Enterprise Strategy Group™ by TechTarget

CLOUD DATA SECURITY

Jack Poller, Senior Analyst

JANUARY 2023

Research Objectives

Digital transformation initiatives and remote work have further accelerated the migration of data assets to cloud stores, and sensitive data is now distributed across multiple public clouds. The use of disparate controls has led to a lack of consistent visibility and control, putting cloud-resident data at risk of compromise and loss.

What's necessary to secure cloud-resident data? Organizations need solutions that support data loss detection and prevention capabilities across a range of cloud applications and services. These solutions need cloud-native controls that provide a unified approach across disparate cloud data stores via API integration.

To gain insights into modern processes for securing cloud-resident data, TechTarget's Enterprise Strategy Group (ESG) surveyed 387 IT, cybersecurity, and DevOps professionals responsible for evaluating, purchasing, testing, deploying, and operating hybrid cloud data security technology products and services at organizations in North America .

This study sought to:

Examine the impact of the public cloud on data security priorities.

Gain insight into top data security challenges and rate data loss from the cloud.

Determine the degree of separate versus unified approaches for cloud and on-premises data sets.

Establish data security spending intentions and priorities.

KEY FINDINGS

CLICK TO FOLLOW

Data is shifting to public clouds ahead of organizational readiness to secure it.

PAGE 4

Data loss from the cloud is common due to a multitude of causes.

PAGE 8

Organizations face numerous cloud data security challenges driven by scale, complexity, and visibility.

PAGE 11

Organizations are applying cloud data security technologies, with a desire for integrated data security platforms.

PAGE 15

Data security is a team sport, with security and IT ops taking the lead.

PAGE 18

Organizations are investing in data security, with a third substantially increasing data security's share of cybersecurity budget.

PAGE 21

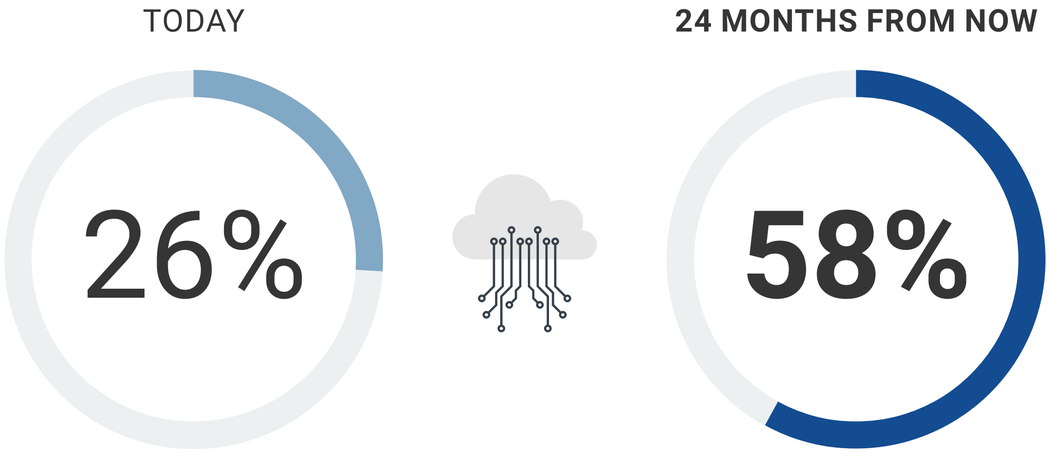

Data is shifting to public clouds ahead of organizational readiness to secure it.

Data, Including Sensitive Data, Continues the Long-term Migration to Public Cloud Platforms

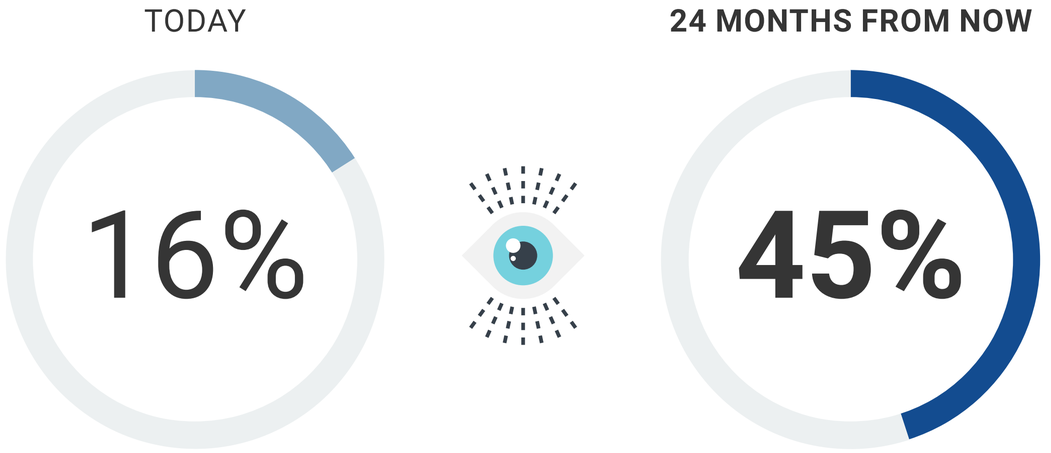
The usage of public cloud services has been pervasive for several years, and digital transformation initiatives and remote work have further accelerated the migration of data assets to cloud stores. Specifically, more than one-quarter (26%) of respondents said that in excess of 40% of their corporate data resides on public cloud services today. This is expected to increase to 58% of organizations within 24 months.

This inherently means that sensitive data is also now distributed across multiple public clouds. Indeed, one in six (16%) respondents said that more than 40% of their organization's corporate data that resides on public cloud services today is sensitive. This is expected to almost triple to 45% of organizations within 24 months.

Organizations with more than 40% of company data in public cloud.



Organizations identifying more than 40% of their SaaS-resident data as sensitive.



BACK TO CONTENTS

The Vast Majority of Data Storehouses Contain Sensitive Data and Are Important to the Business

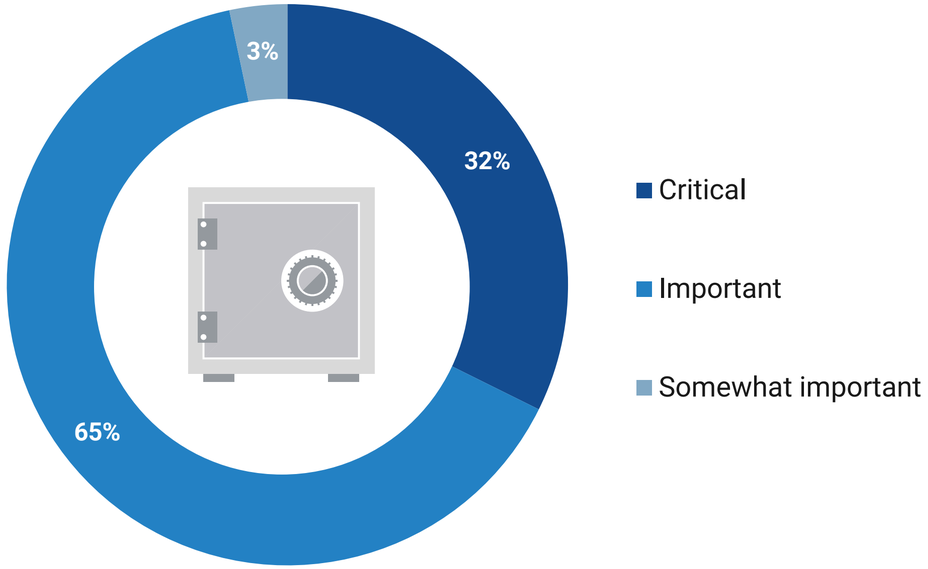
Organizations are using new and powerful business analytics and machine learning capabilities to extract more value from their data, necessitating the use of data lakes, data warehouses, and data lakehouses.

Analytics of business data provides the most utility when analyzing sensitive data, so it's no surprise that the vast majority (86%) of these organizations report these storehouses contain sensitive data. Furthermore, nearly one-third (32%) of respondents say the senstive data in these storehouses is critical to their business.

86%

of respondents said they have **sensitive data** stored in a data lake, data warehouse, or data lakehouse.

Business criticality of sensitive data stored in data lakes, data warehouses, or data lakehouses.



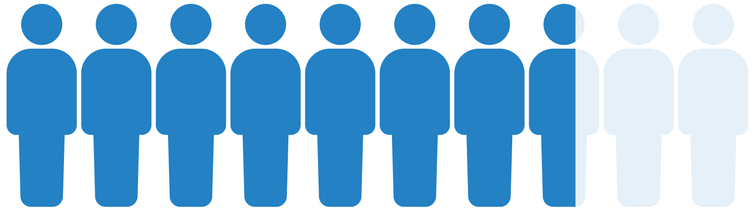
"Analytics of business data provides the most utility **when analyzing sensitive data.**"

BACK TO CONTENTS

Public Cloud Security Is Not Keeping Pace with Requirements

The use of disparate controls puts cloud-resident data at risk of compromise and loss, and respondents agree. In fact, a third (33%) believe that more than 30% of their organization's SaaS-resident sensitive data is insufficiently secured. The greater problem is that more than half (59%) believe that more than 30% of their organization's sensitive data residing in IaaS and PaaS environments is insufficiently secured.

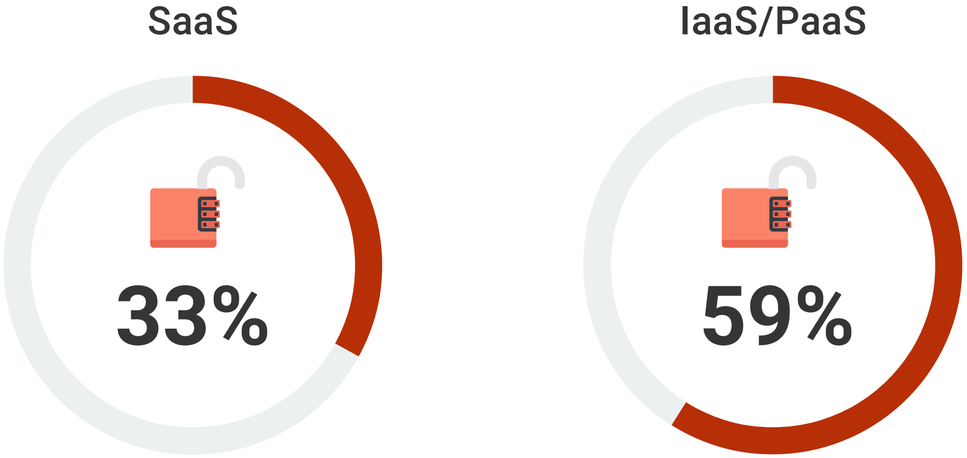
With multi-cloud strategies now being the norm, more than three-quarters currently store sensitive data in more than one IaaS/PaaS platform. With each platform having its own native policies and controls, ensuring complete security of all cloud-resident senstive data can be challenging.



77%

of organizations currently store **sensitive data** in more than one IaaS/PaaS platform.

Percentage of organizations that believe more than 30% of their sensitive cloud-resident data is insufficiently secured.



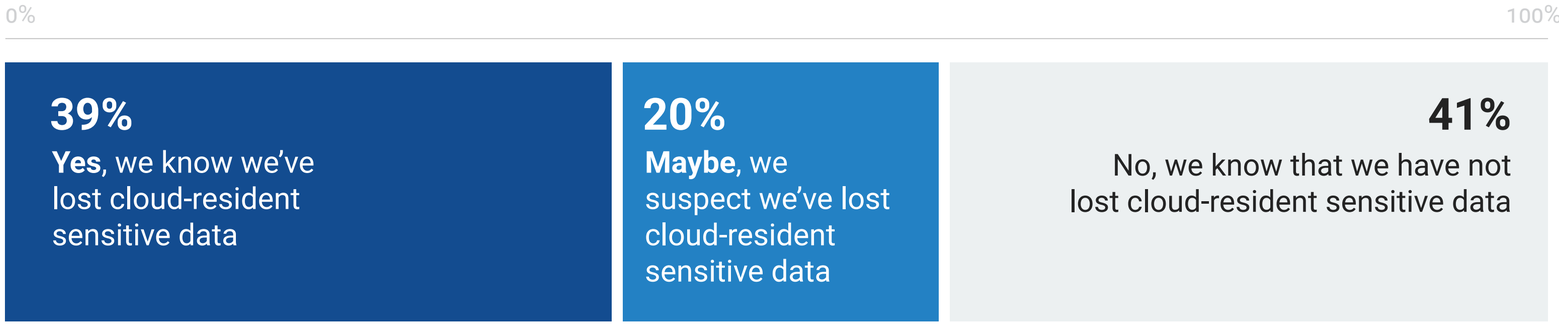
BACK TO CONTENTS

Data loss from the cloud is common due to a multitude of causes.

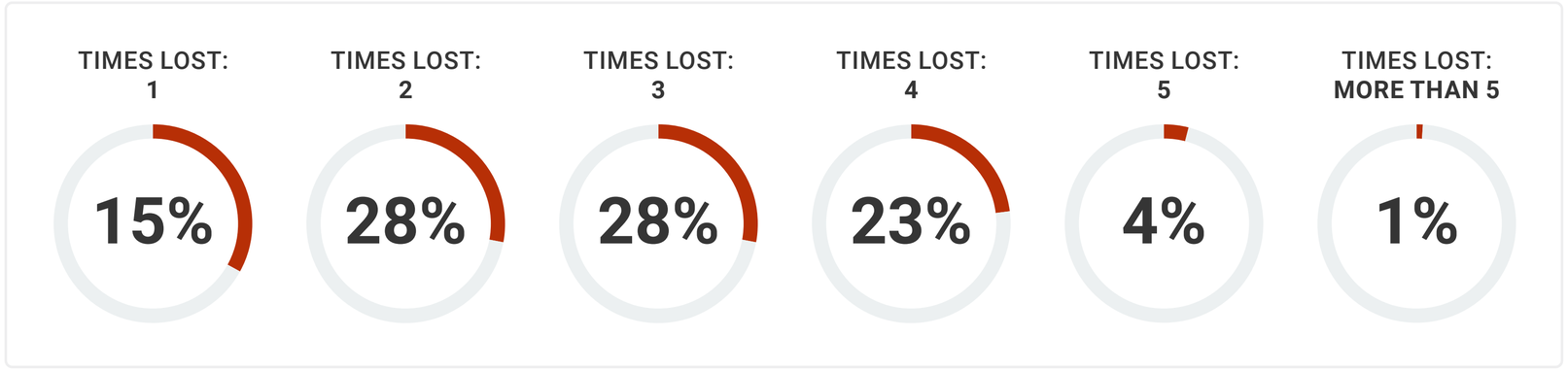
Organizations Are Losing Cloud-resident Sensitive Data

One in four (39%) respondents *know* their organization has lost cloud-resident senstive data. Of greater concern are the 20% who suspect they've lost cloud-resident sensitive data but don't know for sure because they don't have the tooling or expertise to find out. These organizations are failing to learn from and respond to data loss, resulting in multiple incidents.

Unfortunately, 84% indicate they've suffered multiple data loss events in the past 12 months, with more than one-quarter (27%) reporting four or more data loss events.



Number of times these organizations lost, or suspect they lost, cloud-resident sensitive data in the last 12 months.

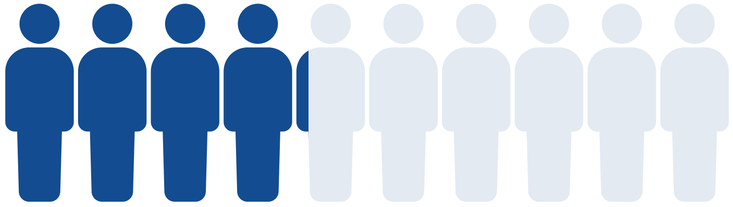


BACK TO CONTENTS

Contributors to Cloud-resident Sensitive Data Loss

Despite IaaS and PaaS platforms having a plethora of block, file, object, and database storage options and a greater attack surface, the most common data loss culprit was SaaS applications: 42% of respondents experienced sensitive data loss from their SaaS platforms.

Confusion regarding the shared responsibility security model and how best to secure SaaS-resident sensitive data may be the prime contributing factor. The most common contributors to cloud-resident sensitive data loss were misconfigurations of services, policy violations, and access controls/credentials issues.



42%

say they have lost cloud-resident sensitive data from SaaS applications.

The top contributors to cloud-resident sensitive data loss.

MISCONFIGURATIONS

- Misconfiguration of SaaS services: **33%**
- Misconfiguration of IaaS/PaaS services: **32%**

POLICY VIOLATIONS

- Data exposure from data misclassification: **33%**
- Unsanctioned apps/services: **26%**
- Incorrect/insufficient security policies: **25%**

ACCESS CONTROLS

- Malicious insider accessing sensitive data: **31%**
- Attacker masquerading as an employee via stolen credentials: **26%**
- Unauthorized access by an over-provisioned account: **23%**

BACK TO CONTENTS

Organizations face numerous cloud data security challenges driven by scale, complexity, and visibility.

Top Data Security Challenges Intersect with Data Classification

When it comes to general data security challenges, organizations identify a variety of issues. However, the top five in terms of the level of difficulty they present include regulatory compliance, determining risk associated with sensitive data, data governance, and the detection/prevention of data exfiltration or misuse.

One way for organizations to potentially overcome most, if not all, of these challenges is to scan the entirety of their data stores to correctly classify and apply the appropriate data security policies. Indeed, when asked for their preferred method for discovering sensitive data, more than two-thirds (70%) of organizations want their data security controls to read **100%** of every file, object, database, or other cloud data store. While this is likely the most effective approach to overcoming key data security obstacles, organizations must account for the time and cost involved, which could actually create additional challenges.

| Top five most difficult data-related tasks.

1.
Regulatory compliance

2.
Determining risk associated with sensitive data

3.
Data governance

4.
Detection of data exfiltration or misuse

5.
Prevention of data exfiltration or misuse

> “More than two-thirds (70%) of organizations **want their data security controls to read 100% of every file, object, database, or other cloud data store.**”

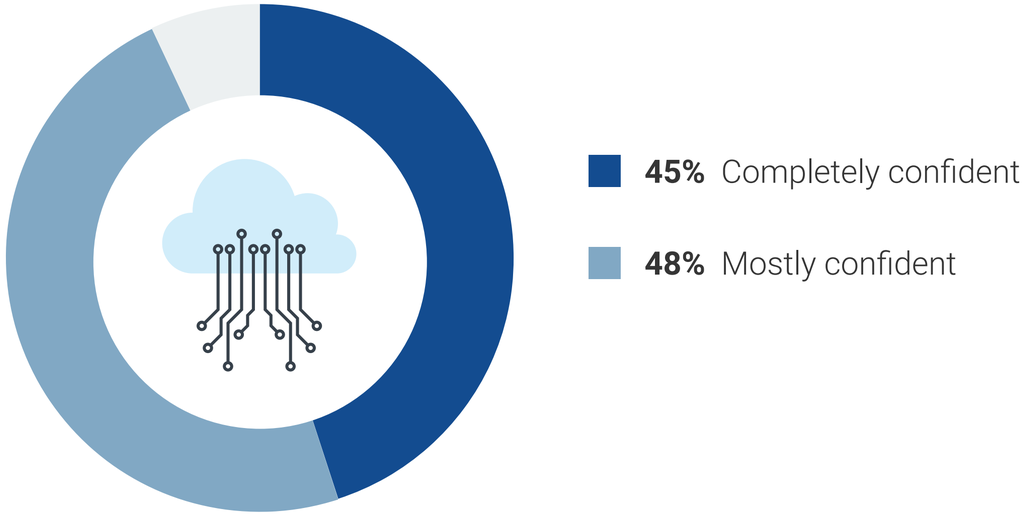
BACK TO CONTENTS

Overconfidence in Discovery and Classification Efforts for Cloud-resident Data?

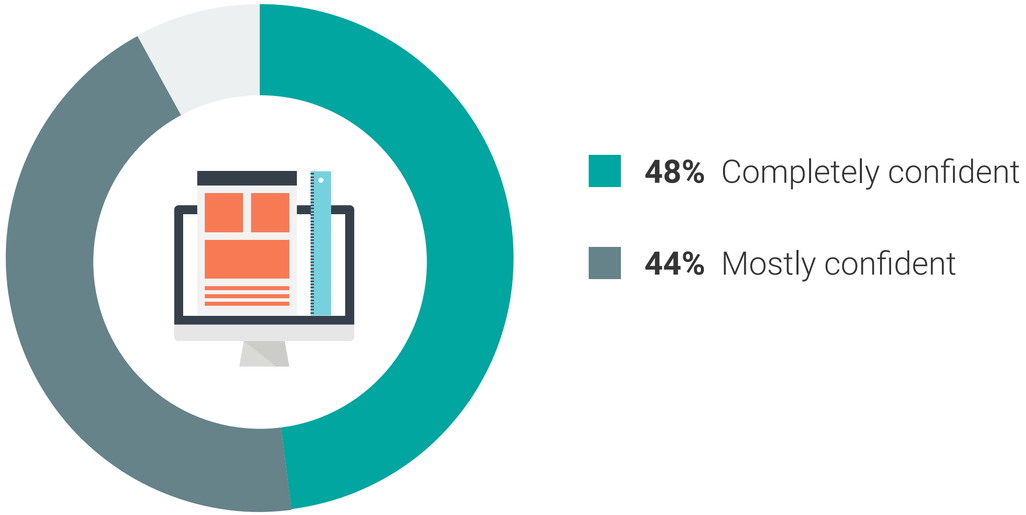
Most organizations place a premium on discovering sensitive data, so confidence in these abilities is high. Specifically, 93% of respondents were mostly or completely confident in their organization's ability to discover cloud-resident data. However, it is worth noting that 19% of organizations attribute a cloud-resident data loss event within the past year to undiscovered shadow data.

Confidence levels are similarly high in classifying public cloud-resident data. Indeed, 92% of respondents were mostly or completely confident in their ability to classify cloud-resident data. As was the case with data discovery capabilities, there does seem to be a disconnect between organizations' confidence levels and actual capacity since 33% have suffered data loss due to misclassification of data in the last 12 months.

Confidence level in ability to **discover all** public cloud-resident data.



Confidence level in ability to **classify all** public cloud-resident data.

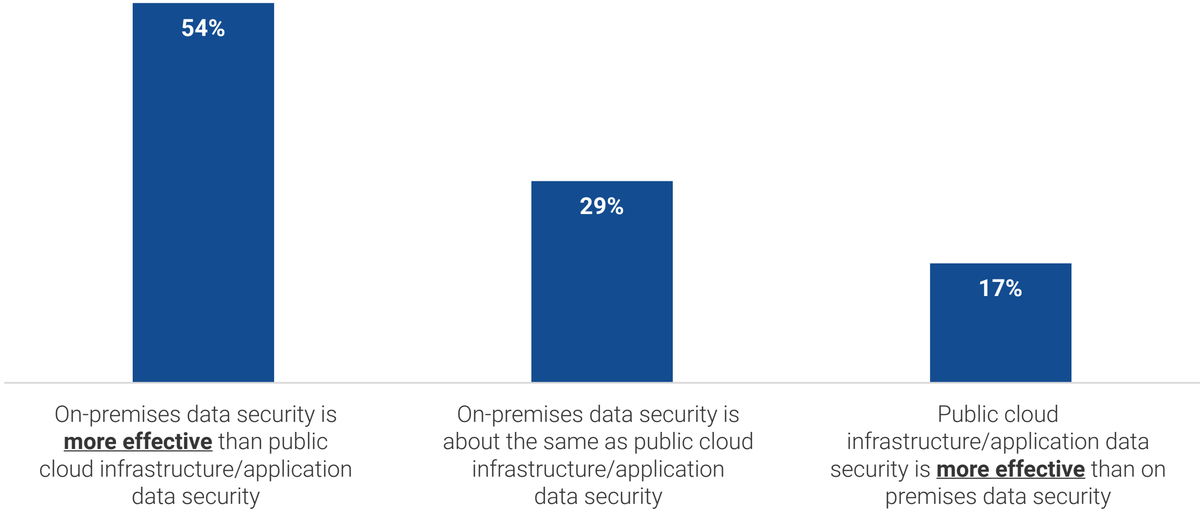


BACK TO CONTENTS

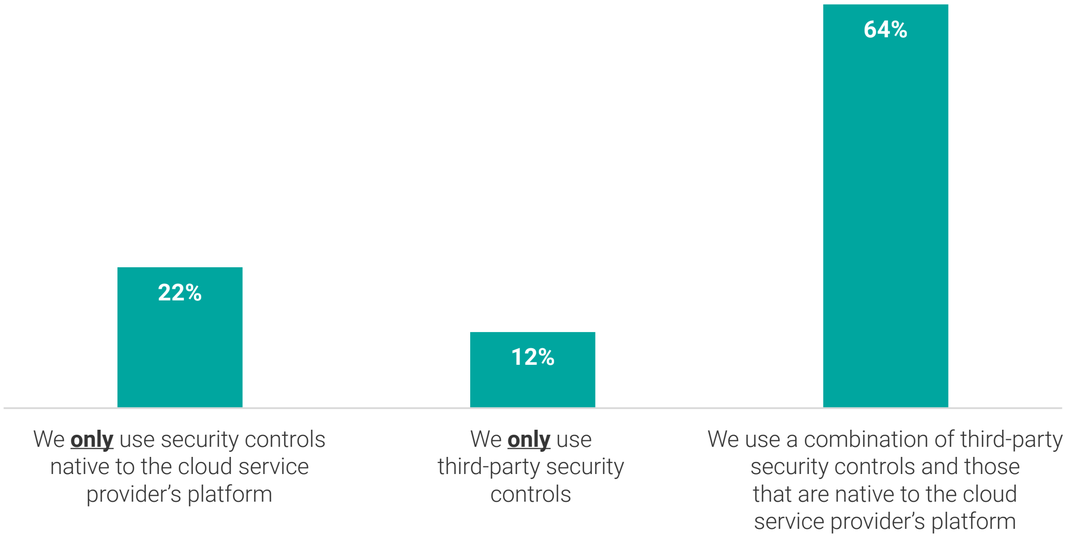
Lukewarm Confidence in Cloud Data Security and CSP Controls

Organizations have greater faith in their ability to protect on-premises data than public cloud-resident data. This is confirmed by the fact that respondents were three times likelier (54% versus 17%) to report their organization's on-premises data security is more effective than its cloud data security. These organizations use a combination of third-party and native cloud service provider (CSP) controls as layers in a comprehensive defense-in-depth strategy.

Perception of on-premises versus public cloud data security.



Controls currently employed to secure IaaS-/PaaS-resident sensitive data.



BACK TO CONTENTS

Organizations are applying cloud data security technologies, with a desire for integrated data security platforms.

Effectiveness of Third-party Tools and CSP Capabilities

As part of their defense-in-depth strategy, organizations view data loss prevention (DLP), data detection and response (DDR), cloud security posture management (CSPM), and data security posture management (DSPM) as the most effective data security tools. What aspects of data security do organizations feel cloud service providers do well? In addition to monitoring and alerting on anomalous activities as well as data breach detection and response capabilities, organizations trust their cloud service providers for encryption key management, audit trail services, and native multi-factor authentication.

Capabilities believed to be most effective for protecting public cloud-resident sensitive data.

22%
DLP module in a CNAP solution

21%
DLP module in a SASE or SSE platform

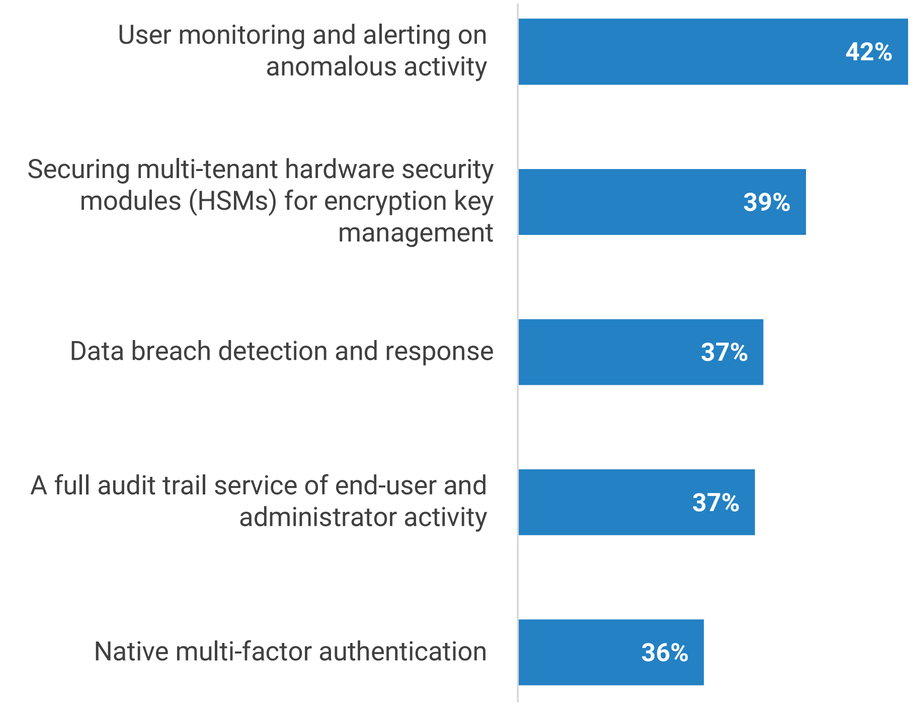
19%
Data detection and response (DDR)

19%
Adaptive and multi-factor authentication

18%
Cloud security posture management (CSPM)

18%
Data security posture management (DSPM)

Areas of data security organizations most trust a CSP to handle.



BACK TO CONTENTS

According to the Enterprise Strategy Group's *2023 Technology Spending Intentions Survey*[1]

45% of organizations have a cybersecurity skills shortage

42% say cloud security is the most difficult cybersecurity role to fill

"Two-thirds prefer to consume data security tools **as a comprehensive integrated data security platform."**

Organizations Prefer a Comprehensive, Integrated Data Security Platform

Faced with the mandate to do more with less, a plethora of cybersecurity tools, and the perpetual global cybersecurity skills shortage, security teams are looking for tool consolidation and breadth of coverage to drive efficiency and risk reduction. Specifically, two-thirds prefer to consume data security tools as a comprehensive integrated data security platform. As far as the attributes that organizations would most prefer to see as part of these platforms, the top five include data type and location coverage, integration with other security tools, and availability as a managed or cloud service.

Top five most important data security platform attributes

1. Data type coverage (structured, unstructured, video, etc.)

2. Data location coverage (SaaS, IaaS, PaaS, and on-premises)

3. Integration with other security tools

4. Availability as a managed service

5. Availability on cloud marketplaces

[1]Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey,* November 2023.

BACK TO CONTENTS

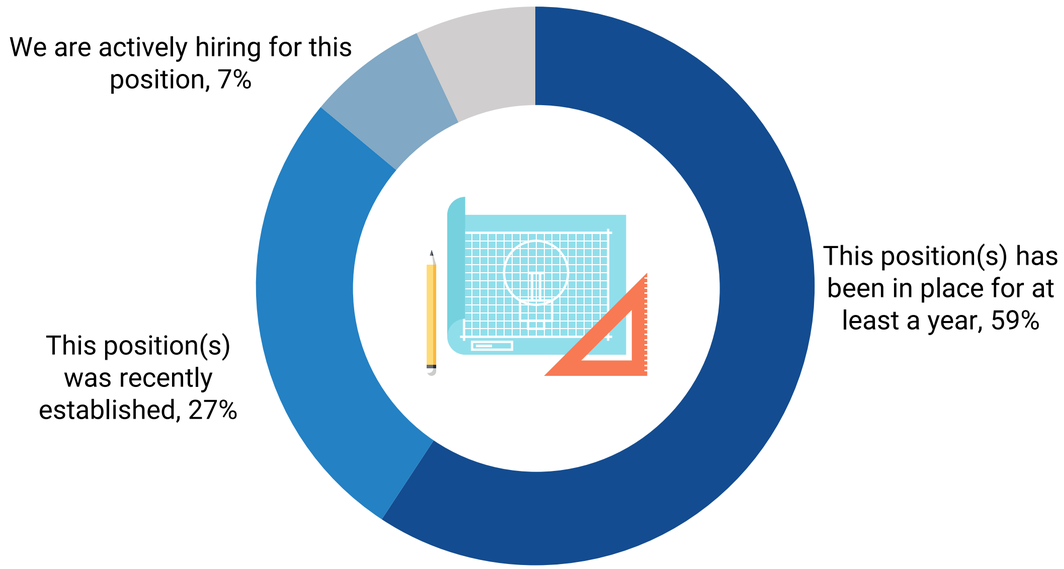
Data security is a team sport, with security and IT ops taking the lead.

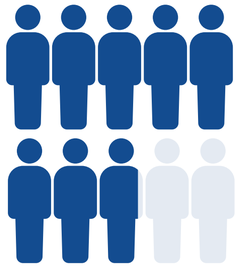
The Emergence of the Cloud Security Architect

Specialists with knowledge and experience are required to secure the organization's cloud footprint. Most organizations (86%) say they currently have a cloud security architect (CSA) in place, with another 11% actively hiring or establishing this position within the next 12-24 months.

More than three-quarters (79%) of these organizations said their CSA does/will report to a C-level executive. The C-level reporting structure indicates cloud data security has a strategic charter. In terms of areas of responsibility, 59% of organizations report that their CSAs define (or likely will define) policies for cloud-resident data, and another 50% state that these individuals are involved in DevSecOps.

Status of cloud security architects.





79%
of organizations say **their CSA does/ will report to a C-level executive.**

59%
say CSAs define or will define policies for cloud-resident data.

50%
say CSAs are involved in DevSecOps.

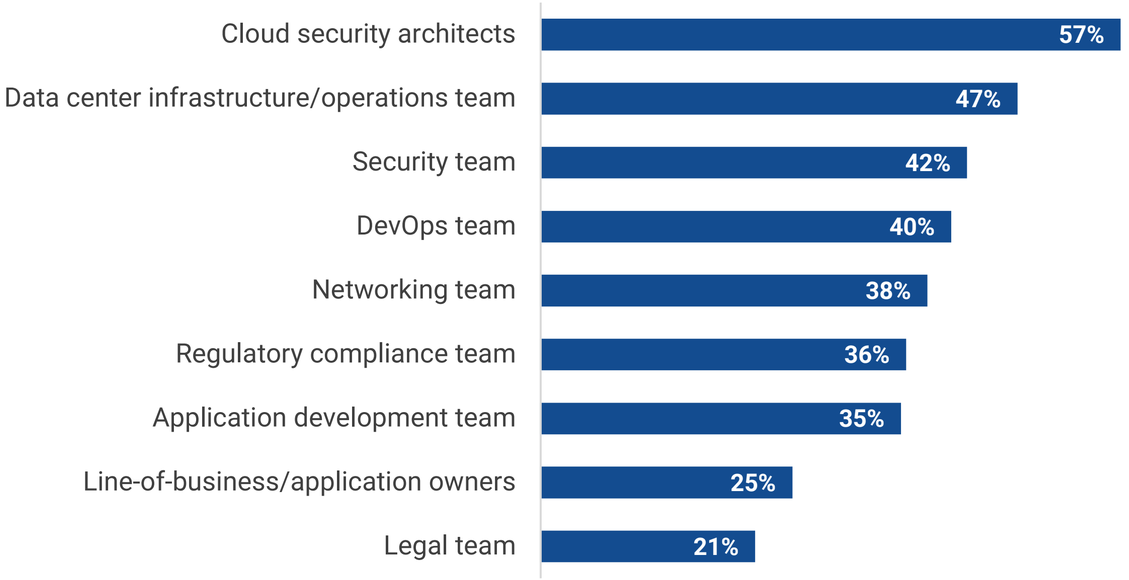
BACK TO CONTENTS

Data Security Is a Team Sport, but Cloud Is Driving Consolidation across Disparate Environments

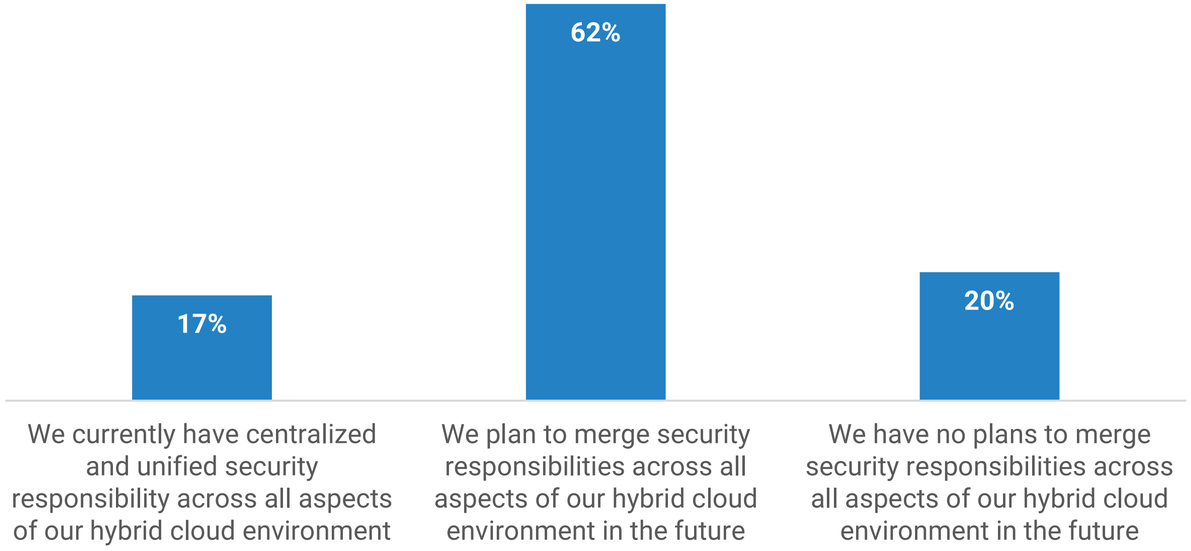
In terms of the individuals or groups that are directly involved in creating data security policies, CSAs lead the way in defining data security policies. However, they are not alone, with other groups representing various interests and responsibilities participating in this process as well, including those in data center operations (47%), security (42%), and DevOps (40%).

While many organizations today have different groups or individuals responsible for the on-premises and public cloud-resident portions of their data security processes, policies, and technologies, as cloud-native applications continue to gain critical mass and become an even more substantial part of the overall IT footprint, companies are looking to merge the related security responsibilities. Indeed, nearly one in five (17%) organizations have already centralized and unified security responsibilities across all aspects of their hybrid cloud environments, while another 62% expect to merge these responsibilities.

Capabilities believed to be most effective for protecting public cloud-resident sensitive data.



Areas of data security organizations most trust a CSP to handle.



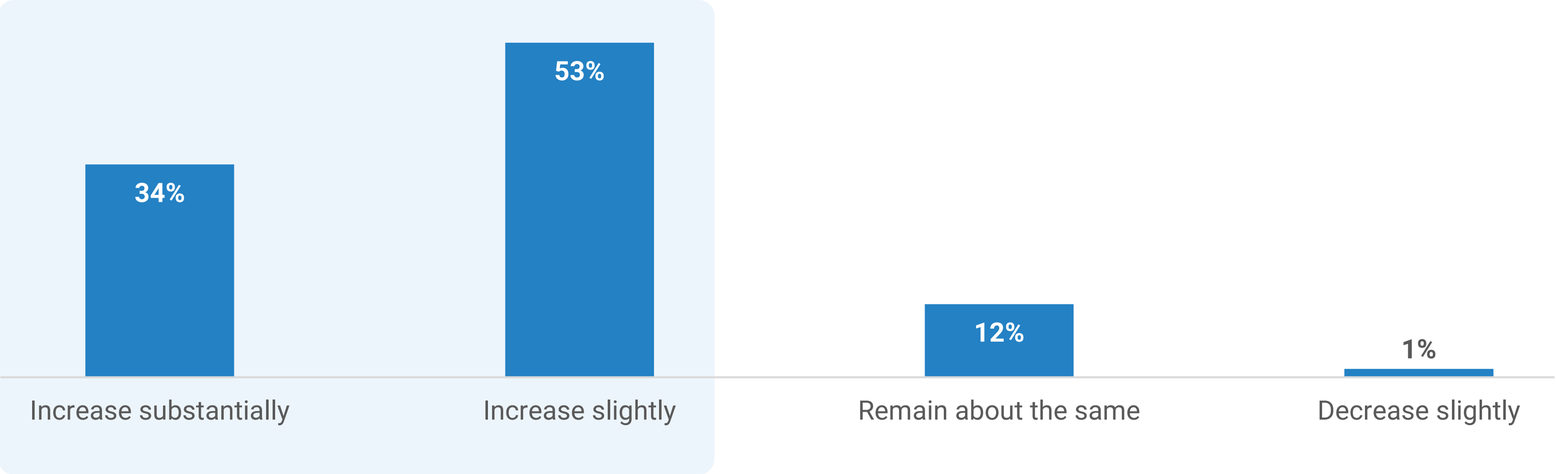
BACK TO CONTENTS

Organizations are investing in data security, with a third substantially increasing data security's share of cybersecurity budget.

Data Security to Garner a Larger Share of Security Budget

The publicity of ransomware and other cybersecurity attacks has raised the awareness of data security as a critical component of an organization's overall cybersecurity strategy. Not surprisingly, organizations are earmarking their cybersecurity budgets to include data security. Specifically, 87% of organizations expect to increase their spending on data security technologies and services over the next 12-24 months, with more than one-third classifying these increases as substantial.

Expected spending change for data security over the next 12-24 months.



According to the Enterprise Strategy Group's *2023 Technology Spending Intentions Survey*[2]

35% say strengthening cybersecurity drives technology spending (top response).

40% say improving cybersecurity justifies IT investment to business management (top response).

65% anticipate a cybersecurity budget increase.

[2]Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey,* November 2023.

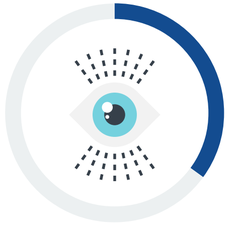
BACK TO CONTENTS

Highest Priorities for Data Security

The desire to gain operational efficiencies and manage the volume and velocity of data are among the most common drivers of investments in third-party data security tools. In terms of more general priorities to protect cloud-resident sensitive data, organizations aspire to develop defense-in-depth data security strategies for heterogeneous public/private clouds by using both CSP and new technologies designed for this purpose.

Top drivers behind usage of third-party data security technologies and services to protect cloud-resident sensitive data.

39%
want to gain operational efficiencies via centralization of policies and controls for hybrid cloud environments.



35%
want to gain operational efficiencies via centralization of policies and controls for cloud-resident sensitive data.

35%
want tools to handle the sheer volume of cloud-resident sensitive data.

Top priorities for protecting cloud-resident sensitive data.

35%
are prioritizing a strategy to secure sensitive data across heterogeneous public and private cloud environments.

31%
are prioritizing new technology specifically designed to protect cloud-resident sensitive data.

29%
are prioritizing cloud service provider data security controls.

BACK TO CONTENTS

Normalyze™

data-first cloud security

Normalyze is a pioneering provider of cloud data security solutions helping customers secure their data, applications, identities, and infrastructure across public clouds. With Normalyze, organizations can discover and visualize their cloud data attack surface within minutes and get real-time visibility and control into their security posture, including access, configurations, and sensitive data to secure cloud infrastructures at scale. The Normalyze agentless and machine-learning scanning platform continuously discovers resources, sensitive data and access paths across all cloud environments. The company was founded by industry veterans Ravi Ithal and Amer Deeba and has several customers, including Corelight, Chargepoint, Fairfield, Netskope, Orkes and Sigma Computing. The company is funded by Lightspeed Venture Partners and Battery Ventures.

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

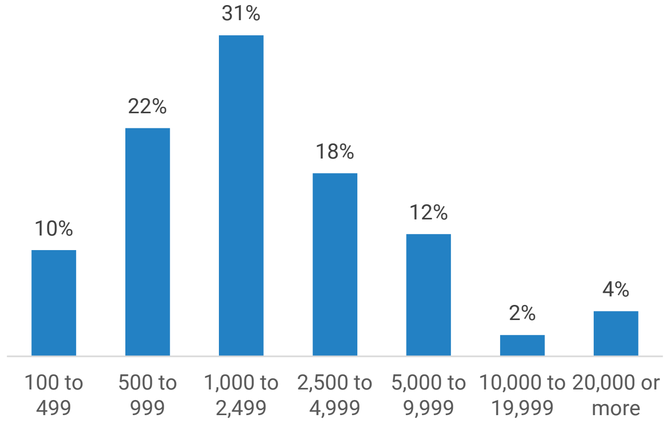
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology and Demographics

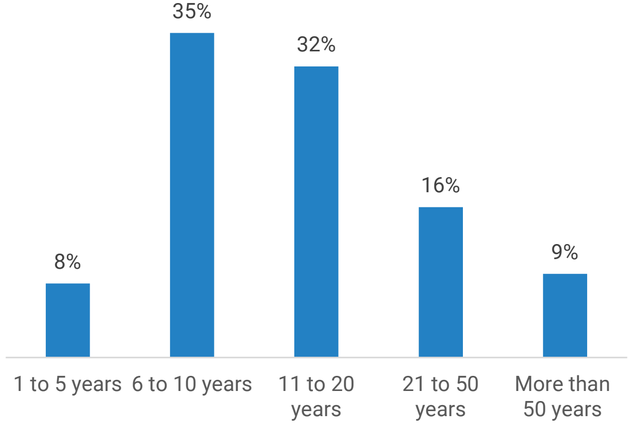
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between November 8, 2022 and November 29, 2022. To qualify for this survey, respondents were required to be IT, cybersecurity, or DevOps professionals personally responsible for evaluating and purchasing hybrid cloud data security technology products and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 387 IT, cybersecurity, and DevOps professionals.

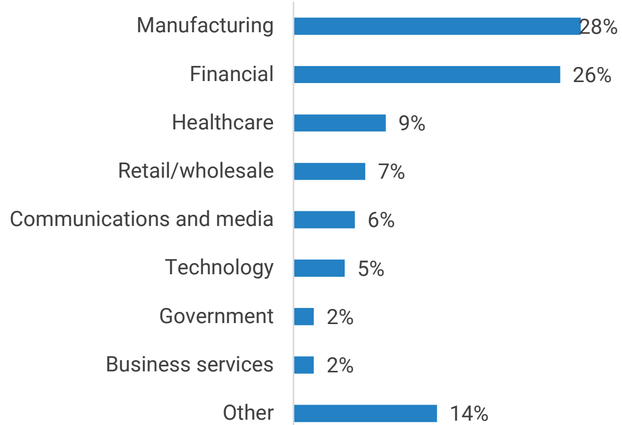
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.