Data Loss Prevention and Data Security Survey Report

netskope

CSA cloud security alliance®

Thank You to Our Sponsor

The Cloud Security Alliance (CSA) is a not-for-profit, member-driven organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge, and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. CSA research prides itself on vendor neutrality, agility and integrity of results.

Thank you to our sponsor, Netskope, for helping fund the development of the research and ensuring quality control through the CSA research lifecycle. Sponsors are CSA Corporate Members who support the findings of the research project but have no added influence on the content development or editing rights of CSA research.

About the Sponsor

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.

http://www.netskope.com/

Acknowledgments

Lead Author

Hillary Baron

Contributors

Josh Buker
Ryan Gifford
Sean Heide
Alex Kaluza
John Yeoh

Designer

Claire Lehnert

Special Thanks

Chad Berndtson
Carmine Clementelli
Tim Whitman

Table of Contents

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.

Netskope commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding data protection in cloud-first technology environments. Netskope financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in October and November of 2022 and received 2673 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 the study were to better understand...

- Current DLP strategies organizations use
- Pain points and challenges encountered with DLP strategies
- Concerns around remote workers with regards to data security
- Security training offerings for employees

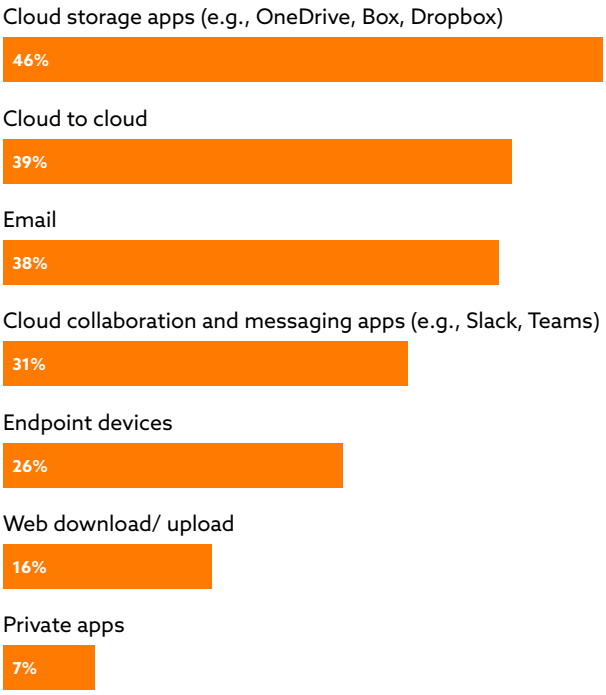
Key Findings

As the traditional perimeter is reduced or eliminated with the move to remote or hybrid work, data security approaches for cloud-first environments have had to adapt. Data security is also a key tenant of zero trust security strategy, which has gained popularity, further spurring this focus on data security. DLP solutions are often an integral part of organizations' data security strategy, but organizations are still struggling with their strategy and implementation of these solutions, especially for how complicated legacy DLP solutions are to manage and maintain.

Key Finding 1:

Cloud is the predominant means for transferring and sharing data

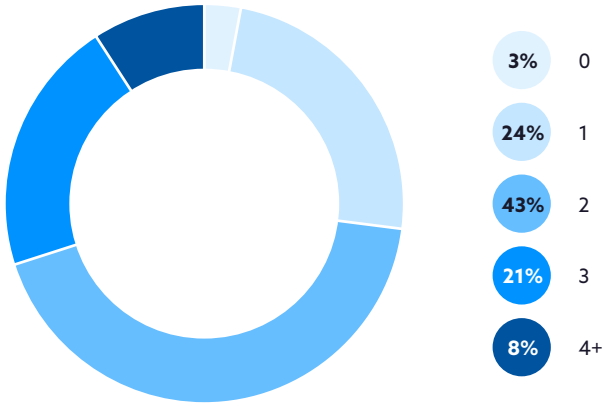
Organizations today are transferring and sharing data primarily through the cloud—a trend catalyzed by the COVID-19 global pandemic. Organizations use a variety and different methods. The most common way is cloud storage applications (46%) such as OneDrive, Box or Dropbox. Other common methods include cloud-to-cloud (39%), which is used slightly more than email (38%) or cloud collaboration and messaging applications (31%) such as Slack or Teams. Regardless of the method, organizations are clearly trusting the cloud with even their most sensitive data.



Key Finding 2:

Most organizations use 2+ DLP solutions

Most organizations (72%) are using two or more DLP solutions as a part of their DLP and data security strategy. With larger organizations (defined as 5,000+ employees), 50% use three or more DLP solutions. A single DLP solution does not meet the needs of the majority of organizations, and several DLP solutions are instead cobbled together. This could be due to the complex IT environments organizations use, requiring them to use multiple solutions to fully cover their environment. A majority of organizations today are dealing with legacy environments in addition to complex multi cloud environments.



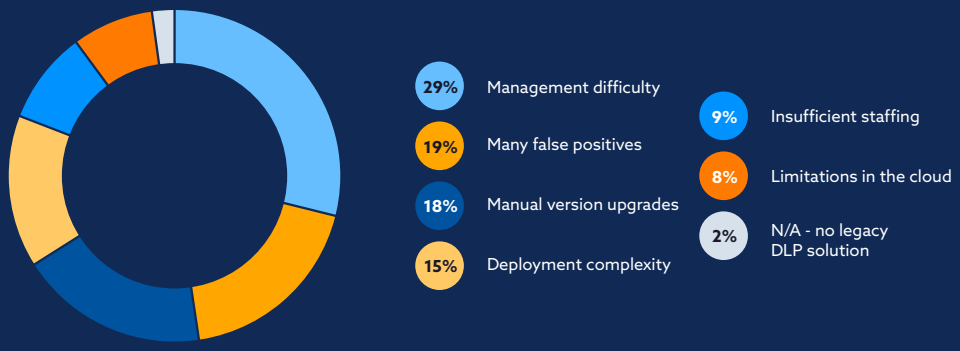
Key Finding 3:

Organizations struggle to manage their complex DLP environments

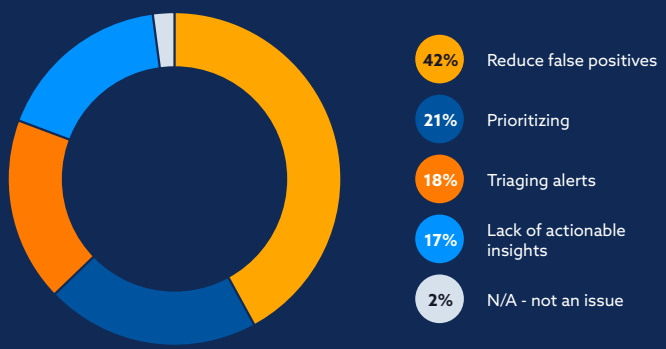
Many of the top challenges with DLP are directly or implicitly tied to management issues. Security teams are already overworked, and the current method of cobbling together multiple DLP solutions is making the problem worse. Organizations are left struggling with management difficulties (29%) as a top challenge. The second most common struggle cited by survey respondents is too many false positives (19%), indicating difficulty with refining the DLP product for their environment. When it comes to false positives, organizations are primarily struggling with how to reduce them and the manual administrative burdens they create.

Other challenges with DLP include the need for manual version upgrades (18%), likely further contributing to the management difficulties, and also deployment complexity (15%), likely due to the need for multiple solutions to cover their complex environments or security needs. On top of these challenges, employees are also struggling to find policy templates with 86% of respondents rating this as a moderately to a highly difficult task. In sum, the current DLP strategies organizations are using are too cumbersome, and organizations need a more streamlined approach/strategy.

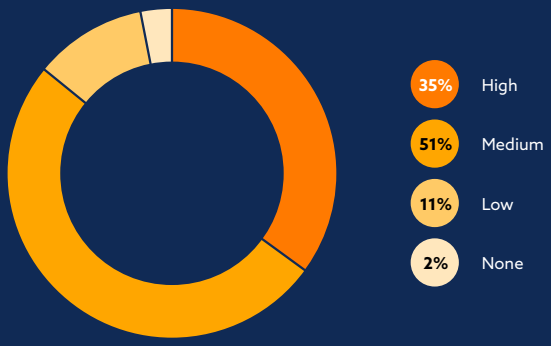
Top challenges with legacy enterprise DLP



Top challenges with false positives



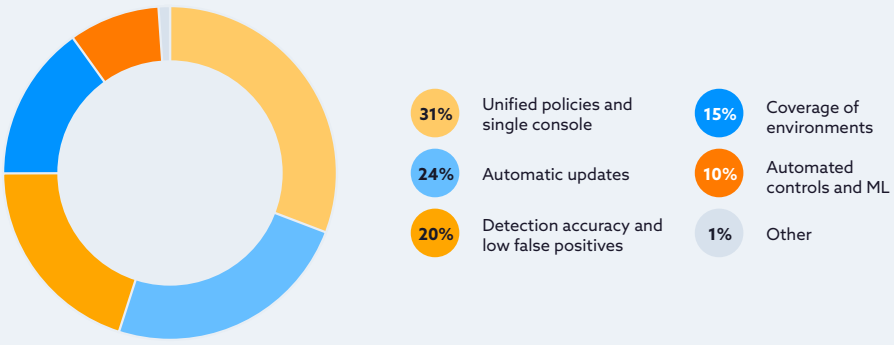
Level of difficulty with finding policy templates



Key Finding 4:

Organizations should prioritize DLP solutions that simplify management

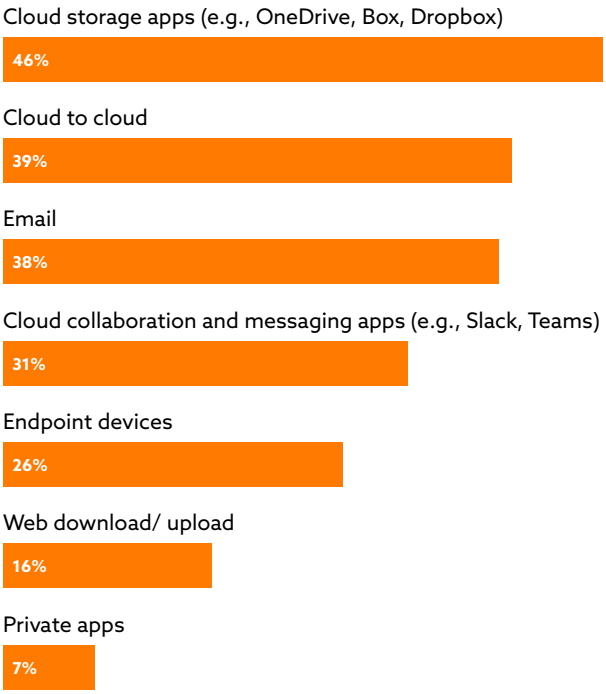
Organizations are looking for DLP and data protection solutions that resolve these issues and management difficulties. Unified policies and single console solutions (31%) will help organizations with the management difficulty and deployment complexity. Automatic updates (24%) avoid additional manual work and reduce the difficulties of management. Additionally, detection accuracy (20%) reduces the number of false positives. In sum, organizations are looking for data protection solutions that are easier to manage and fit cloud needs.



Overview of DLP Strategy

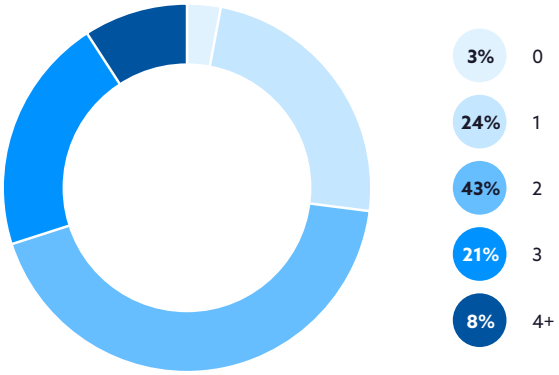
Methods to share and transfer data

Employees are transferring and sharing data primarily through the cloud.The most common method is cloud storage applications (46%) such as OneDrive, Box or Dropbox. Other common methods include cloud-to-cloud (39%), which is used slightly more than email (38%) or cloud collaboration and messaging applications (31%) such as Slack or Teams. Regardless of the method, organizations are trusting cloud with their data.



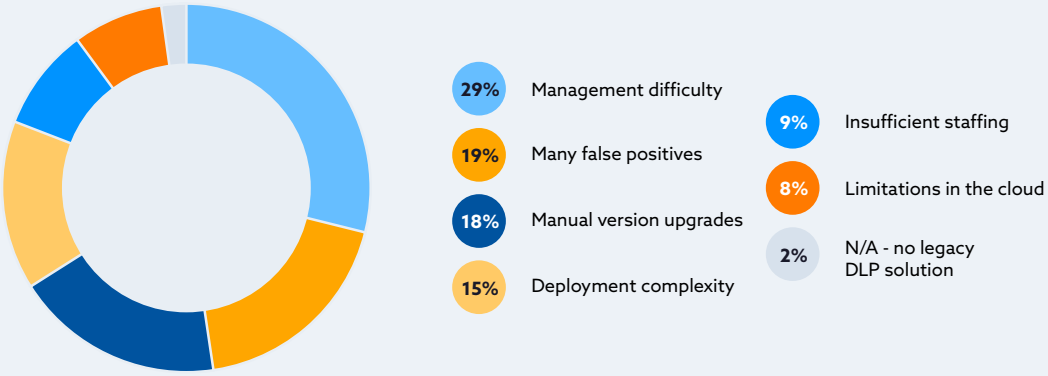
Number of DLP solutions

Most organizations (72%) utilize two or more DLP solutions as a part of their strategy. With larger organizations, 5001+ employees 50% use three or more DLP solutions. This could be due to various environments organizations need to cover. Regardless it appears organizations have to cobble together multiple solutions in order to meet their needs.



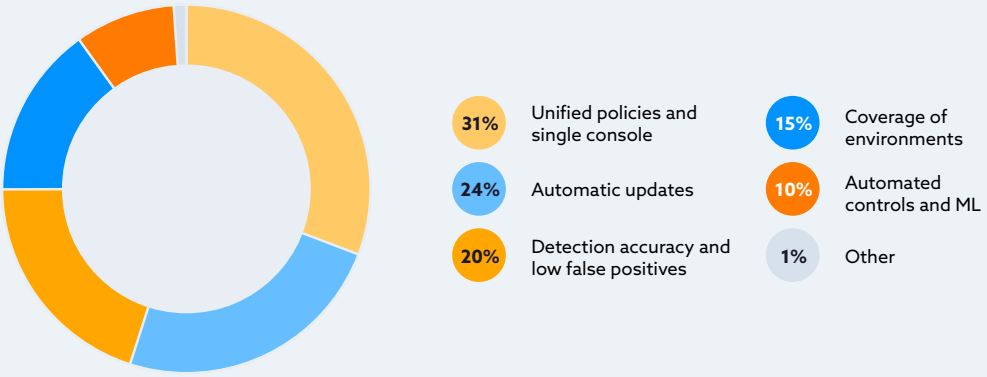
Top challenges with legacy enterprise DLP

The top challenge for organizations when it comes to legacy enterprise DLP solutions is management (29%). This is unsurprising since organizations are often using two or more solutions. Another common challenge is receiving too many false positives (19%), which speaks to issues with fine-tuning the product to meet the organization's needs. Manual version upgrades (18%) was the third most common challenge, which can cause additional strain when managing the product. Deployment complexity was also a challenge for 15% of organizations which may be caused by the use of multiple solutions and contribute to the management difficulties reported earlier.



Features desired in new data protection solutions

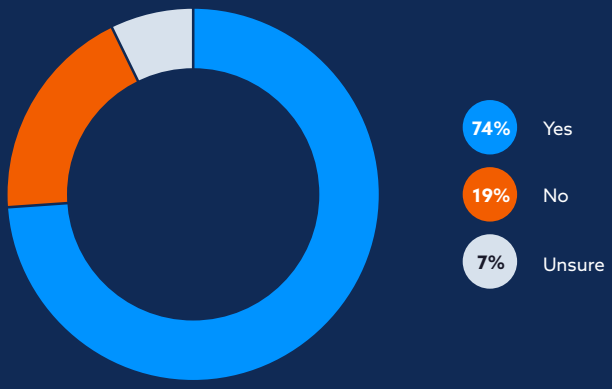
Organizations, as a direct response to the challenges they experience, are looking for DLP and data protection solutions that resolve these issues. Unified policies and a single console (31%) will help organizations with management difficulty and deployment complexity. Automatic updates (24%) avoid additional manual work and reduce the difficulties of management. Also, detection accuracy (20%) reduces the number of false positives. In sum, organizations are looking for data protection solutions that address their current pain points.



Zero Trust and DLP

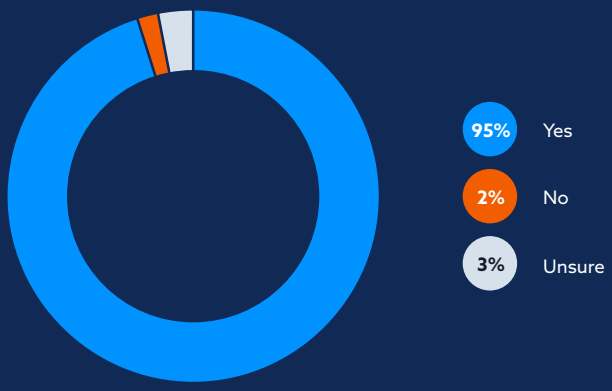
Use of a Zero Trust strategy

Zero Trust has been trending in the industry for the past few years. Unsurprisingly, organizations have taken a keen interest in implementing their own Zero Trust strategy (74%). This doesn't indicate that all these organizations have fully implemented their strategy, but rather that they have created one.



DLP integration into Zero Trust strategy

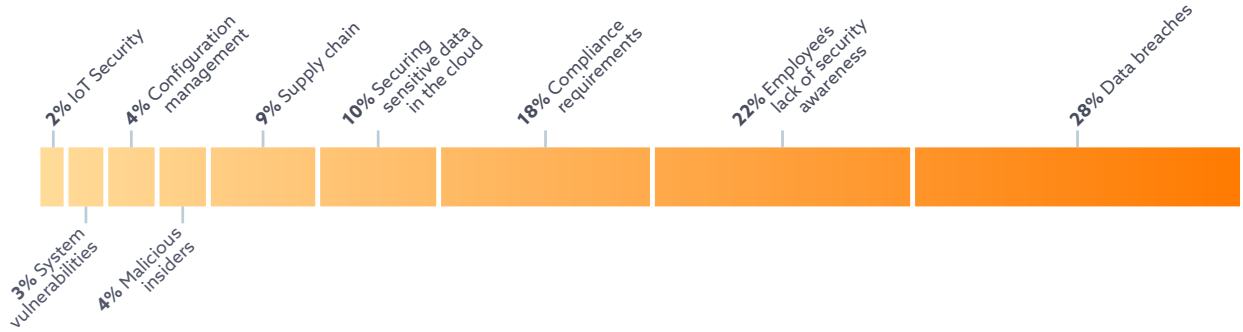
Data protection is a key pillar of any Zero Trust strategy. It is therefore also unsurprising that many organizations include their DLP solution as a part of their overall Zero Trust strategy (95%).



Pain Points and Challenges

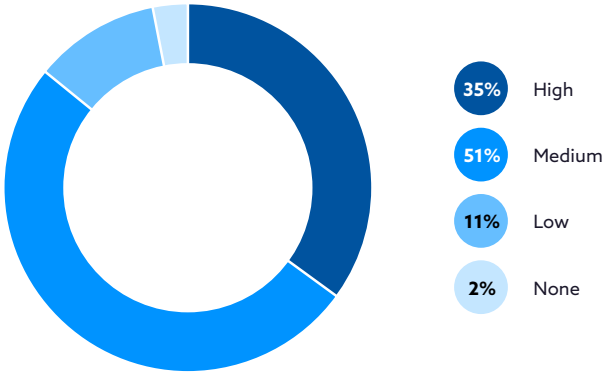
Top security concerns

The top three security concerns for organizations are as expected. The most commonly selected were data breaches (28%), followed by employees' lack of security awareness (22%), and compliance (18%). Data breaches have been a top concern for decades, but preventing data breaches have only become more complex with growing attacks surfaces in cloud-first environments. Now security has become everyone's role in the organization making security awareness and reduction of human error all the more important. Particularly with the amount of access employees and contractors throughout the supply chain have to sensitive data.



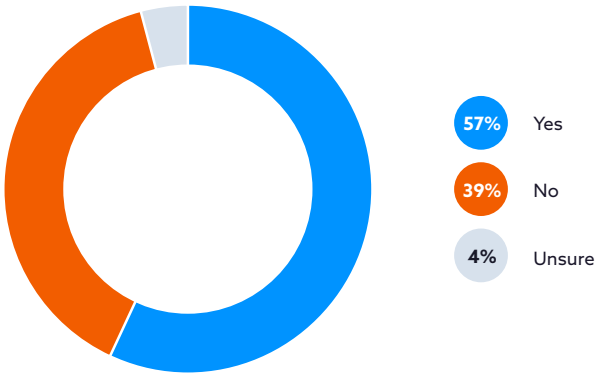
Difficulty finding policy templates

Most employees are having a difficult time finding policy templates for their organization (86%). Over a third reported this to be highly difficult, and over half reported this task to be of moderate difficulty. Only 13% indicated that finding policy templates was of low or no difficulty. This difficulty could be due to infrequent use.



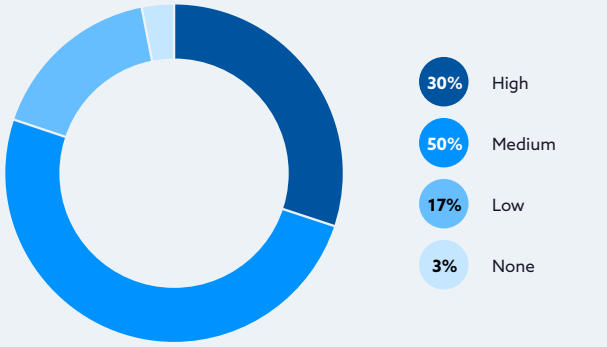
Security incidents over the past year

The majority of organizations (57%) report having experienced a significant security incident in the past year. It's important to note that these are incidents, not necessarily breaches. Thirty-nine percent have not experienced an incident and only 4% reported they were unsure.



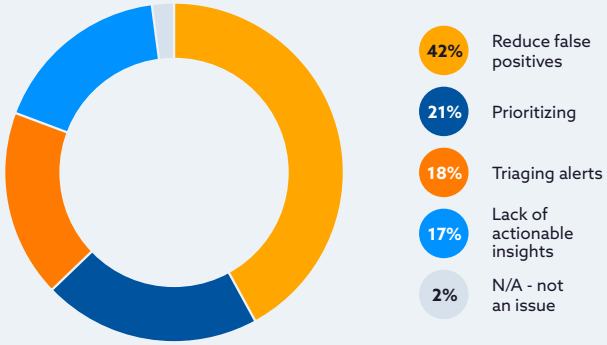
Difficulty of managing false positives

Most employees are having difficulty managing false positives for their DLP solution(s) (80%). Under a third reported this to be highly difficult and exactly half reported this task to be of moderate difficulty. Only 20% indicated that managing false positives was low or of no difficulty. These levels of difficulty are consistent with it being a top challenge with legacy enterprise DLPs.



Challenge of reducing false positives

The top challenges organizations encounter with false positives center around fine-tuning the DLP tool to reduce false positives (41%). Other common challenges include prioritizing (21%), triaging alerts (18%), and lacking actionable insight (17%). Only 2% report false positives aren't a challenge. This speaks to the complexity of many DLP products.



Data governance challenges ranked

Organizations find data governance related to data types (e.g., images, links, mobile data) to be the most challenging, followed by data classification (e.g., PII, financial data), data location and determining data risk. The ranking of these challenges follows a natural progression for data governance. Organizations need to understand the type of data and the classification before they can determine the data risk.

1. Data types (e.g., images, links, mobile data)
2. Data classification (e.g., PII, sensitive data, financial)
3. Data location
4. Determining data risk

DLP Strategy with Remote Workers

Percentage of the workforce that is remote

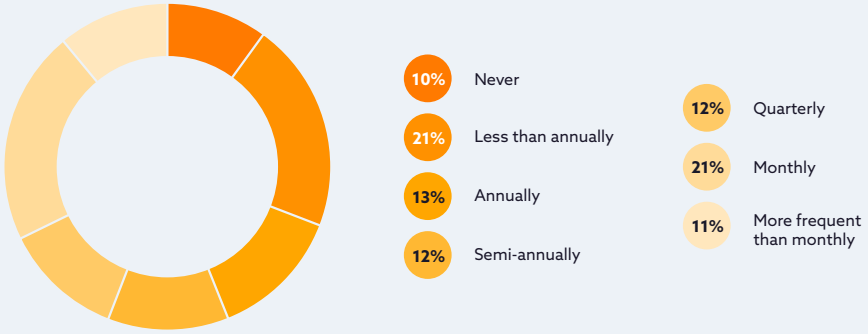
On average, the percentage of the workforce that is remote is 51%. The trend of remote work, while necessary for the recent health crisis, has become more permanent for about half of all employees.

Top security concerns regarding remote workers

The top security concern organizations have regarding remote workers is limited network security (41%). Since remote workers are no longer on the corporate network, network security becomes key to overall security. This is followed closely by unsanctioned data movement (42%). Remote workers may have an easier time accessing personal devices and accounts while performing their work tasks. Other common concerns include phishing scams (33%), device theft (30%), poor visibility into user behavior (30%) and unauthorized device access (30%).

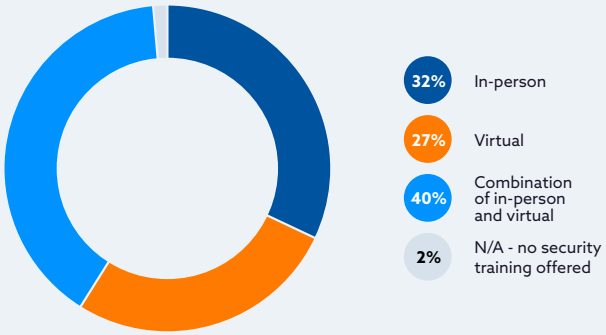
Frequency of security training

Nearly 1/3 of organizations (31%) offer security training less than annually to never. The second most common frequency of security training was monthly (21%). Annually (13%), semi-annually (12%), and quarterly (12%) were less common frequencies for security training. Finally, there were 11% that reported offering training more frequently than monthly. It is likely that these trainings are offered frequently but not required regularly for staff.



Delivery method for security training

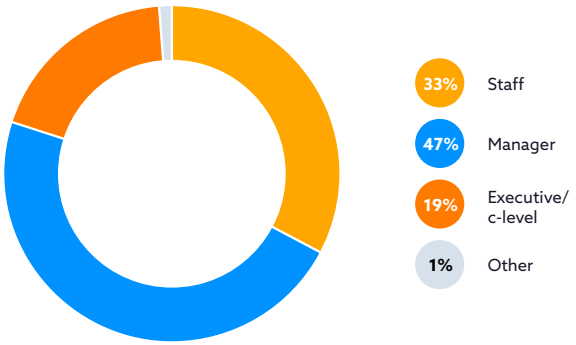
Organizations that provide security training prefer a combination of in-person and virtual security training (40%). For organizations only offering a single method in-person training (32%) is still preferred slightly over virtual (27%).



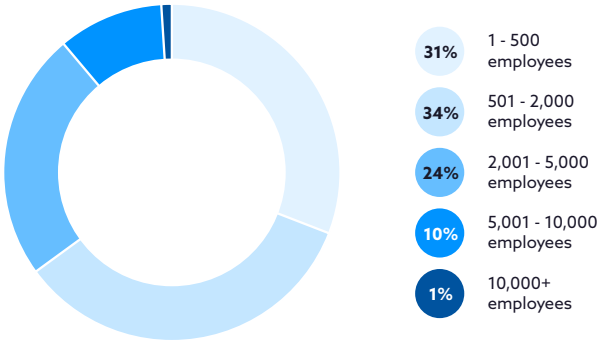
Demographics

The survey was conducted online by CSA in October and November of 2022 and received 2673 responses from IT and security professionals from organizations of various sizes and locations.

What is your primary role?



What is the size of the organization you work for?



Which best describes the region you live in?