

ManageEngine 

REPORT

2023 CLOUD SECURITY OUTLOOK



Table of Contents

Introduction	2
The rise of multi-cloud	5
The cloud security threat landscape	6
Are small SOCs enough?	8
The great CASB	9
Cloud security strategy and solutions	11
Cloud security 2023 outlook: Predicted trends based on the survey findings	13
Conclusion	16
About ManageEngine	17

INDEX

Introduction

The cloud landscape has grown significantly over the past decade due to which many organizations are making the shift to the cloud. The rapid cloud adoption is partly because of the cloud's efficiency and partly because remote and hybrid work has become the norm following the pandemic. Following the increase in cloud adoption, the surface area for attacks grew and the different ways in which attacks could be executed also expanded, but due to the lift and shift approach that many organizations followed, negligible attention was given to cloud security. This left many vulnerable to threats and data breaches, which impacted both the finances and reputations of organizations.

Organizations have since opted for cloud security tools such as cloud access security brokers (CASB) to obtain visibility into their cloud network and prevent further attacks. But a CASB tool alone isn't enough to adequately protect an organization from all kinds of threats; integration with other security tools is what the market currently demands. Is consolidation the way forward?

To understand the cloud landscape and the market demand for cloud security tools, we conducted a survey with [Censuswide](#).

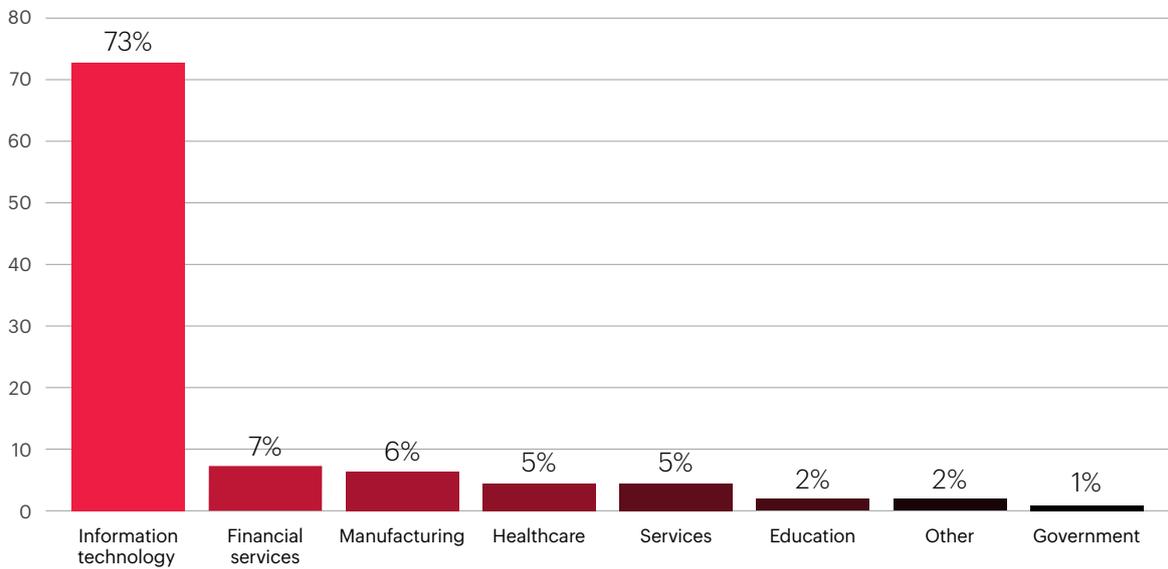
We surveyed

500+

IT professionals in the United States spanning various industries, including healthcare, financial services, manufacturing, and government.

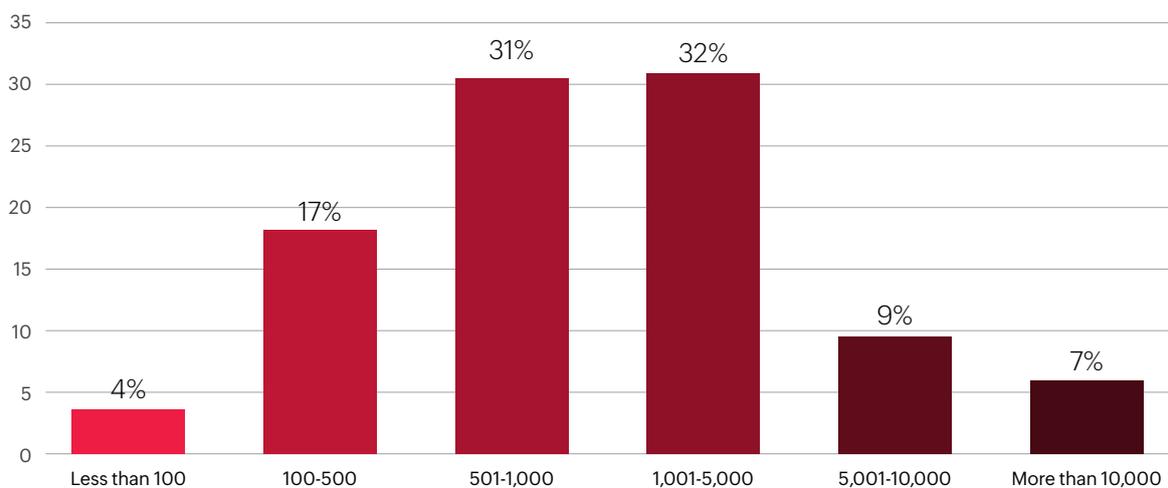
Industry

Q. Which industry does your organization fall under?



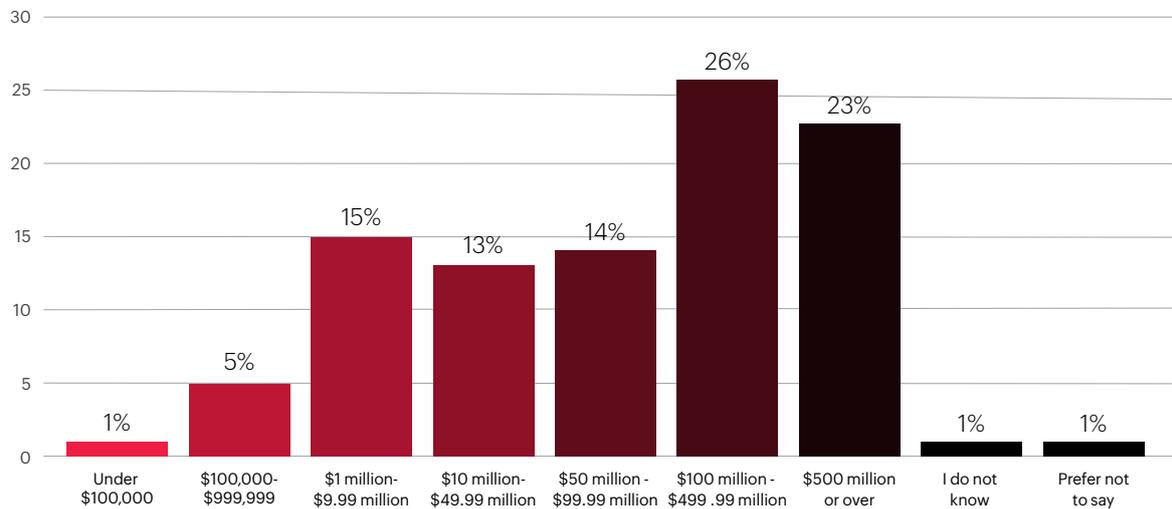
Company Size

Q. How many employees work at your organization?



Company turnover

Q. Approximately what is your company's average annual turnover?



The survey included a total of 20 questions, which addressed cloud usage in the surveyed organizations, cloud security budgeting and resources, cloud security tool usage, what organizations expect and prioritize from CASBs, and what cloud security threats organizations consider the most impactful. This report contains our findings.



The rise of multi-cloud

It takes a team to detect and secure the network from threats—not just in terms of security analysts and IT resources, but in terms of tool capabilities as well.

72%

of surveyed organizations opt for multi-cloud applications.

5%

have deployed a hybrid cloud system.

23%

plan to adopt cloud computing within the next 24 months.

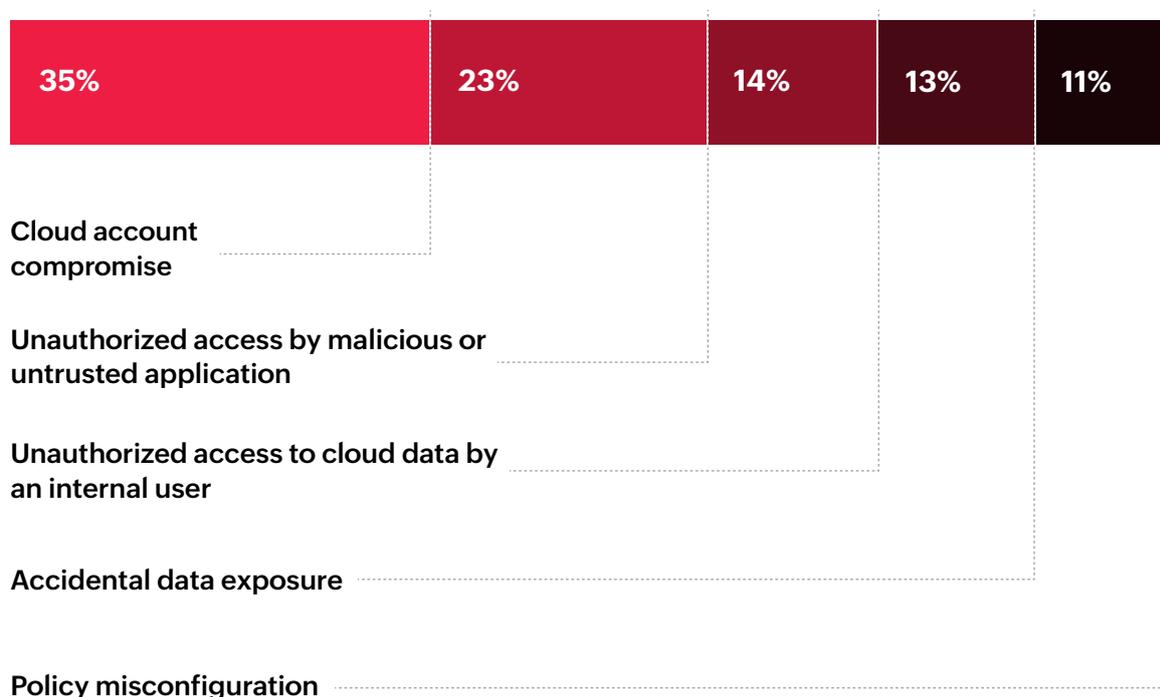
Organizations opt for multi-cloud applications due to the vendor-specific capabilities that each service provider offers and to avoid a concentration of data within one cloud platform. But this can make it tough to form one concise cloud security strategy for all platforms, as each cloud service provider (CSP) has its own set of security policies that need to be adhered to.

The cloud security threat landscape

Organizations flocked to the cloud because of its scalability. However, this also increased the probability of cyberthreats, as the urgency to shift to the cloud took precedence over implementing cloud security strategies. This left organizations vulnerable to cyberattacks that impacted their reputations and finances.

Survey participants were asked:

What, if anything, do you believe is the most common and impactful cloud security threat?



Thirty-five percent of survey respondents believe that cloud account compromise is the most impactful cloud security threat. This is followed by unauthorized access by external malicious or untrusted application (23%) and internal users (14%). **Together, identity-based security threats are the top most impactful cloud security concerns.**

Following the shift to cloud, identity-based attacks surged, likely as a result of the surge in cloud users and identities across organizations to accommodate remote and hybrid work environments. Furthermore, identities are easier to target than perimeter security systems, as these systems have several layers of protection that make it tough for the attacker to bypass. Users are an easy target, because something as simple as a phishing email is often enough for the threat actor to gain access to the network.

It is for this reason that organizations find cloud account compromise and unauthorized access to be the most impactful cloud security threats.

US firm, Civicom, suffered a data breach when it left its Amazon S3 bucket open and accessible without user authentication processes in place. The misconfigured S3 bucket left over 100,000 customer video and audio files exposed—the total equating to over 8TB of data. The breach exposed thousands of hours of private conversations between Civicom clients, along with personally identifiable information (PII) such as full names and images of clients' employees.

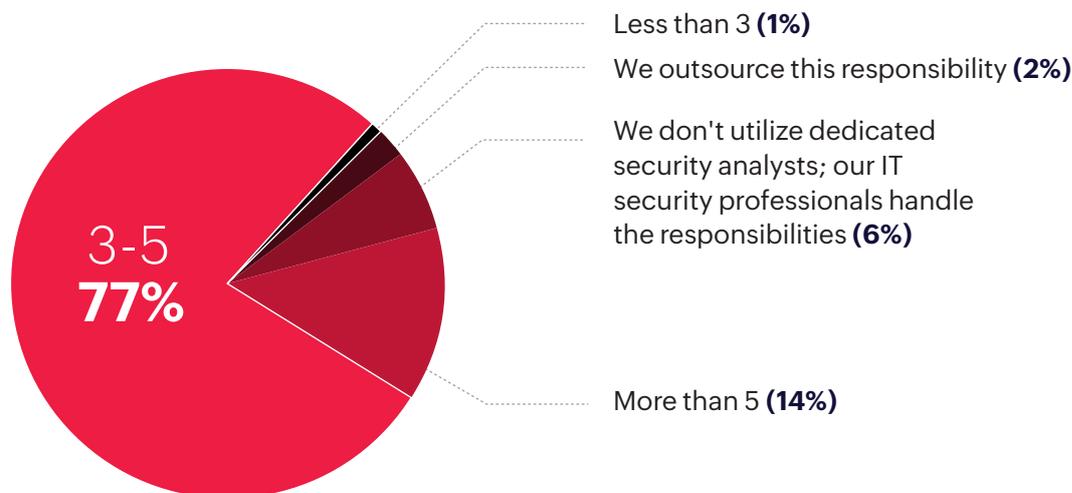
This incident highlights the way in which threats such as unauthorized access can impact an organization. The attack did not just affect Civicom's reputation, but also the privacy of its clients. This goes to show just how easy it can be for attackers to gain access to a network and how important it is to have a cloud security strategy in place to detect and prevent attacks.

Are small SOCs enough?

It takes a team to secure a network from threats effectively. However, only 14% of surveyed organizations have more than five security analysts in their SOC. Six percent don't have dedicated security analysts to devise security strategies and 2% outsource the task.

Survey participants were asked:

How many security analysts are there in your security operations center?



A network has various endpoints that need continuous monitoring—it requires continuous monitoring of systems, users, and the access of resources within the network. SOCs also need to not only ensure data and network security, but also meet compliance requirements, which can be hard for a small SOC team.

Furthermore, a majority of organizations have adopted multi-cloud applications, and each cloud service provider follows their own security policies. This makes it hard to form one concise security strategy, which is why many organizations make the use of a CASB tool.

The great CASB

According to [Gartner](#), CASBs are "on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement."

[The functionalities of a CASB](#) can be divided into four pillars: visibility, threat detection, data security, and compliance. It is these functions that make a CASB a crucial element of an organization's cloud security strategy.

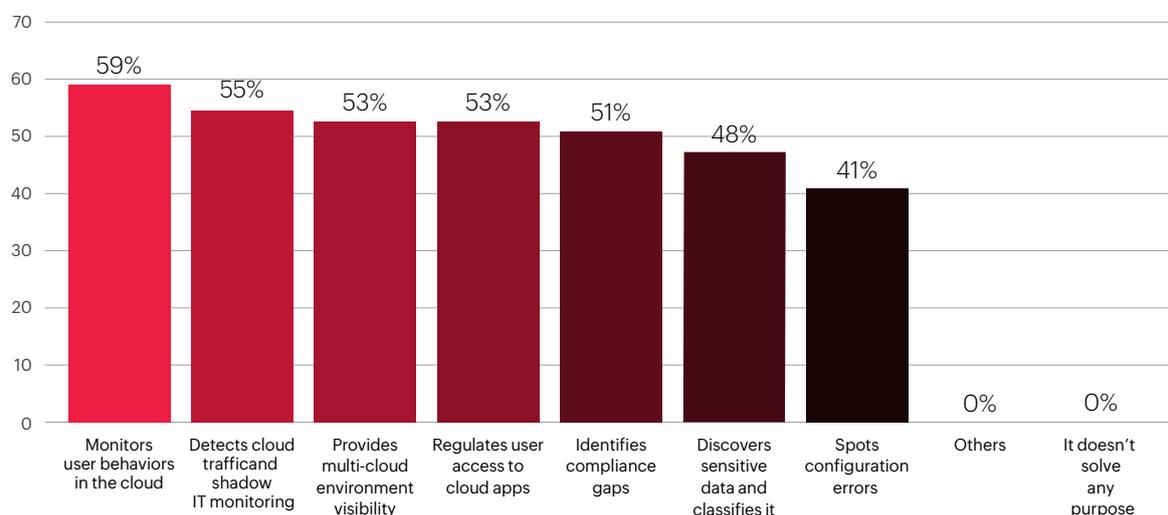
96%

of organizations surveyed used a CASB solution to secure their cloud security architecture

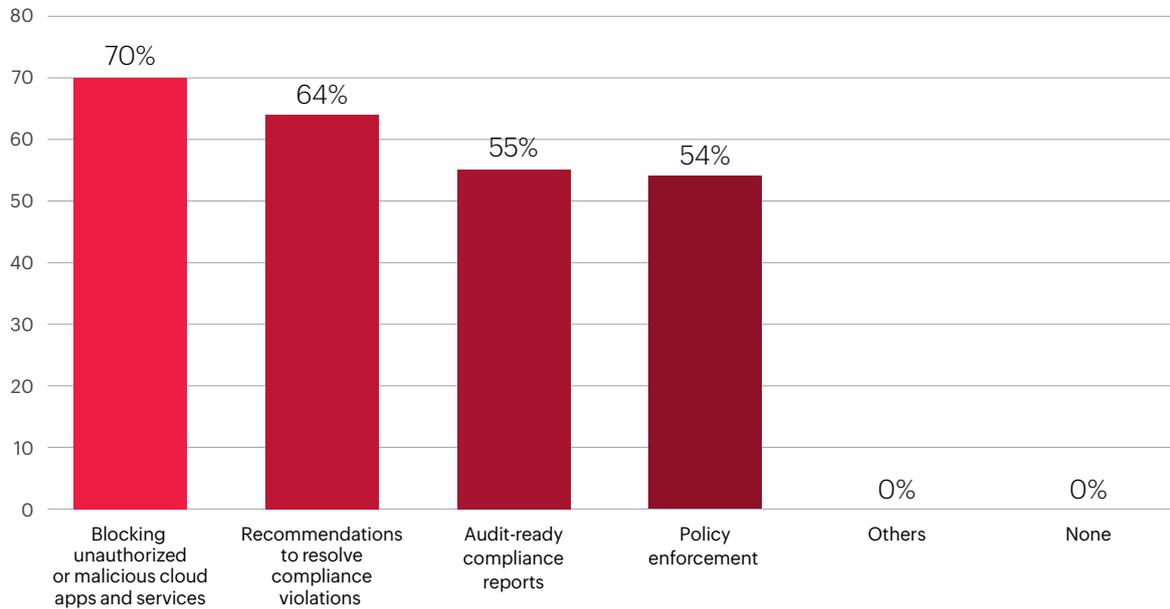
Out of this percent, 70% use a cloud-hosted CASB tool and 30% have deployed the solution on-premises.

Survey participants were asked the following questions:

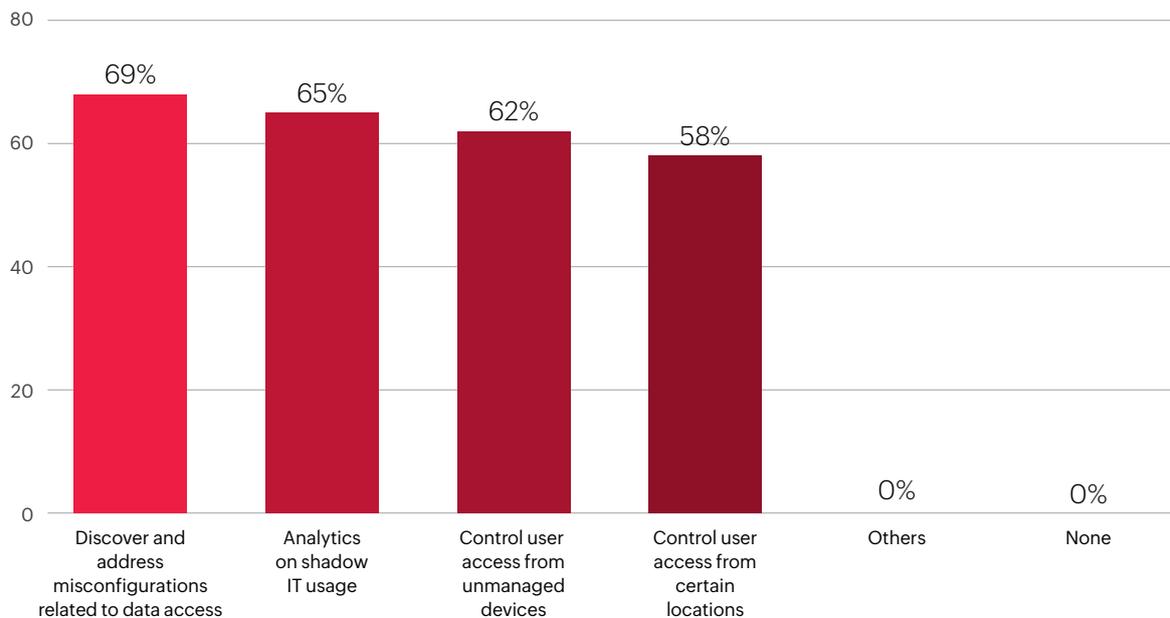
What purpose does your CASB solution solve?



What are the most important compliance capabilities of your CASB solution?



What are the most important security control capabilities of your CASB solution?

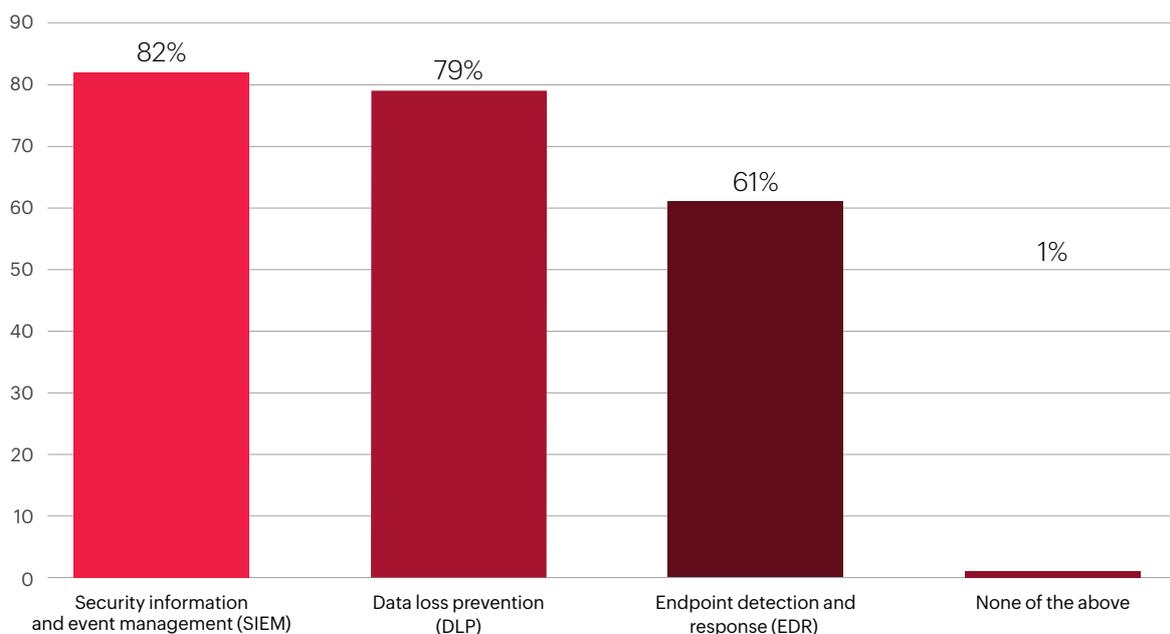


Cloud security strategy and solutions

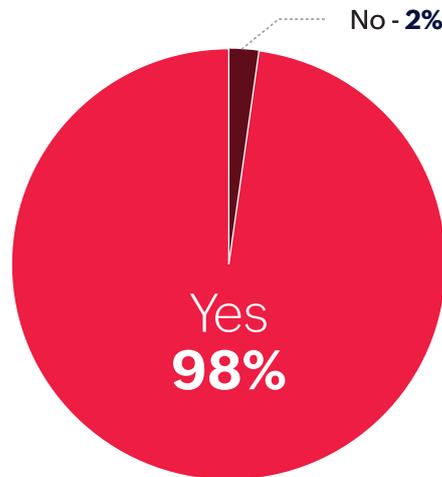
Multi-cloud adoptions seem to be here to stay, so it's imperative to implement a security strategy that provides visibility into the different cloud platforms, monitors data movement across all platforms, defends against internal and external threats, and adheres to compliance regulations simultaneously. Most organizations make use of different tools in order to perform these various functions.

Survey participants were asked the following questions:

Which of the following security solutions, if any, do you use in your organization?



Do you monitor your users' accesses to data stored in the cloud?



CASBs consolidate these various functions—they offer visibility into the different cloud environments and help with adhering to compliance mandates, securing data, and protecting against threats, becoming an integral part of cloud security architecture. But a CASB tool alone isn't enough to secure a network, as it only monitors the cloud. The market therefore demands integration and orchestration of CASBs with other tools to create a strong cloud security architecture.



Cloud security 2023 outlook:

Predicted trends based on survey findings



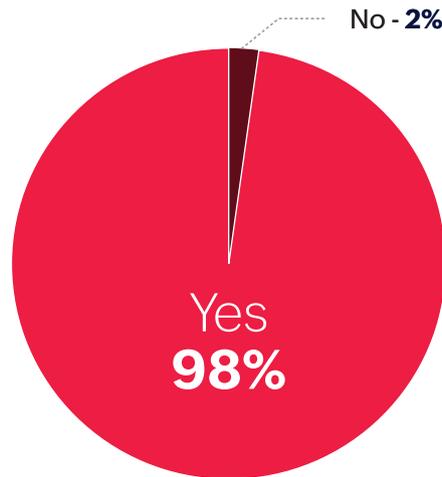
Integration and consolidation

There exists a gap between the demand and available cybersecurity workforce. [The \(ISC\)² Cybersecurity Workforce Study](#) states that though the workforce is increasing rapidly (the cybersecurity workforce stands at 4.7 million in 2022, a 11.1% increase compared to the previous year and the highest number recorded to date), the demand for it is growing much faster, fuelled by the rapid shift to cloud. As the cyber space grows, so does the surface area for attackers, and organizations need a team just as big to tackle the various threats looming over the horizon.

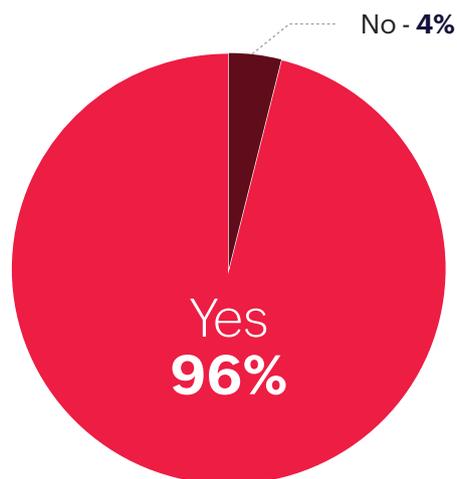
The study also states that the cybersecurity workforce gap has increased by 26.2% in 2022. This gap needs to be filled, and one way to do it is through consolidation. Ninety-four percent of those surveyed stated that they use different security tools to cover the different aspects of their cloud security strategy. Ninety-six percent of surveyed organizations stated that they would evaluate a solution that performs all functions from a single console.

Survey participants were asked the following questions:

Do you use different security tools to protect data, monitor user access, adhere to compliance mandates, and gain visibility into activities in cloud platforms?



Will you be evaluating a solution that can perform all these functions from a single console?



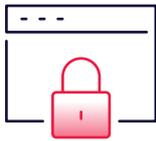
Consolidation of security infrastructures and integration of CASB with other security solutions such as SIEM is a way to improve cloud resiliency and reduce workload.



Budgeting ahead of recession

In light of the likely global recession in 2023, organizations should be prepared for budget cuts and tighter expenses. However, a lower budget and fewer resources in an organization's SOC leaves for many vulnerabilities.

Consolidation again plays a factor here, where it offers increased visibility, operational efficiency, and improves the internal bandwidth to leave space for fewer errors and vulnerabilities.



Data protection laws

US states like California, Utah, Colorado, Virginia, and Connecticut are introducing data privacy laws that are to be enacted from 2023, and many states are looking to follow. While data and privacy laws already exist in the US, they more or less pertain to specific industries. This new set of laws projects a trend of protecting user's general right to privacy rather than specifying the types of data that particular industries can process. This compliance trend can be in light of the numerous data breaches seen in 2022.

Forty-eight percent of those who monitor their cloud access or have hybrid cloud systems deployed said the process of ensuring compliance is highly challenging. Only 16% say they're all sorted. A consolidated security tool that ensures compliance while monitoring the cloud and protecting data is the way forward.

Conclusion

With over 77% of organizations using multi-cloud applications or hybrid deployments and the predicted 2023 recession looming, achieving cloud security resilience has become essential.

Taking into account the large number of threats and attacks that can take place within a network, the large number of resources required to defend against those attacks, and the cybersecurity workforce gap that exists, organizations need a concise, consolidated tool that can provide visibility into the various cloud platforms, defend against threats, protect data, and help with compliance, such as a CASB.

While a CASB effectively protects data in the cloud, it isn't as effective outside of the cloud. A CASB solution alone isn't sufficient to adequately secure a network. To build a strong security architecture, a CASB needs to work in tandem with other security tools such as EDR, SOAR, SIEM, and UEBA to build a strong cloud security architecture and to achieve cloud security resilience.

About ManageEngine

ManageEngine is the enterprise IT management division of Zoho Corporation. Established and emerging enterprises — including 9 of every 10 Fortune 100 organizations — rely on ManageEngine's real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine has offices worldwide, including the United States, the Netherlands, India, UAE, Mexico, Singapore, Japan, China and Australia, as well as 200+ global partners to help organizations tightly align their business and IT.

For more information, please visit manageengine.com

[Blog](#) | [LinkedIn](#) | [Facebook](#) | [Twitter](#)

ManageEngine SIEM Solutions

[ManageEngine Log360](#)

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 is also available as a cloud deployment ([Log360 Cloud](#)) that provides SIEM functionalities as a service. It can detect, prioritize, and resolve security incidents; and help you comply with regulatory mandates-all from the cloud.

[ManageEngine EventLog Analyzer](#)

EventLog Analyzer is the log management component of Log360 that can collect, analyze, correlate, and securely store log data, and perform threat analytics to spot and mitigate security incidents.

[ManageEngine ADAudit Plus](#)

ADAudit Plus is the security auditing component of Log360 that monitors and audits Active Directory environment to detect, analyze, and mitigate internal security threats, and monitor GPO changes. It is a UBA-driven auditor that helps keep your AD, Azure AD, file systems (including Windows, NetApp, EMC, Synology, Hitachi, and Huawei), Windows servers, and workstations secure and compliant. ADAudit Plus transforms raw and noisy event log data into real-time reports and alerts, enabling you to get full visibility into activities happening across your Windows Server ecosystem in just a few clicks.

✉ Support Email: support@log360.com

☎ Direct Inward Dialing: **+1-408-352-9254**

Toll Free Numbers

🇺🇸 US: +1 844 649 7766

🇬🇧 UK: 0800 028 6590

🇨🇦 CN: +86 400 660 8680

🇺🇸 Intl: +1 925 924 9500

🇦🇺 AUS: 1800 631 268