recovery (33%), auditing and assessing data protection processes (32%), adhering to standards and regulatory compliance (31%), and establishing policies and procedures (31%). Some of the less commonly used components include triaging alerts (18%), zero trust (19%), and data sovereignty (19%). It seems that despite movement toward zero trust, data protection has yet to be integrated fully for many organizations.

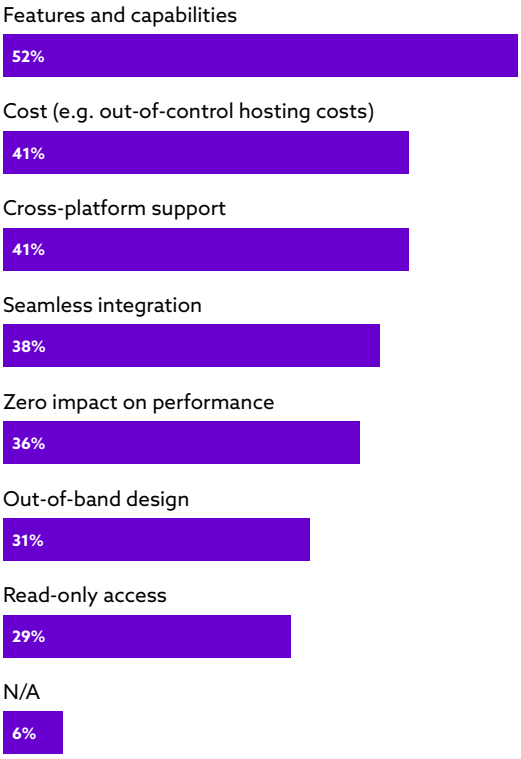


© Copyright 2022, Cloud Security Alliance. All rights reserved.

Type of service used for cloud data security

Organizations primarily rely on cloud service provider features, whether that be built-in (57%) or add-on features (58%). Only a quarter of organizations report using third-party services.





Drivers for selecting third-party cloud data security vendors

For organizations utilizing a third-party service for cloud data security, the top three reasons they selected their vendor were features and capabilities (52%), cost (41%) and cross-platform support (41%). This suggests that organizations selecting third-party services are looking for something more cost effective or additional features that CSPs are not providing. In addition, the use of multi-cloud and hybrid environments has organizations focused on cross-platform support.

© Copyright 2022, Cloud Security Alliance. All rights reserved.

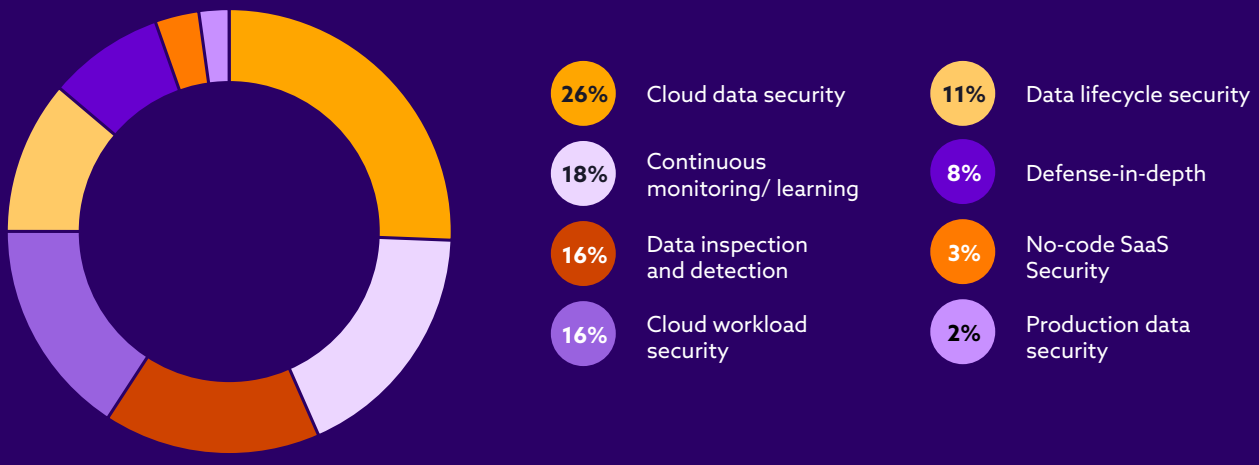
Data Security Priorities

Data security features organizations use

The most common data security features organizations use are continuous monitoring/ learning (48%), cloud workload security (42%), cloud data security (42%), and data inspection and detection (41%). Interestingly, the least utilized data security feature is data discovery and classification. The low rates of data discovery and classification use could be due to the fact that these types of features are well integrated in the continuous monitoring/learning function. Alternatively, these low rates could be because organizations assume discovery and classification is part of the data security lifecycle. However, if use is this low, it could be a contributing factor to the issue of dark data. Organizations need to utilize data discovery and classification tools to properly understand the data they have and how to protect it. Without taking this step, data will continue to remain dark.

High-priority data security product features

Of the data security features organizations use, the highest priority features are cloud data security (26%), continuous monitoring/learning (18%), data inspection and detection (16%), and cloud workload security (16%). These results follow a similar pattern to the data security features organizations use in general.

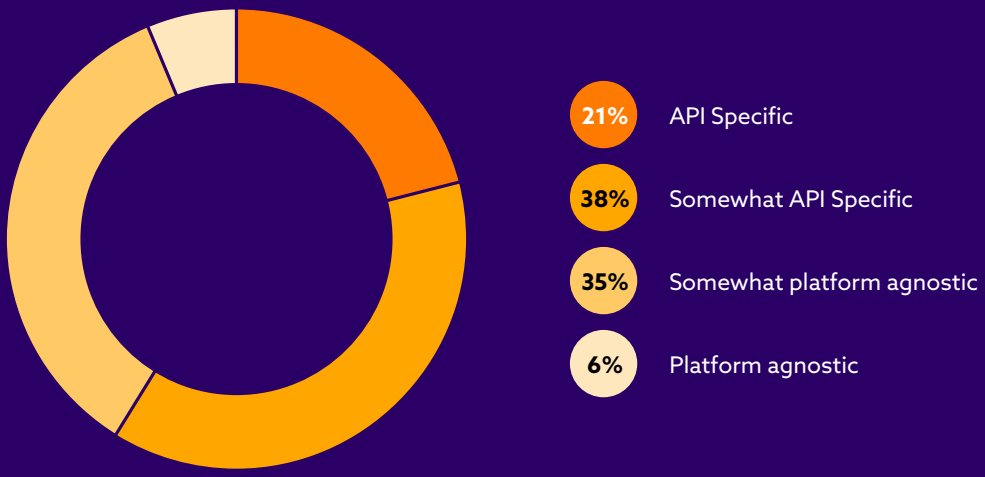


© Copyright 2022, Cloud Security Alliance. All rights reserved.

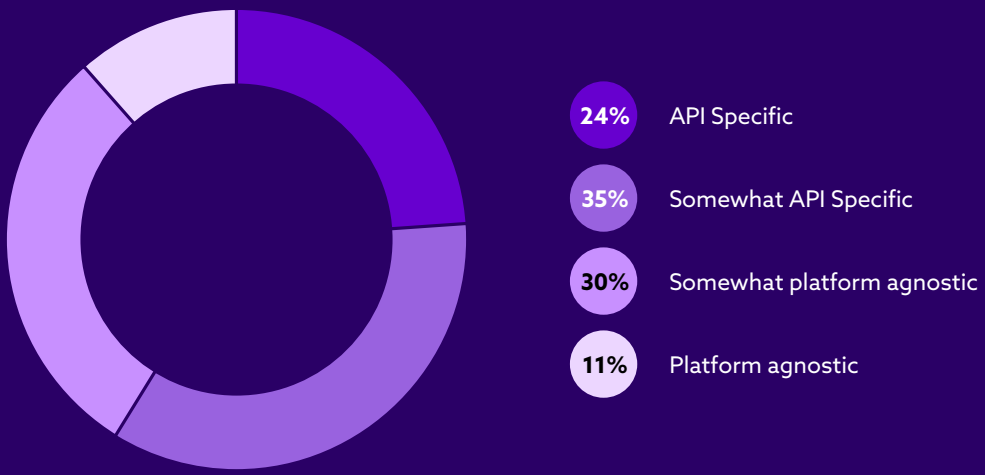
Current and ideal approach to data interoperability

In general, organizations trend slightly more toward an API-specific approach (59%) to data interoperability rather than platform agnostic (41%). It appears that organizations are content with their approach. When asked about the ideal approach to data interoperability, the responses are largely the same, with organizations leaning toward an API-specific approach (59%) rather than platform agnostic (41%). Organizations need tools that can easily integrate with their current solutions and that utilize open APIs.

Current Approach to Data Interopability



Organization's Ideal Approach to Data Interoperability



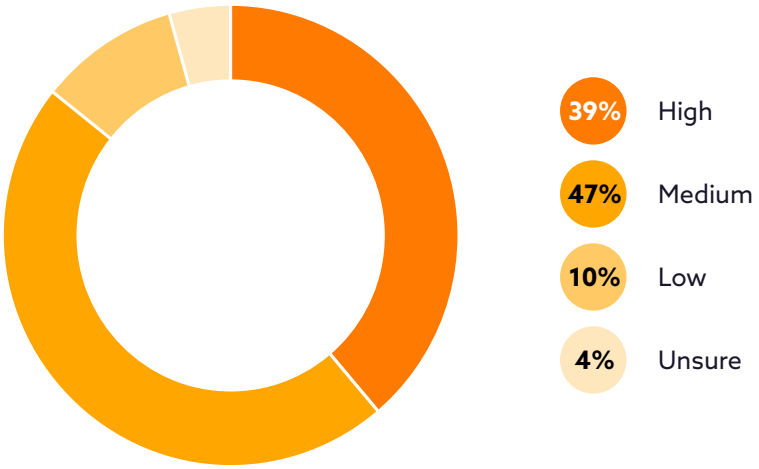
© Copyright 2022, Cloud Security Alliance. All rights reserved.

Sensitive Data

Confidence in ability to secure data in the cloud

Organizations are confident in their ability to protect data in the cloud, with 39% indicating a high level of confidence and 47% indicating a medium level of confidence. While these results may seem encouraging, ideally the majority of organizations should feel highly confident in their organizations' abilities. The fact that most fall in the medium confidence category indicates there is significant room for improvement with organizations' data security strategies in the cloud.

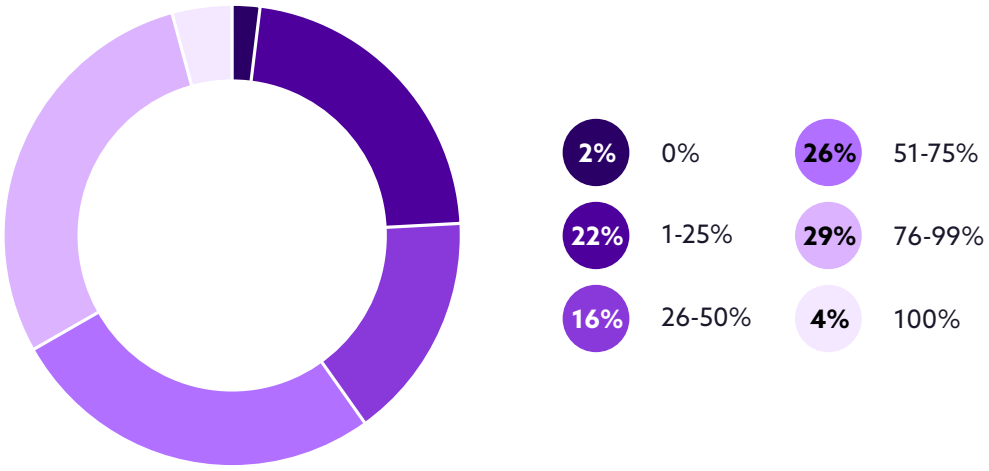
It should be noted that confidence level is influenced by recent events and the respondent's position in the company. Confidence decreases for organizations that have had a data breach in the past year. Out of the respondents that marked they had high confidence in their ability to protect data in the cloud, 36% had been breached in the last year and 40% had not been breached. Organizations that haven't had a recent breach may be overconfident in their ability to secure data in the cloud until they experience a breach for themselves. Additionally, managers(40%) select high at greater rates than their exec (35%) and staff (34%) counterparts.



© Copyright 2022, Cloud Security Alliance. All rights reserved.

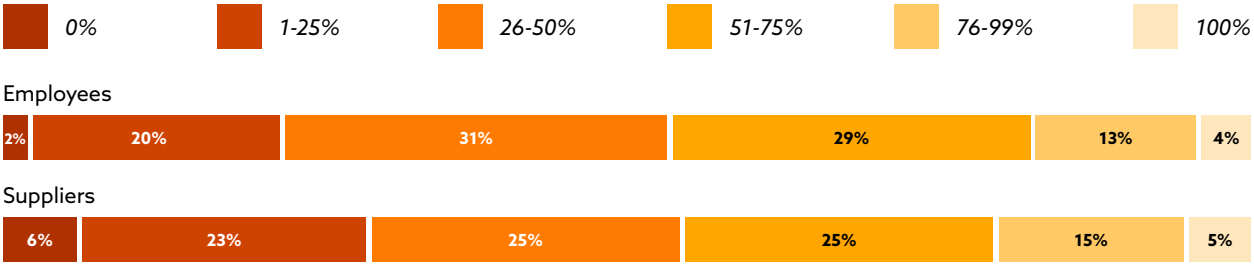
Percentage of sensitive data in the cloud with sufficient security

Forty percent of organizations indicate that 50% or less of their sensitive data in the cloud has sufficient security. Only 4% report sufficient security for 100% of their data in the cloud. This means that 96% of organizations have insufficient security for at least some of their sensitive data. These numbers are quite shocking. This could be contributing to the lack of confidence in organizations' abilities to secure data in the cloud and may even indicate that organizations have an overinflated sense of their ability to secure data.



Percentage of users with access to sensitive data

Organizations appear to give employees and suppliers nearly identical levels of access to sensitive data. This seems to indicate that third parties and suppliers may have too much access to organizations' sensitive data, particularly in light of the recent newsworthy supply chain attacks. Organizations should be keenly aware of who has access and what they have access to in order to prevent unintentional exposure.

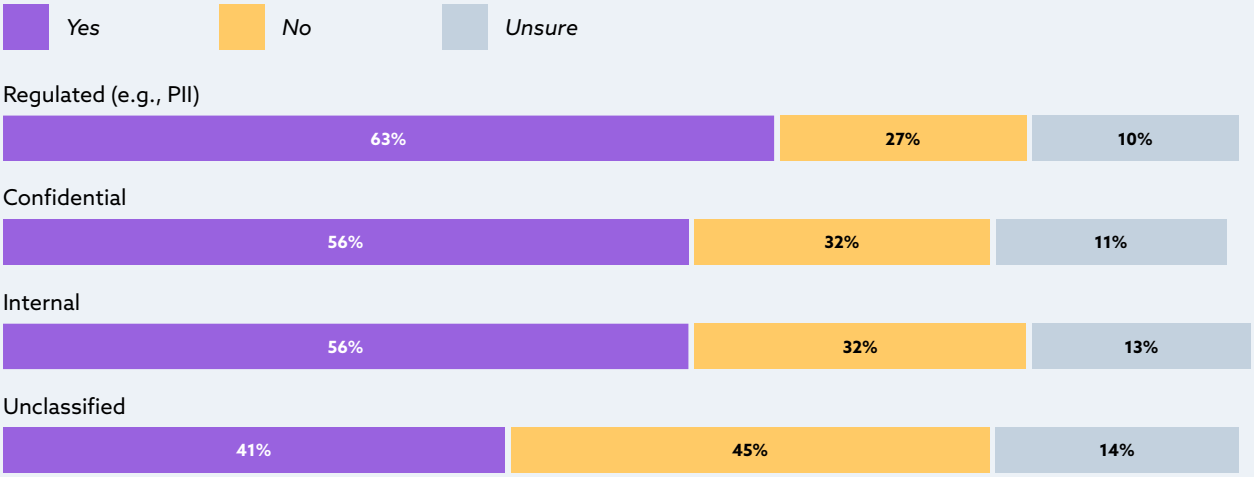


© Copyright 2022, Cloud Security Alliance. All rights reserved.

Dark Data

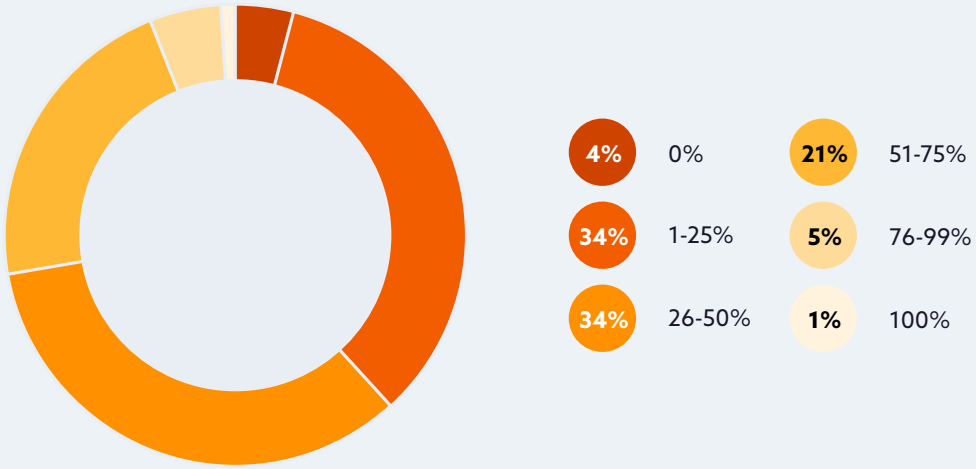
Tracking data in the cloud

Organizations are struggling with tracking data in the cloud. Over a quarter of organizations aren't tracking regulated data, nearly a third aren't tracking confidential or internal data, and 45% aren't tracking unclassified data. This suggests that organizations' current methods of classifying data aren't sufficient for their needs.



Percentage of dark data

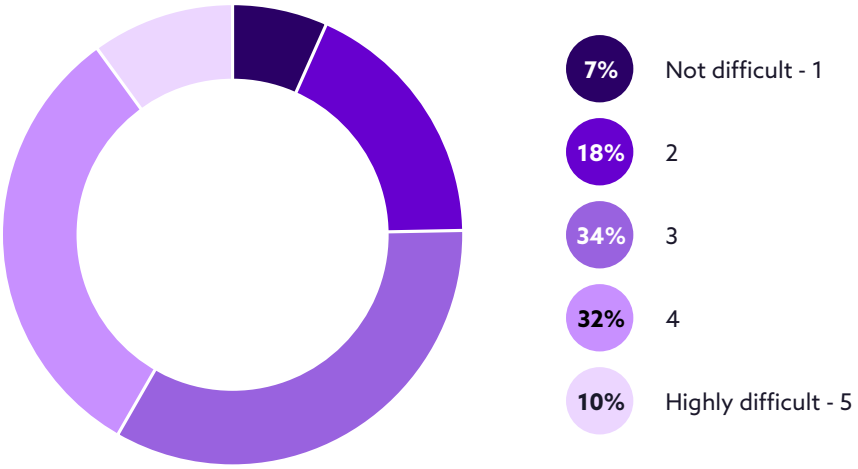
Admittedly, it is difficult to estimate the amount of dark data organizations have without proper tooling. However, when asked to estimate, over a quarter of security and tech professionals (27%) believe that 51% or more of their organization's data is dark data. While these numbers are alarmingly high, it's likely that the actual numbers are even higher. It seems that security professionals are aware that there is an issue, but still struggle to understand how great the issue is. This is particularly problematic because organizations aren't able to protect data if they don't have proper visibility into what they have or its location. Without getting a handle on the issue of dark data, organizations can't properly understand their data risk posture or assess their attack surface. This can only lead to vulnerabilities and security gaps.



© Copyright 2022, Cloud Security Alliance. All rights reserved.

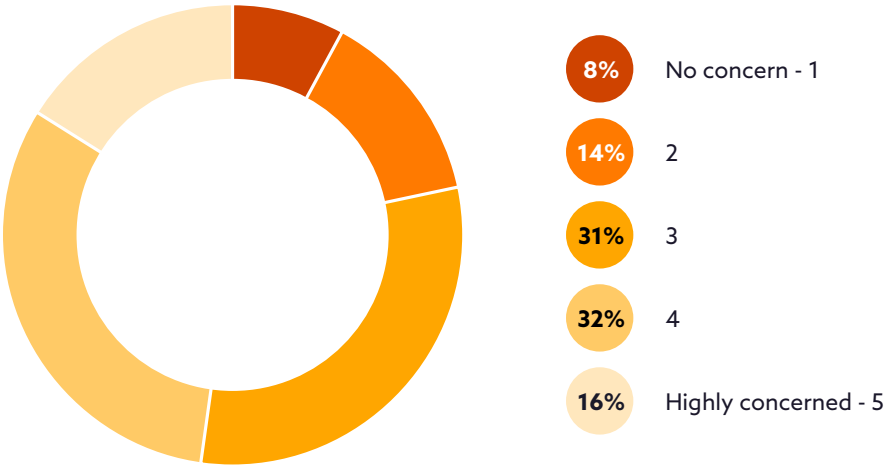
Level of difficulty tracking data in SaaS platforms

Organizations are struggling with tracking data in SaaS platforms. Seventy-six percent rate it as moderate to highly difficult for their organization. Only 7% report that they have no difficulties at all. These struggles could be due to lack of visibility, the volume of data coming in, or even a lack of proper tooling. Many organizations (91%) report not using data classification or discovery tools, which may be contributing to the problem. This could be due to a lack of capabilities in current tools (e.g., they are unable to provide organizations with proper visibility into sensitive data within these SaaS applications). Organizations need to continue to emphasize cross-platform support for their third-party data security vendors to ensure that coverage is extended across their data ecosystem, especially SaaS platforms.



Level of concern about dark data proliferation

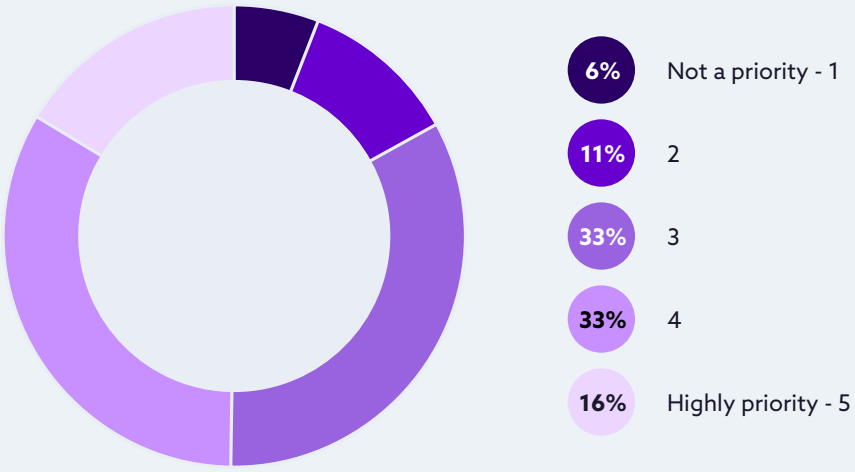
Nearly half of organizations (48%) have high levels of concern around the proliferation of dark data in their organization. Organizations are unclear about how to get a handle on the issue, given the lack of tracking currently occurring and the difficulty of tracking data in SaaS platforms. It's clear that organizations are struggling with asset management and lack complete data visibility and control.



© Copyright 2022, Cloud Security Alliance. All rights reserved.

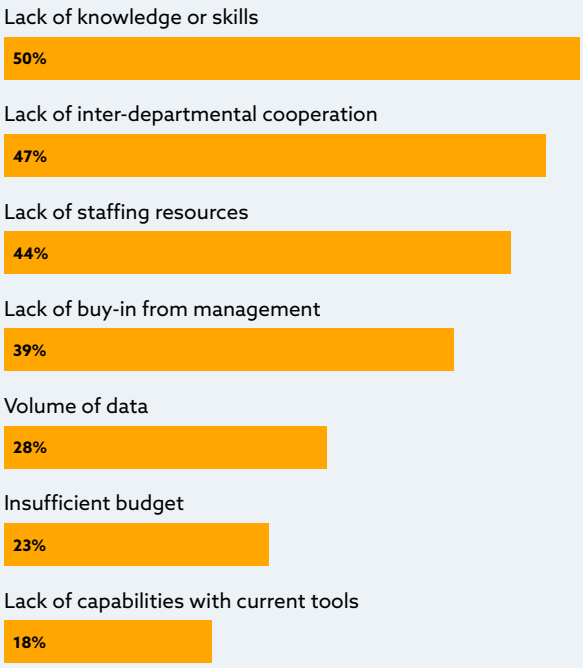
Priority of capturing dark data

Despite the difficulty, organizations' concerns around dark data appear to be driving them to prioritize capturing dark data, with 82% reporting that it's a moderate to high priority. Organizations seem to understand the security, privacy, and compliance violations, cost, and competitive disadvantage that dark data poses for their organization. More organizations need to consider the use of data discovery tooling to curb the issue of dark data..



Top barriers to capturing dark data

The top three barriers for organizations capturing dark data are related to staffing issues: lack of skills/knowledge (50%), lack of interdepartmental cooperation (47%), and lack of staff resources (44%). Organizations will need to dedicate themselves to educating their staff and prioritizing technologies that can support staffing gaps. They'll also need to leverage tools with automation, ML, or AI to help augment their team's knowledge/ skills and supplement the lack of staffing resources available. Organizations should also establish a single platform for various departments to work from. This will provide unified base knowledge these teams need to work cohesively.

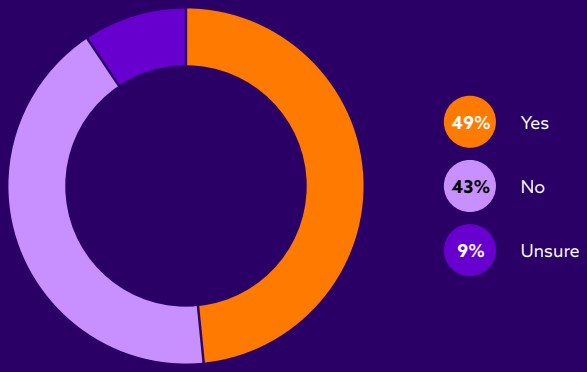


© Copyright 2022, Cloud Security Alliance. All rights reserved.

Data Breaches

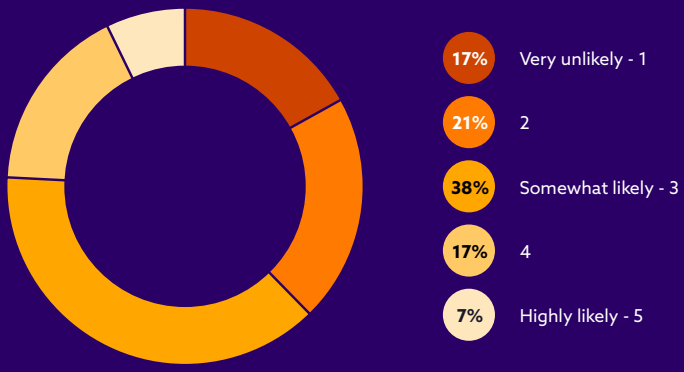
Cloud data breaches in the past 12 months

Nearly half of organizations (49%) report having a cloud data breach within the past 12 months. Given the high levels of confidence in their ability to protect data in the cloud, it appears the reality is more grim. This could be due to increasingly complex cloud environments that organizations work from, making a universal data security strategy more difficult.



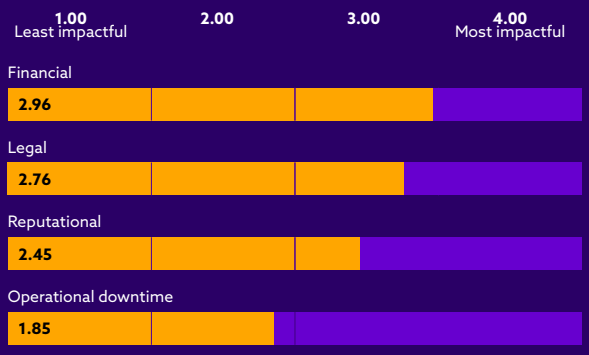
Likelihood of an attempted cloud data breach in the next 12 months

Sixty-two percent of organizations report an attempted cloud data breach to be somewhat to highly likely. Given the high number of organizations who report having experienced a cloud data breach in the past 12 months, it would be expected for there to be more concern around an attempted breach in the upcoming 12 months. For organizations that had experienced a breach in the past 12 months, their average response was somewhat likely, while those who hadn't experienced a breach had an average response between very unlikely and somewhat likely.



Impact of data breaches

The most impactful aspects of a data breach for organizations are the financial aspects. This is likely because all the other potential impacts such as legal, reputational, and operational downtime ultimately boil down to a cost to the organization through fines, cost of services, or loss of work. For operational downtime, the average ranking was notably lower as well. This may be due to the use of redundancies which would reduce or eliminate this issue.

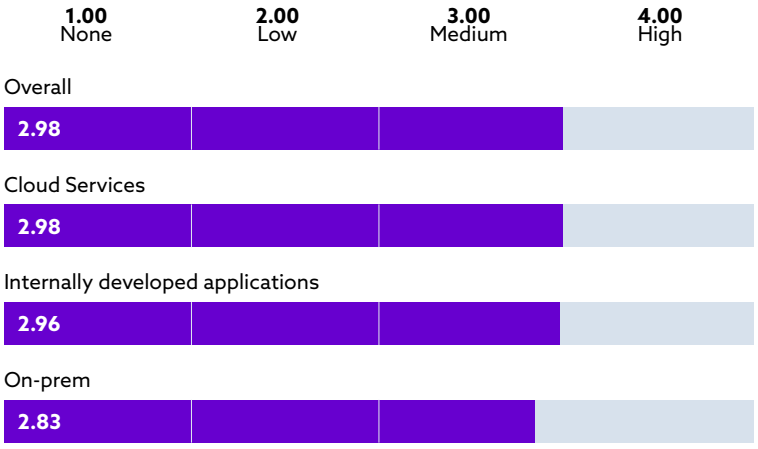


© Copyright 2022, Cloud Security Alliance. All rights reserved.

Regulatory Compliance

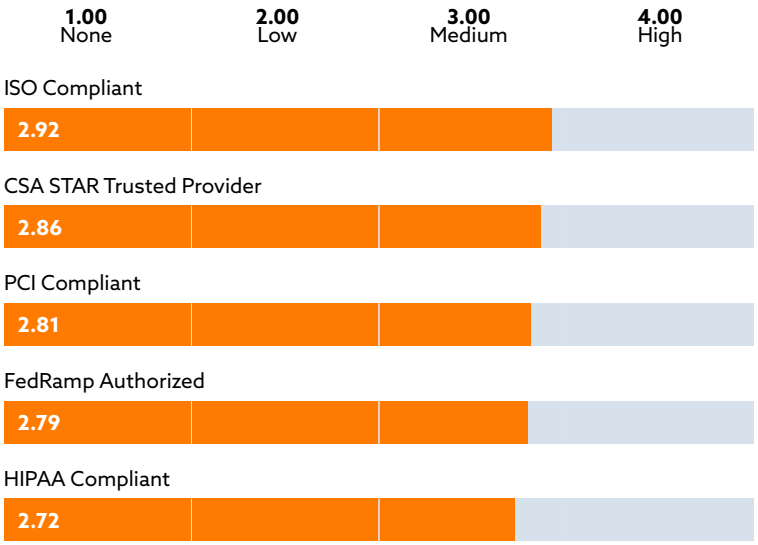
Level of difficulty for regulatory compliance

Regulatory compliance poses a moderate level of challenge for organizations regardless of environment. On-prem is rated only slightly less difficult than cloud services or internally developed apps.



Importance of security compliance certifications with third-party vendors

Regarding security compliance certifications for third-party vendors, it appears that most certifications hold a medium level of importance for organizations regardless of the type of certification. Depending on the industry and the type of data organizations work with, this can vary.

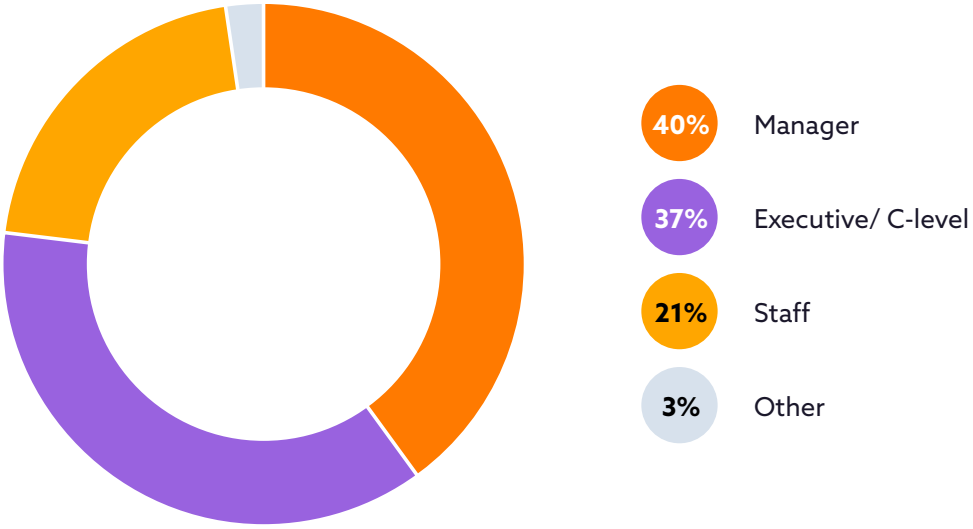


© Copyright 2022, Cloud Security Alliance. All rights reserved.

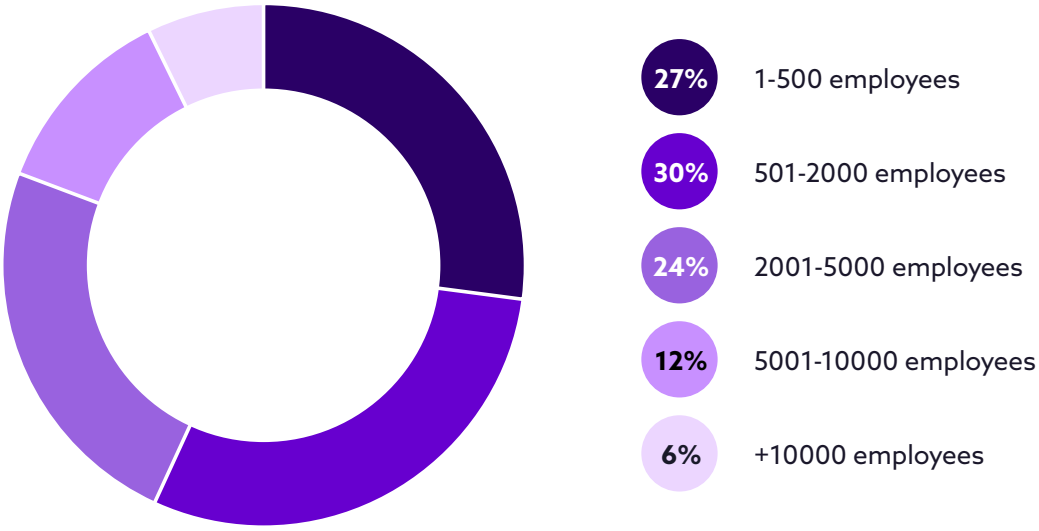
Demographics

This survey was conducted in July 2022 and gathered 1663 responses from IT and security professionals from organizations of various sizes, industries, locations, and roles.

What is your job role?

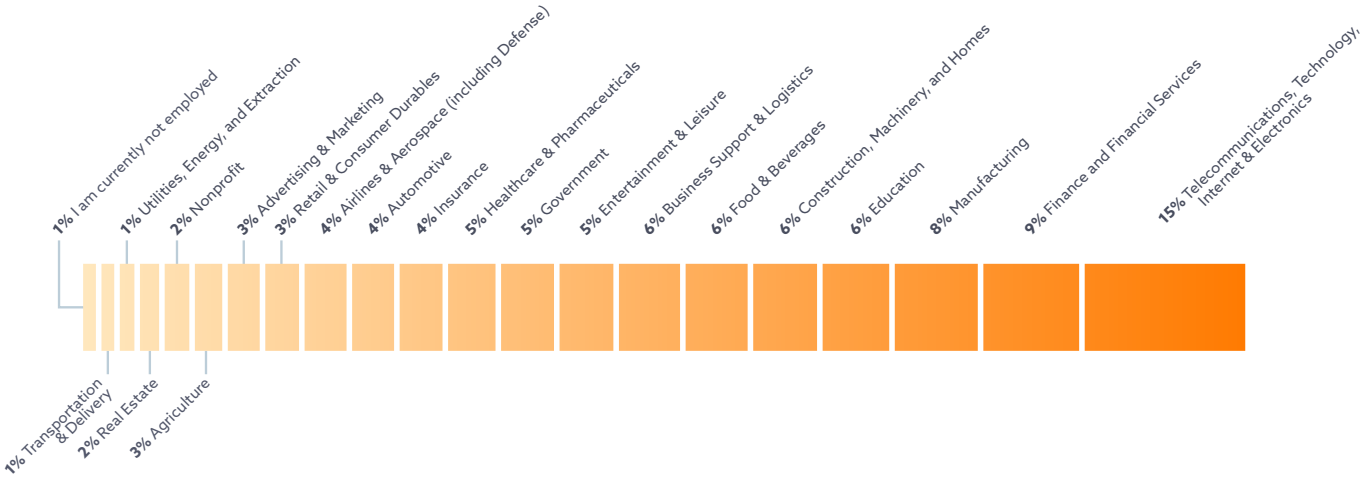


What is the size of the organization you work for?

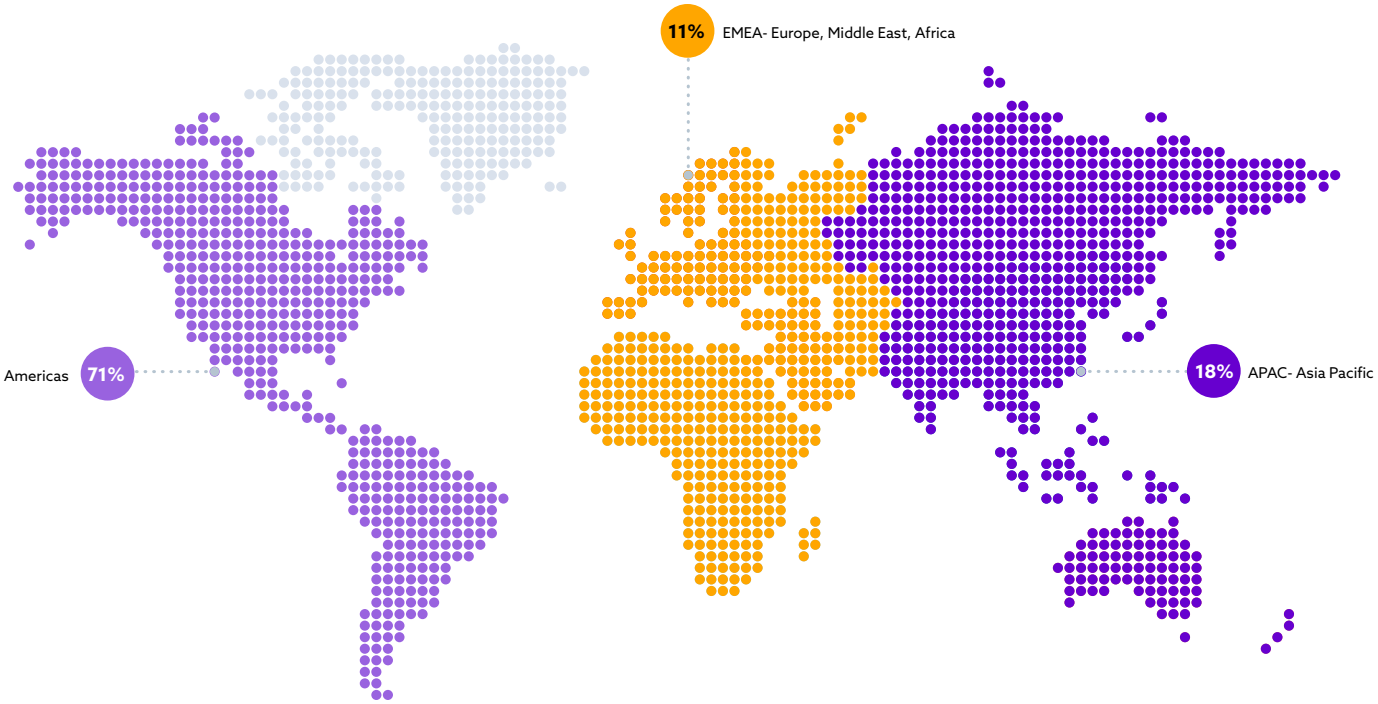


© Copyright 2022, Cloud Security Alliance. All rights reserved.

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



What region are you located in?



© Copyright 2022, Cloud Security Alliance. All rights reserved.