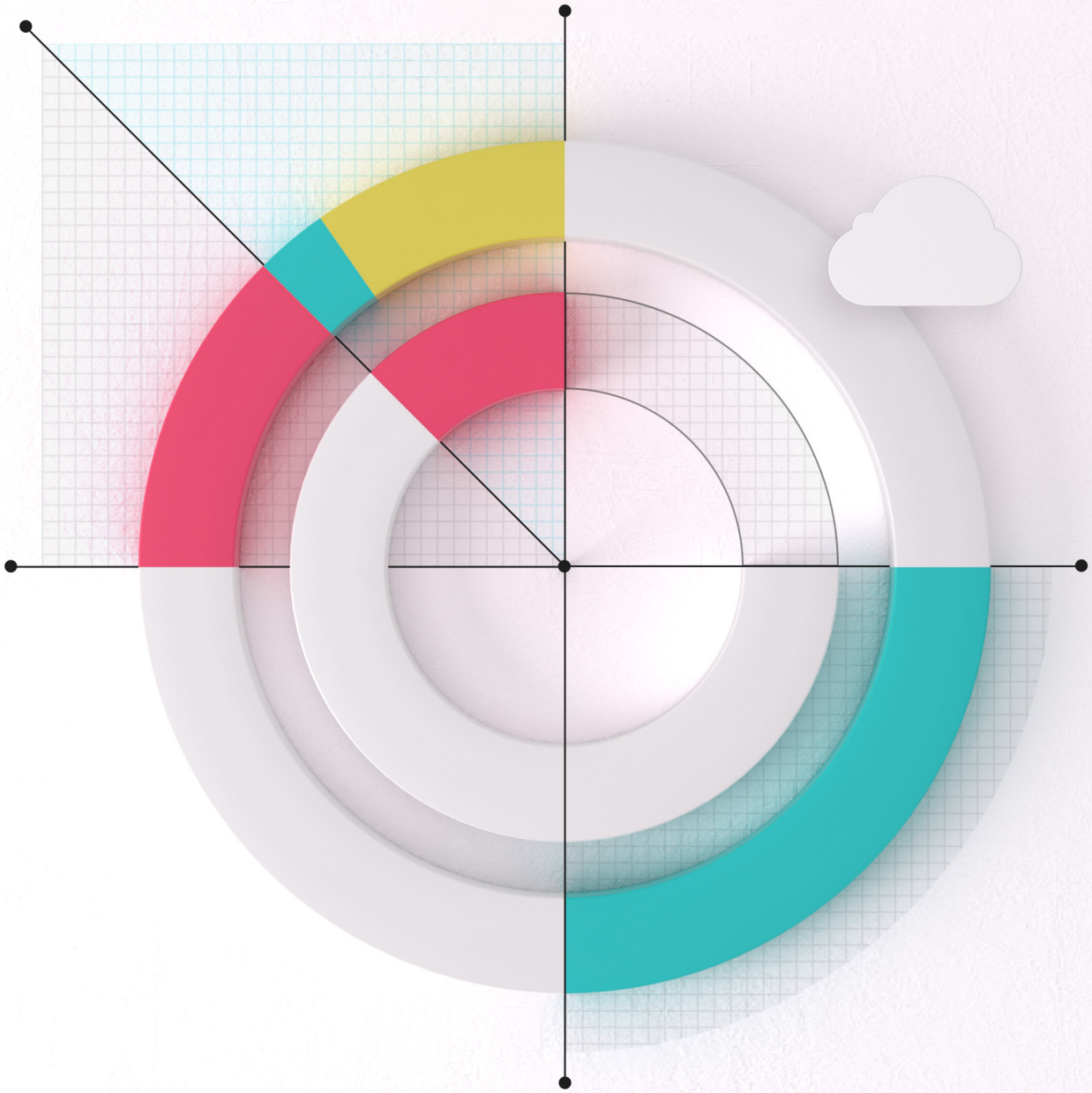
The Annual SaaS Security Survey Report

2024 Plans and Priorities



Contents

Key Findings

1 SaaS Security Incidents on the Rise

55% of organizations report that they experienced an incident in the past two years, with another 12% unsure. These findings underscore that companies are coming to understand the harsh reality that common on-prem types of attacks, such as ransomware, malware, and data breaches, can also occur in their cloud SaaS environments.

2 Current SaaS Security Strategies and Methodologies Don't Go Far Enough

The survey finds that over half (58%) of organizations estimate their current SaaS security solutions only cover 50% or less of their SaaS applications. It's becoming clear that manual audits and CASBs are not enough to protect companies from SaaS security incidents.

3 Stakeholder Spread in Securing SaaS Apps

CISOs and security managers are shifting from being the controllers to governors as the ownership of SaaS apps are spread out through all the different departments of their organization. Alignment, communication and collaboration are key to being able to secure the organization's SaaS stack.

4 How Organizations Are Prioritizing Policies & Processes for Their Entire SaaS Security Ecosystem

SaaS security continues to adapt to encompass the expanding broad range of concerns in the SaaS Ecosystem, including SaaS Misconfigurations, SaaS-to-SaaS Access, Device-to-SaaS Risk Management, Identity and Access Governance, and Identity Threat Detection & Response (ITDR). Organizations are putting robust policies, processes, and capabilities in place that are essential for protecting these different domains.

5 Investment in SaaS and SaaS Security Resources Are Drastically Increasing

66% of organizations have increased their investment in apps, with 71% increasing their investment in security tools for SaaS. More specifically, the survey shows that adoption of SaaS Security Posture Management (SSPM) solutions has grown significantly, increasing from 17% in 2022 to 44% in 2023. This can be attributed to the fact that SSPMs provide coverage in areas where other methods and strategies have fallen short, offering more comprehensive protection against various security risks throughout the whole SaaS Security Ecosystem.

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.

Adaptive Shield commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding SaaS application use, SaaS security policies and processes, SaaS threats, and SaaS security strategy/solutions. Adaptive Shield financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in March of 2023 and received 1130 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 primary objectives of the survey were to gain a deeper understanding of several critical aspects of SaaS security in organizations.

- Current SaaS application use in organizations
- Organizations' security policies and processes regarding SaaS applications
- Awareness and experience with SaaS threats
- Current and future use of security solutions

Data & Discussion

In today's digital landscape, SaaS security is of critical importance for organizations of all sizes. As businesses increasingly move their operations and data to the cloud, or more specifically – SaaS applications, the security of these apps becomes paramount. While SaaS applications are secure by design, the way they are configured and governed is what poses a risk. Without proper security measures, organizations are exposed to data breaches, cyber-attacks, and other security incidents that can result in significant financial and reputational damage. Understanding SaaS security is therefore essential for organizations to protect themselves from these risks.

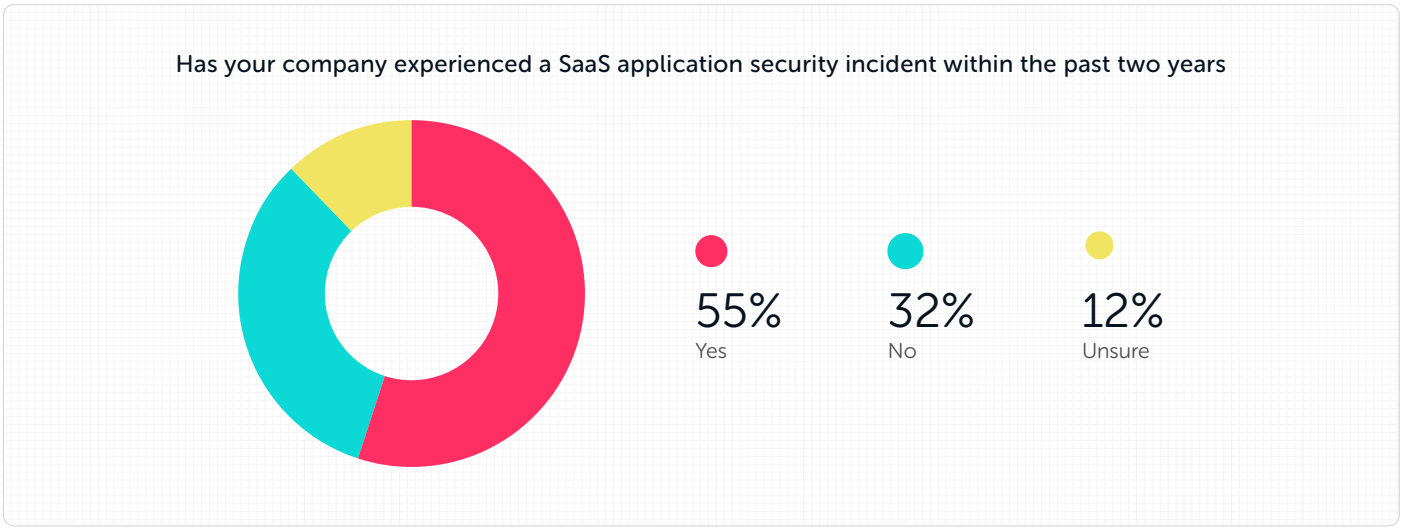
It's with this backdrop that this survey returns, delving into the intricacies of SaaS security and offering a follow-up to last year's report. Below are this year's findings and insights.

Key Finding #1

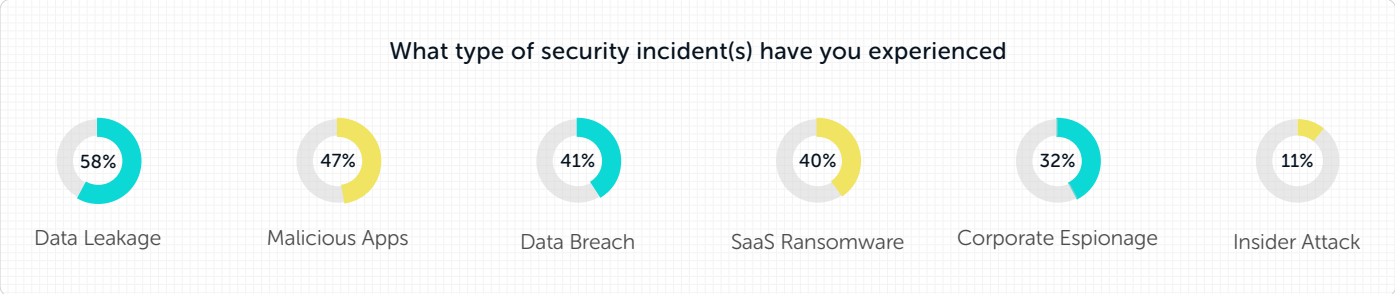
SaaS Security Incidents on the Rise

The survey reveals a significant increase in security incidents within the SaaS ecosystem, with 55% of organizations reporting that they experienced an incident in the past two years, up 12% from the previous year. About a third (32%) of respondents stated that they hadn't encountered a SaaS security incident within the same period, while 12% were unsure.

The findings underscore that many companies are coming to understand the harsh reality that common on-prem types of attacks, such as ransomware, malware, and data breaches, can also occur in their SaaS environments.



Among the most prevalent SaaS security incidents reported were data leakage (58%), malicious apps (47%), data breaches (41%), and SaaS ransomware (40%), highlighting the growing need for robust security measures and increased awareness of the potential risks associated with the expanding SaaS landscape.

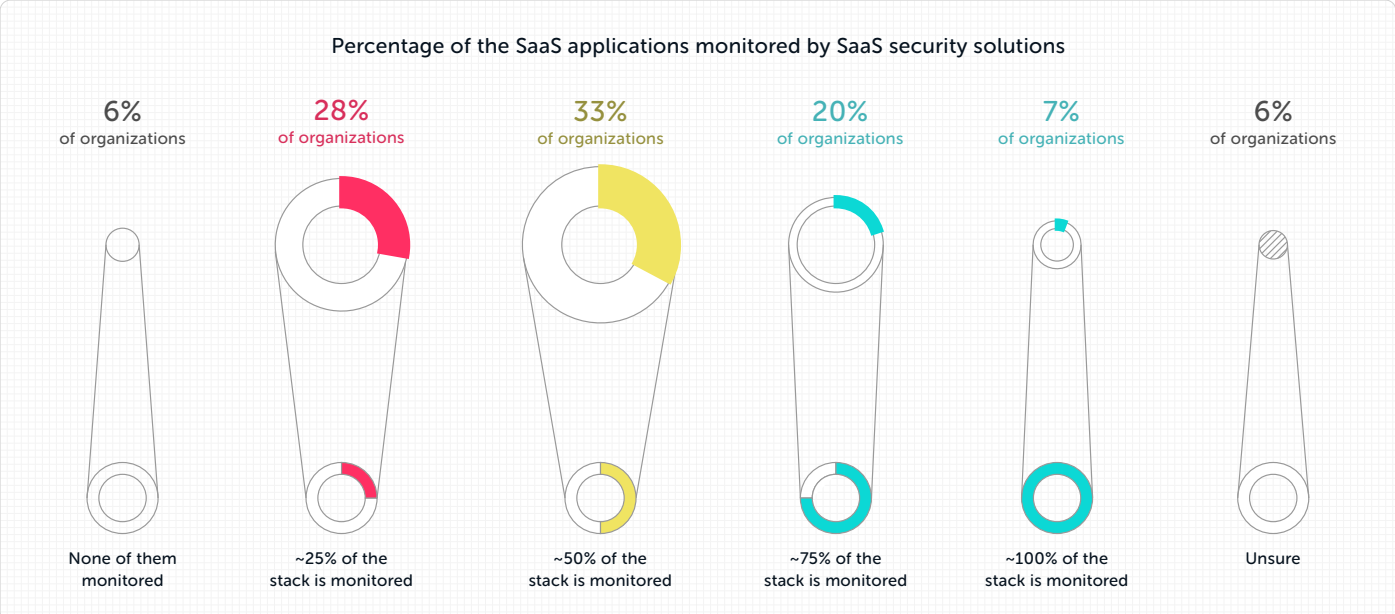


Key Finding #2

Current SaaS Security Strategies and Methodologies Don't Go Far Enough

Insufficient Monitoring of SaaS Applications

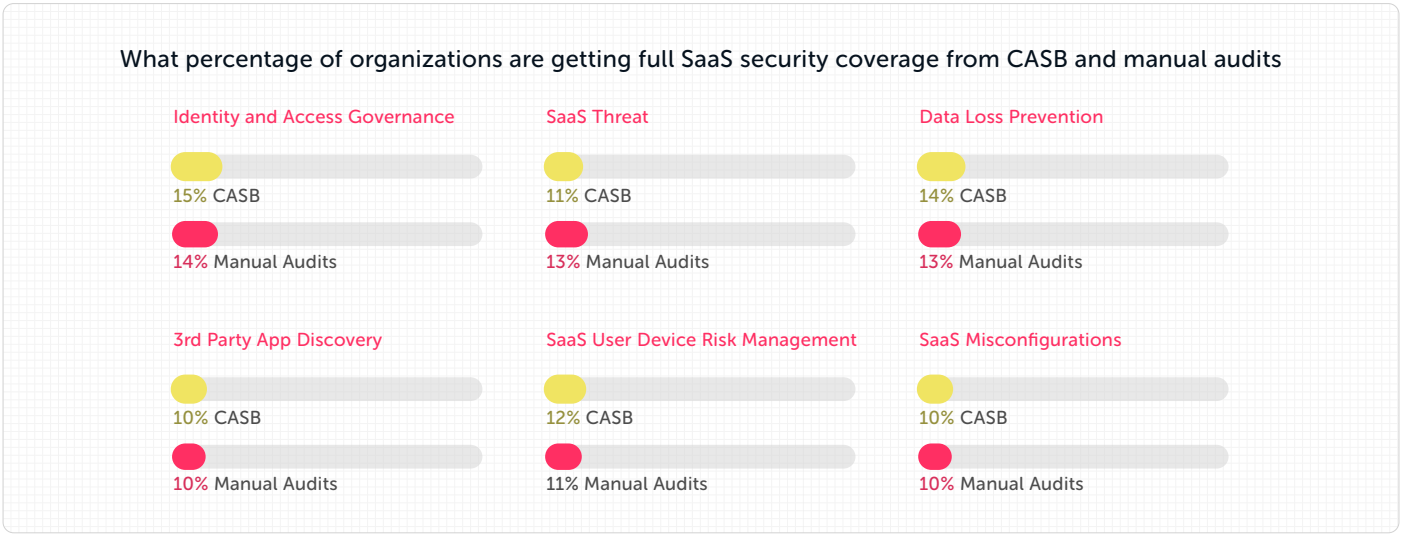
A key contributor to the noted increase in SaaS security incidents, the findings from the survey suggest that a significant number of organizations are falling short when it comes to implementing effective SaaS security measures. Many companies are using security solutions that do not cover their entire SaaS stack, leaving their applications and data exposed to cyber threats. Specifically, the survey found that over half (58%) of organizations estimate their current SaaS security solutions only cover 50% or less of their SaaS applications.



These findings highlight the pressing need for companies to reassess their security solutions and ensure they provide comprehensive coverage across their entire SaaS ecosystem. By doing so, organizations can significantly reduce their risk of security incidents, including data breaches, ransomware attacks, and other types of cyber-attacks. Ultimately, this will help to safeguard their reputation and maintain the trust of their customers.

CASBs and Manual Audits Falling Short for SaaS security

Many organizations rely on Cloud Access Security Brokers (CASBs) and manual audits to secure their SaaS applications. However, these methods are proving to be insufficient in a number of key areas. Additionally, manual audits expose company data between audits, leaving organizations at risk for security incidents during those gaps.



These findings indicate that organizations need to reevaluate their security strategies and invest in more comprehensive solutions and strategies that provide full coverage across their SaaS ecosystem to reduce the risk of security incidents. This is also likely what is contributing to the increased use of SaaS Security Posture Management (SSPM) tools.

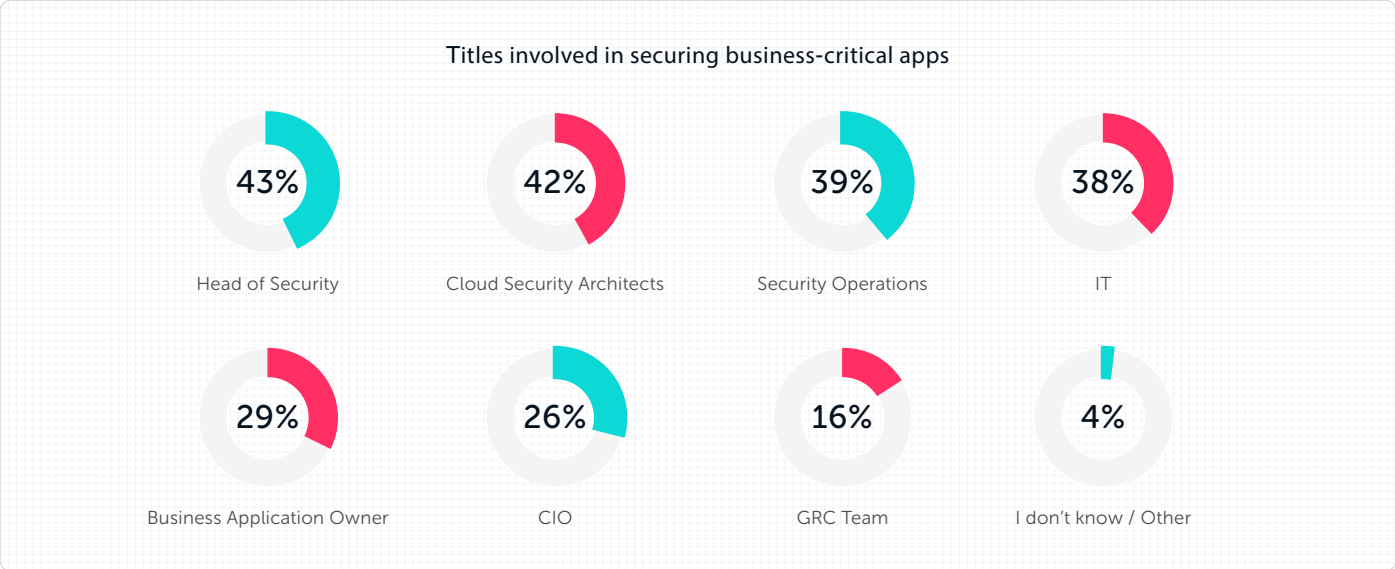
Key Finding #3

Stakeholder Spread in Securing SaaS Applications

In addition to monetary investments in tools, security, and staff, organizations are increasingly involving numerous stakeholders in the process of securing business-critical applications. Across a typical organization, a wide array of SaaS apps are used from file sharing and collaboration apps to CRM, project and work management, marketing automation, and many more. SaaS apps fill a variety of niche roles, yet this stakeholder spread complicates the threat landscape.

Now, CISOs and security managers are shifting from being the controllers to governors of SaaS app security, and the survey shows how many of those engaged in security governance hold executive-level positions or serve as department heads, indicating that businesses are taking SaaS security seriously. The involvement of key decision-makers underscores the growing recognition of the critical role that SaaS security plays in protecting valuable assets and ensuring operational continuity.

However, with so many individuals involved, it can become challenging to determine who is ultimately responsible for SaaS security. SaaS applications often require close collaboration between the security team and app owners, as the security team may not always have direct access to the SaaS app. This necessitates processes and tools that can bridge the gap and actively engage app owners, who are crucial for effective SaaS security management.



By fostering a collaborative environment and implementing solutions or strategies that facilitate communication and coordination between security teams and app owners, organizations can create a more robust and streamlined approach to securing their business-critical applications. This, in turn, will help minimize potential threat and ensure a higher level of protection against the ever-evolving landscape of SaaS security threats.

Key Finding #4

How Organizations Are Prioritizing Policies & Processes for Their Entire SaaS Security Ecosystem

Over the past year, the focus of SaaS security has evolved significantly, driven by factors such as increased investment in business-critical SaaS applications, a rise in security incidents, and the growing number of threat actors targeting SaaS apps. Previously, organizations and security tools, like SSPMs, were primarily focused on misconfiguration management. However, SaaS security has adapted to encompass a broader range of concerns, including SaaS-to-SaaS Access, Device-to-SaaS Risk Management, Identity and Access Governance, and Identity Threat Detection & Response (ITDR).

SaaS Policies and Procedures

With the rising importance of SaaS in the business landscape, having robust policies, processes, and capabilities in place is essential for protecting an organization's SaaS stack and the data it contains from threat actors.

Organizations are now putting measures in place to address key areas. The data below presents what organizations are starting to prioritize when securing their SaaS stack throughout the different domains of the SaaS Security Ecosystem.

Misconfiguration Management

Addressing misconfiguration issues is vital to protect an organization's SaaS stack from misconfigured security settings that can be exploited by threat actors. The main priorities for misconfiguration management of respondents include:

Communication and collaboration between security and app owner teams	Detailed fixes and mitigation of misconfigurations	Prioritization based on the application, security domain, and risk level

With a strong system and process in place, these high-impact areas can help reduce the SaaS attack surface.

Third-Party App Access

As organizations increasingly rely on third-party SaaS applications (apps that are connected to the core stack), it becomes crucial to have policies in place to assess and manage potential risks. The main priorities for 3rd-party app access include:

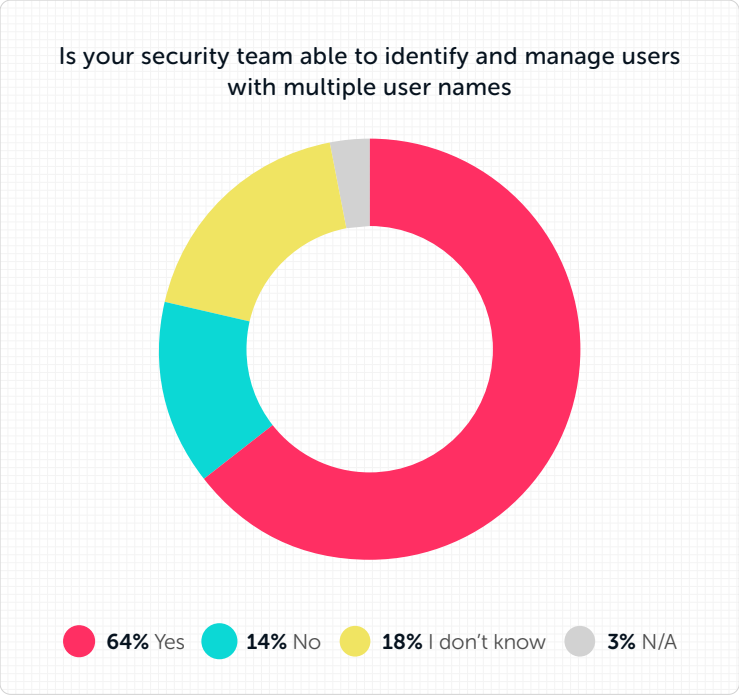
- Search, detect, and quantify risk of connected third-party SaaS applications
- Detect malicious apps that have been integrated into the SaaS stack
- Process for app owners requiring them to submit a request to security before connecting an app

These priorities reflect the need for strong systems and processes in place to protect against third-party app access threats.

SaaS Identity and Access Governance

Proper identity and access governance is essential for safeguarding sensitive data within the SaaS ecosystem. The priorities in Identity and Access Governance in organizations today include:

- Ensure each user has the right level of access needed
- Detect users that have been disabled in the Active Directory but still have access to SaaS applications
- Detect dormant accounts to quickly ensure the deprovisioning of their access to SaaS if needed
- Notification of Admin access
- Authentication practices (e.g., key management, certificate management)

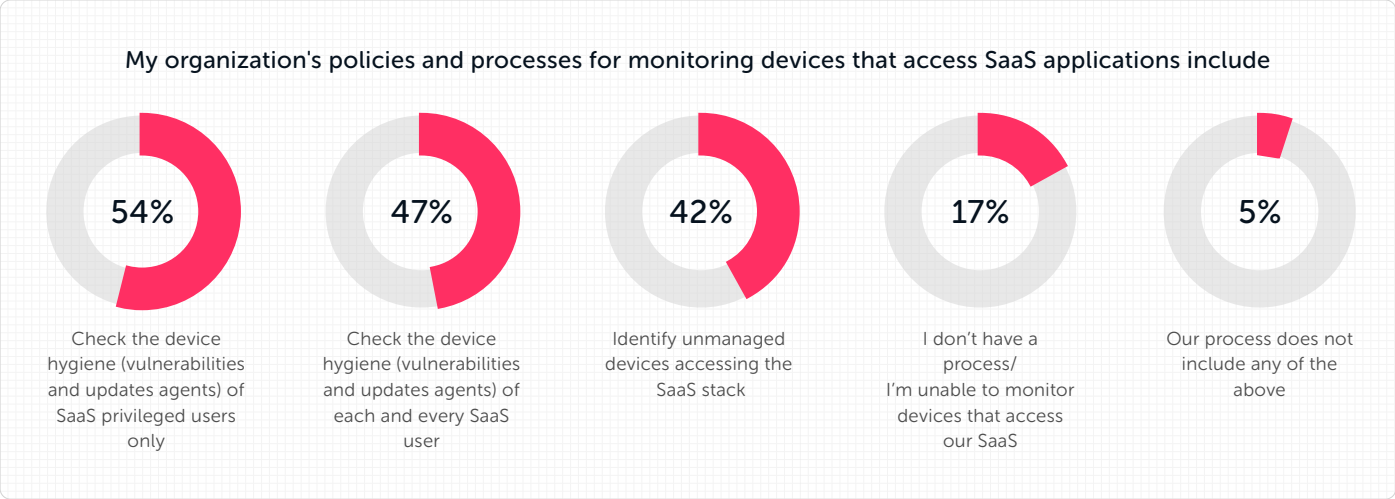


Monitoring SaaS User Devices

Ensuring the security of devices that access the SaaS stack is critical for preventing unauthorized access and data breaches. Organizational priorities for ensuring SaaS risks are not stemming from devices include:

- Checking the device hygiene (vulnerabilities and updated agents) of each and every SaaS user, especially privileged ones
- Identifying unmanaged devices accessing the SaaS stack

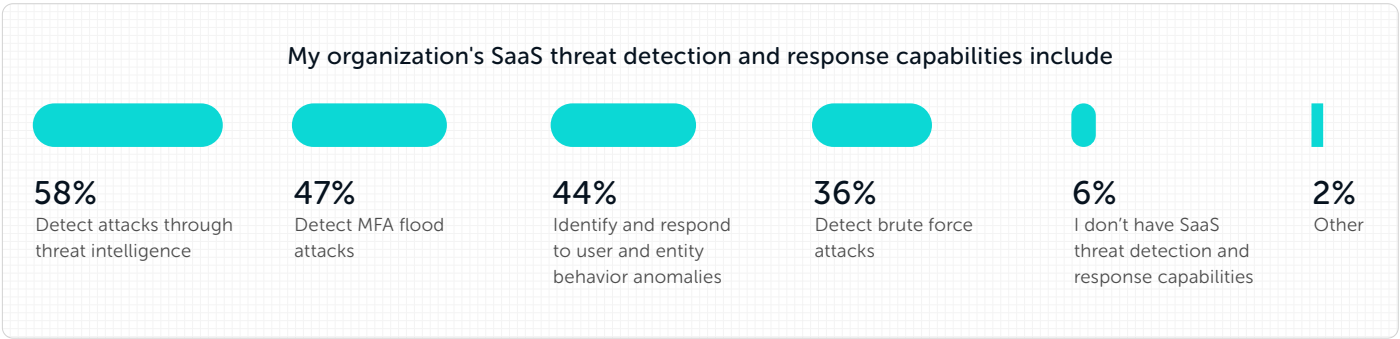
Many don't view devices as a weak spot in their SaaS app security. The opposite is true; devices are a gateway — and if a privileged user's device is not secure, the damage if a threat actor succeeds would be significant.



Threat Detection and Response

Proactive threat detection and response is crucial for defending organizations from targeted attacks. In today's environment, the priorities for threat detection and response are:

- Identify and respond to user and entity behavior anomalies
- Detect MFA flood attacks
- Detect attacks through threat intelligence
- Detect brute force attacks



Key Finding #5

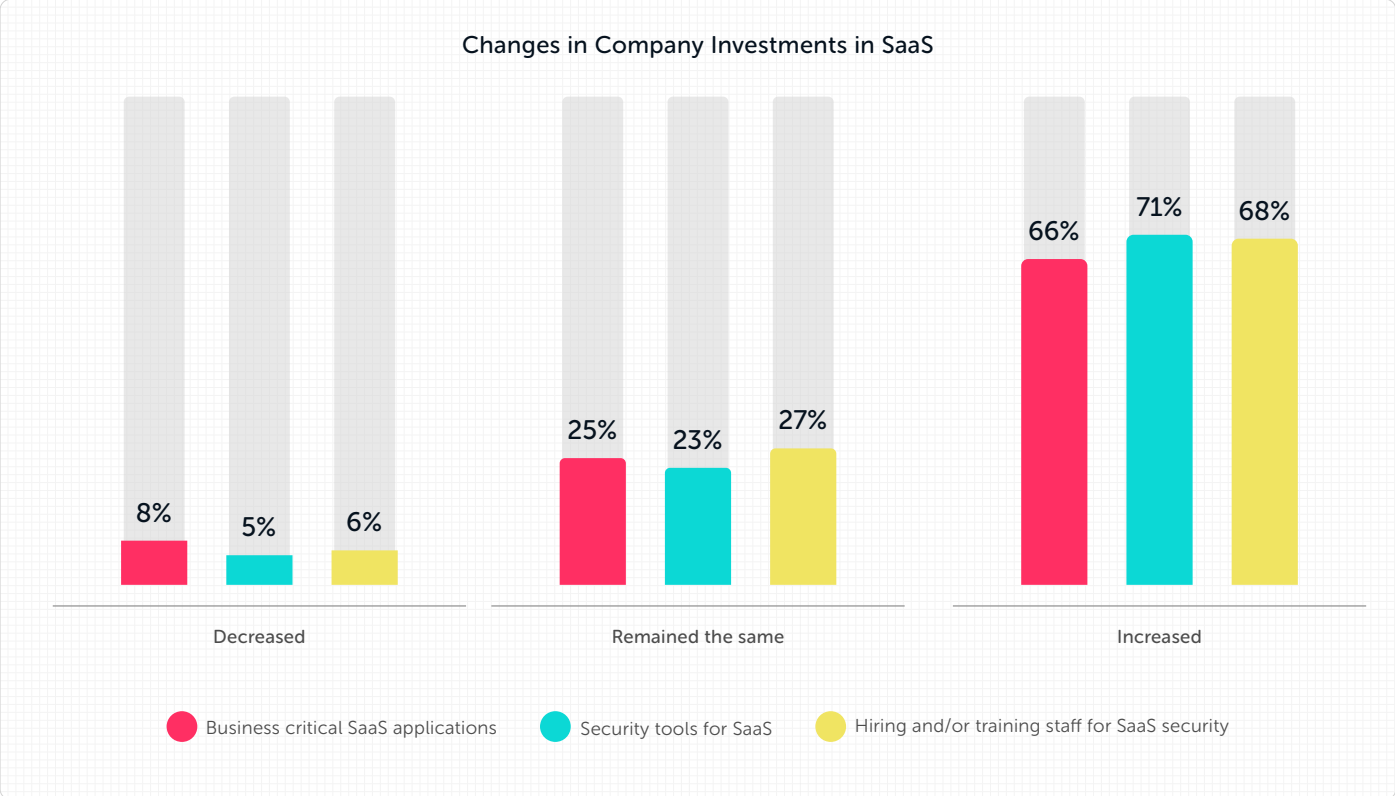
Investment in SaaS and SaaS Security Resources Are Drastically Increasing

Increased Investment in SaaS

Organizations are relying more heavily on SaaS resources, encompassing not just business-critical apps and staff but also the right security tools focused on SaaS security.

According to the survey, 71% of organizations have increased their investment in security tools for SaaS, demonstrating a growing commitment to protecting their digital assets. Furthermore, 68% of organizations have ramped up their investment in hiring and training staff on SaaS security, recognizing the importance of human capital in safeguarding their SaaS ecosystems. Additionally, 66% of organizations have increased their investment in business-critical SaaS applications, reflecting the growing reliance on these tools for core business functions.

This holistic approach to SaaS investment, encompassing security tools, personnel, and applications, underscores the importance of robust security solutions like SSPMs.



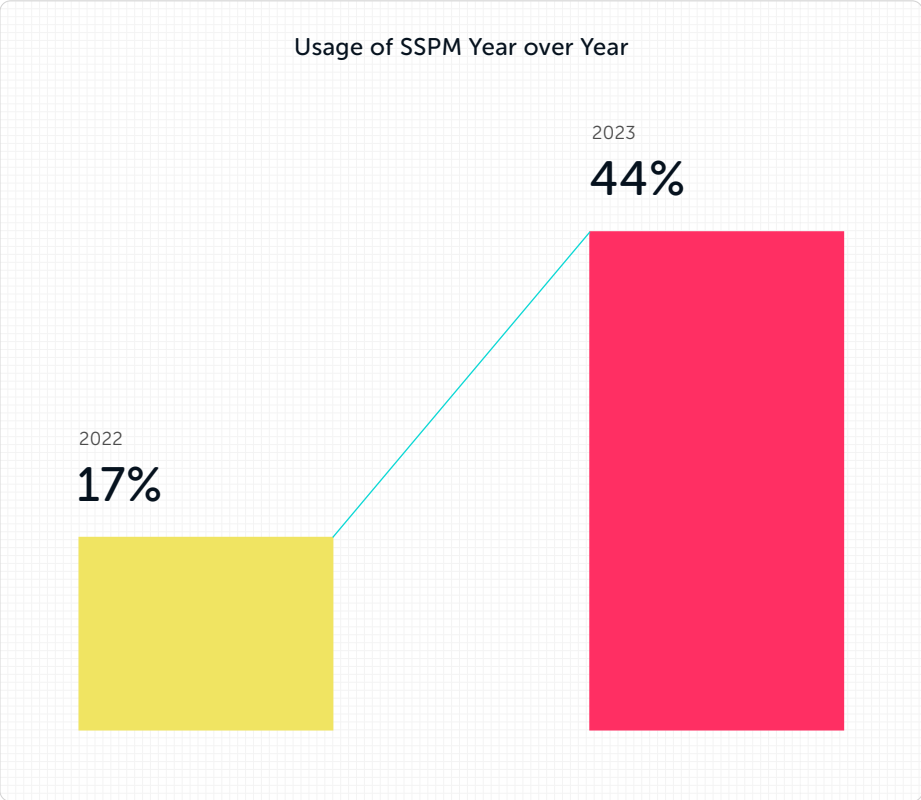
Increase in Use of SaaS Security Posture Management (SSPM)

With SaaS security incidents on the rise and current SaaS security methods (e.g., CASB and manual audits) falling short, organizations are seeking out more advanced SaaS security tooling such as SSPMs. The survey shows that adoption of SSPM tools has grown significantly, with the percentage of organizations using SSPM increasing from 17% in 2022 to 44% in 2023.

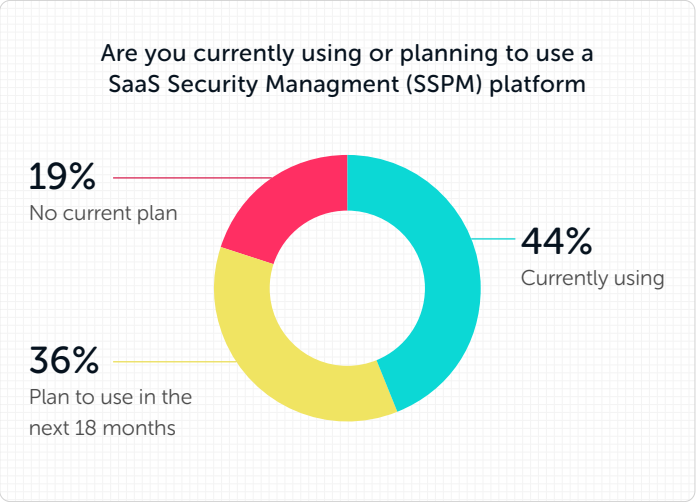
This can be attributed to the fact that SSPMs provide coverage in areas where other methods and strategies have fallen short, offering more comprehensive protection against various security risks throughout the whole SaaS Security Ecosystem.

As broken down earlier in this paper but summarized here, these areas include

- **SaaS Misconfigurations:** Ensuring proper configuration of SaaS applications to avoid breaches.
- **Identity & Access Governance:** Managing and controlling user access to SaaS applications and resources.
- **Third-Party App Access:** Identifying and managing the risks associated with third-party applications accessing SaaS environments.
- **Data Loss Management:** Preventing and mitigating the loss or leakage of sensitive data in SaaS applications.
- **Connected Malicious Apps:** Detecting and removing malicious applications that could compromise the security of the SaaS environment.
- **Threat Detection & Response:** Proactively identifying and responding to security threats in real-time.
- **SaaS User Devices:** Monitoring and managing the security risks associated with user devices connecting to SaaS applications.

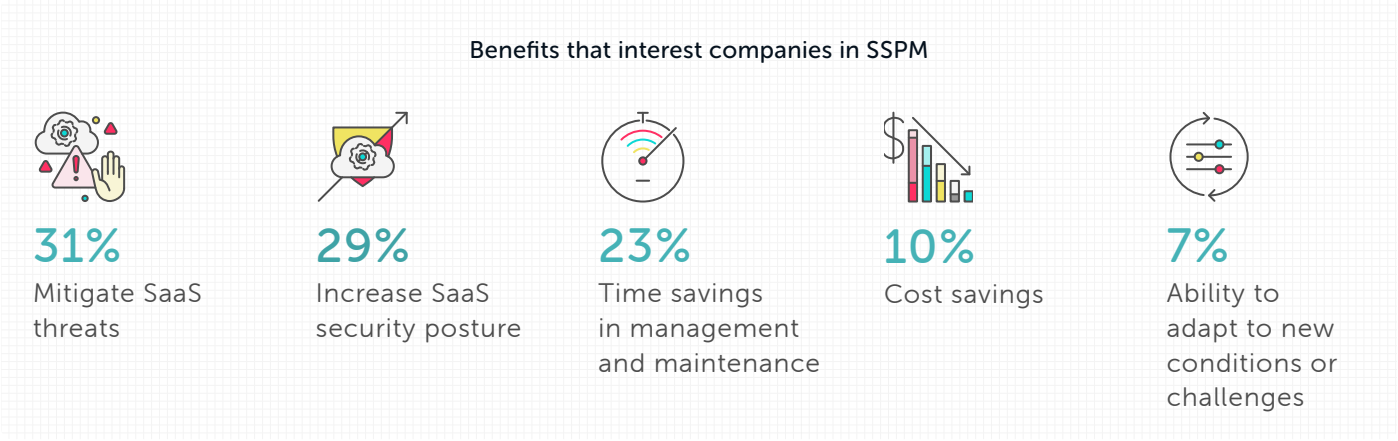


As SaaS security incidents continue to rise, organizations are recognizing the limitations of other security methods like CASBs and manual audits for SaaS. The increased adoption as well as the significant percentage of those planning on adopting SSPM solutions reflects the growing awareness of the need for more robust and comprehensive security measures to protect against the ever-evolving landscape of SaaS security threats.



SSPM Benefits

Given the increasing importance of SaaS security, there is a clear need for a more comprehensive and robust approach. There are SaaS security tools such as SSPMs that can assist organizations with the policies, processes, and capabilities that today's SaaS security landscape requires. By focusing on these critical aspects, organizations can better protect their valuable assets and ensure the safe operation of their business-critical applications in an increasingly complex threat landscape.



Organizations are increasingly recognizing the value of adopting SaaS security tools like SSPMs to address the evolving challenges in the SaaS landscape. This explains why 44% have already adopted an SSPM solution in the past year and why 36% are planning to adopt SSPM in the next 18 months. By leveraging these tools, businesses can effectively mitigate SaaS threats and significantly enhance their overall security posture.

In addition, the use of SSPMs enables organizations to achieve time savings in management and maintenance, as these solutions streamline and automate various security processes that would otherwise require manual effort. This automation not only leads to cost savings by reducing the need for manual work but also allows organizations to reallocate resources to other critical areas. Moreover, SaaS security tools provide the adaptability needed to respond to new conditions and emerging threats, ensuring that businesses remain agile and prepared to protect their digital assets and critical applications in a constantly changing environment.

Demographics

The survey was conducted online by CSA in March 2023 and received 1130 responses from IT and security professionals from organizations of various sizes and locations.

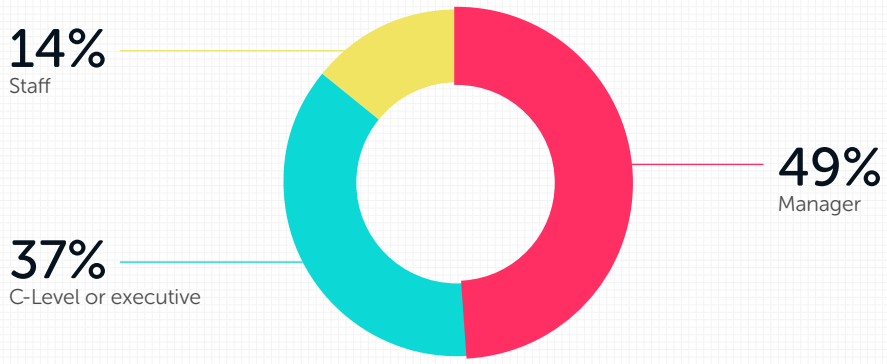
In which industry do you work?

17% Technology	11% Financial Services	6% Government	6% Professional services (Law, Consulting, etc.)	6% Media
5% Healthcare	5% Education	5% Insurance	5% eCommerce & Retail	5% Energy & Utilities
5% Food	5% Industrials (Manufacturing, Construction, etc.)	4% Pharmaceutical	3% Banking	3% Transport & Logistics
3% Public Services	2% Telecom	1% Agriculture & Mining	1% Other	1% Travel & Hospitality

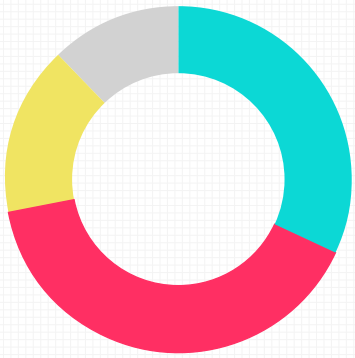
Which of the following most closely matches your role?

18% IT	12% Cyber Security	9% Cloud Security Architect	8% SaaS Security	7% Deputy CISO	7% InfoSec
7% Cloud security	5% GRC	4% SaaS Security Architect	4% CISO	3% Security Engineer	2% CIO
2% SecOps (Security Operations)	2% Forensics Expert	2% Vendor Risk Assessment	2% Penetration Tester	1% Vulnerability Management	5% Other

What is your job level?



What is the size of your organization?



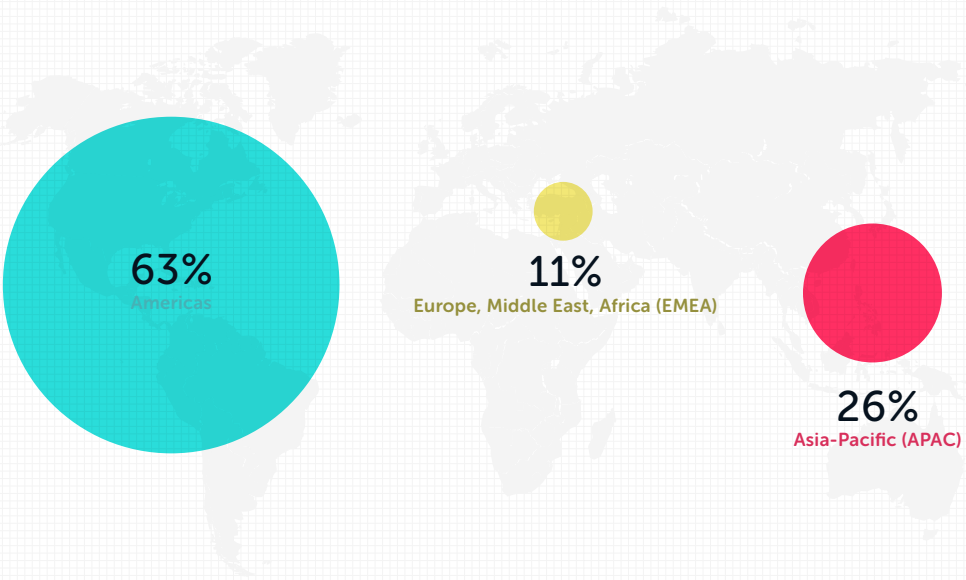
32%
<1000
employees

40%
1001 - 5000
employees

16%
5001 - 10000
employees

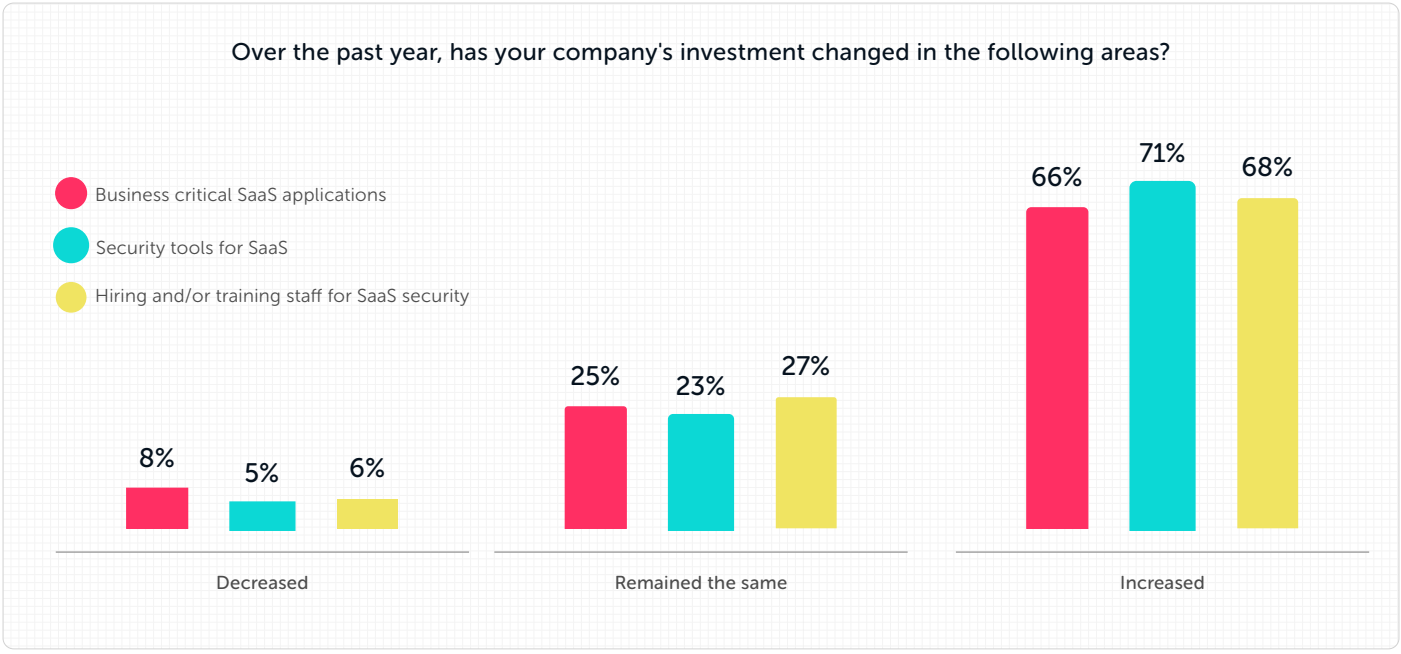
12%
+10001
employees

What region of the world you located in?

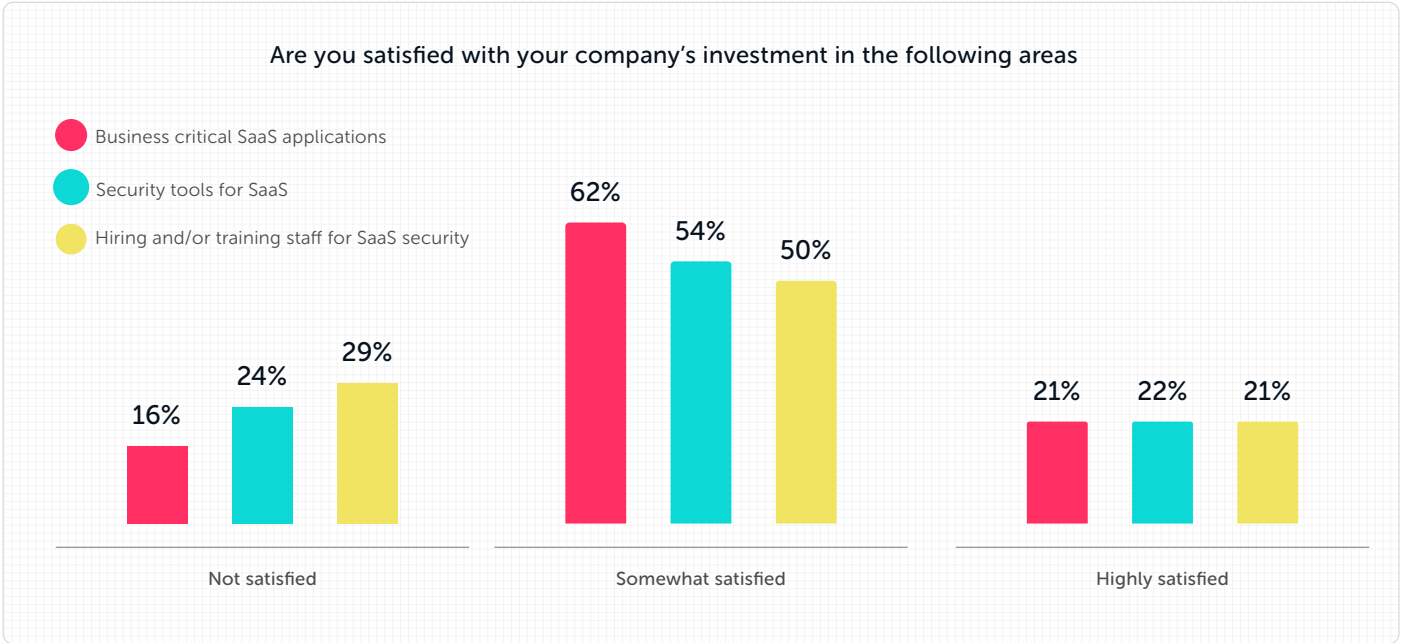


Appendix A: Survey Results

Change in company's SaaS investments

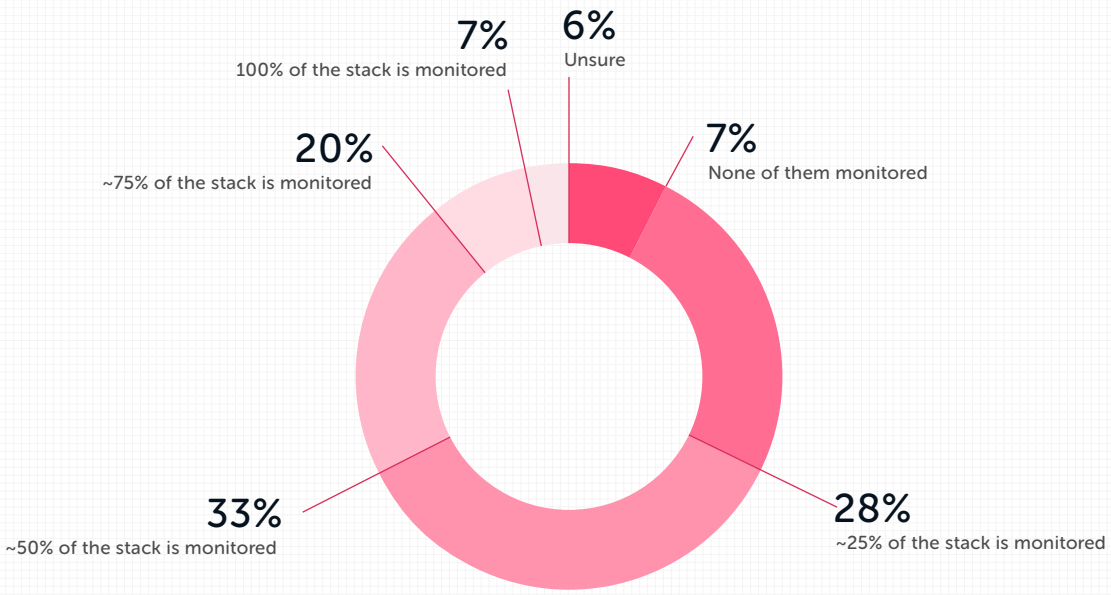


Satisfaction with company's investment in SaaS



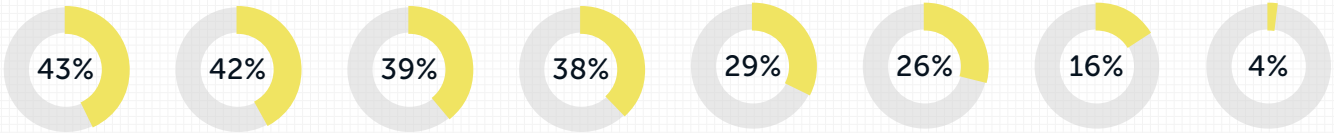
Percentage of SaaS applications monitored by a SaaS security solution

What percentage of the SaaS applications being used by your company are monitored by a SaaS security solution



Job roles involved in securing business-critical applications

Titles involved in securing business-critical apps



Top Security Concerns

What are the top security concerns when adopting SaaS applications in your company

43% Identity and access governance

40% 3rd party app access and their level of permissions

32% Data loss management

31% Connected malicious apps

31% Threat detection and response

29% SaaS misconfiguration

14% SaaS user devices and their risk

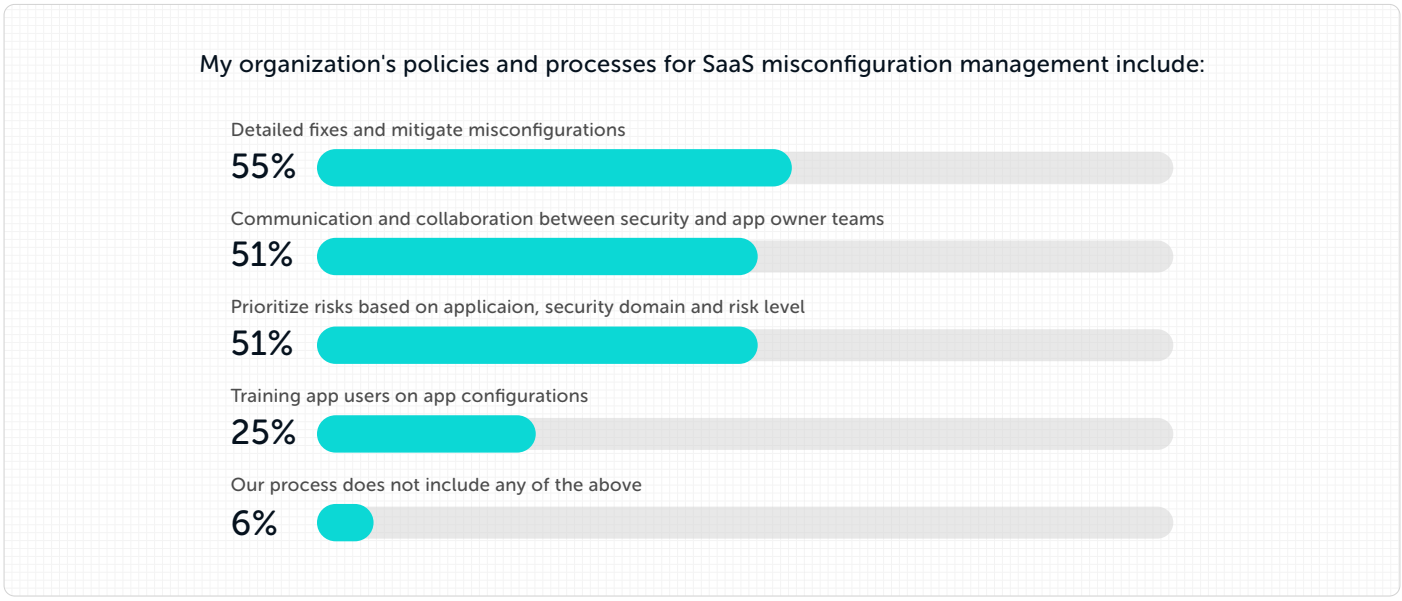
9% SaaS security personnel

1% I am not aware of any SaaS-related risks or threats

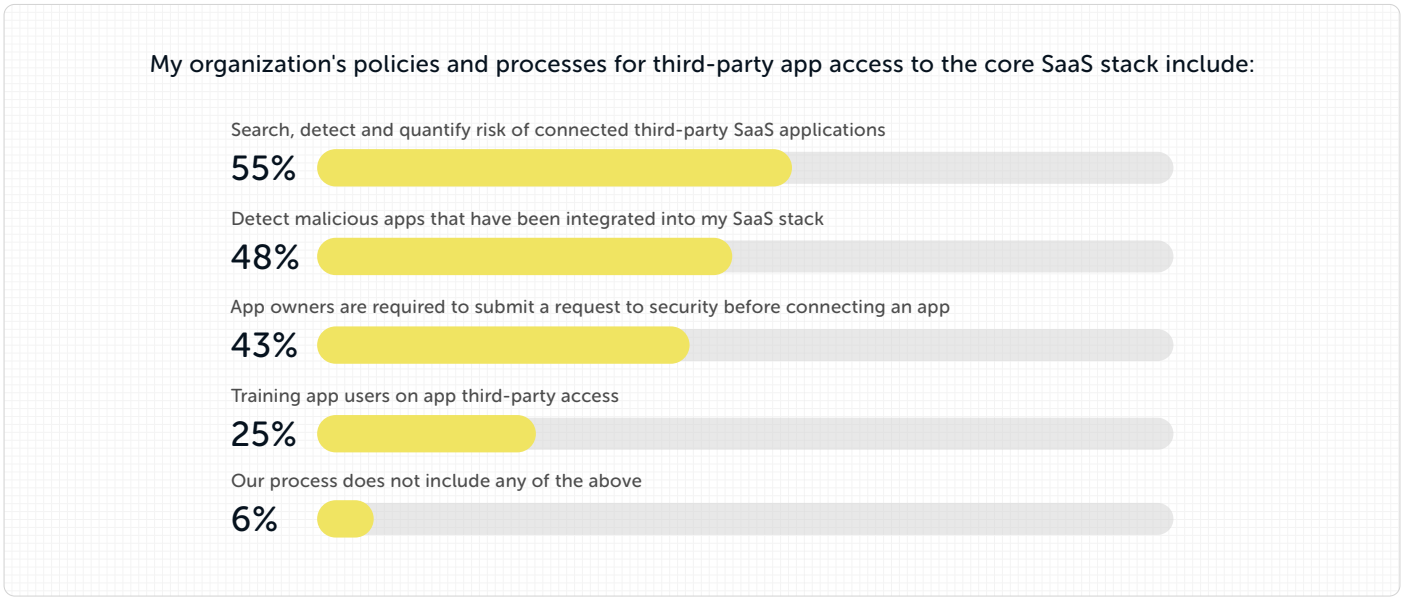
SaaS Security Policies and Processes

In this section, respondents were asked to select all answers that applied

Misconfiguration management

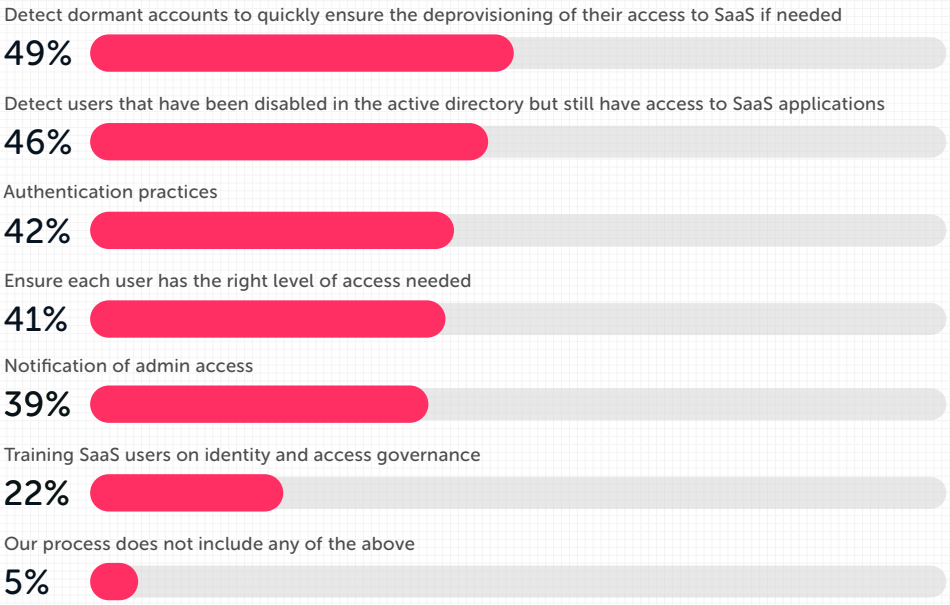


Third-party application access to core SaaS stack

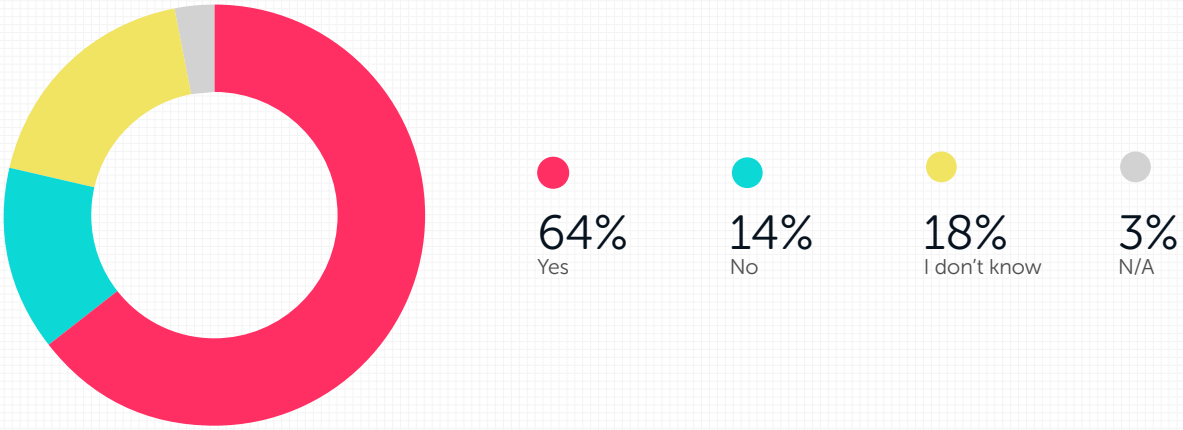


Identity and access governance

My organization's policies and processes for SaaS and access governance include

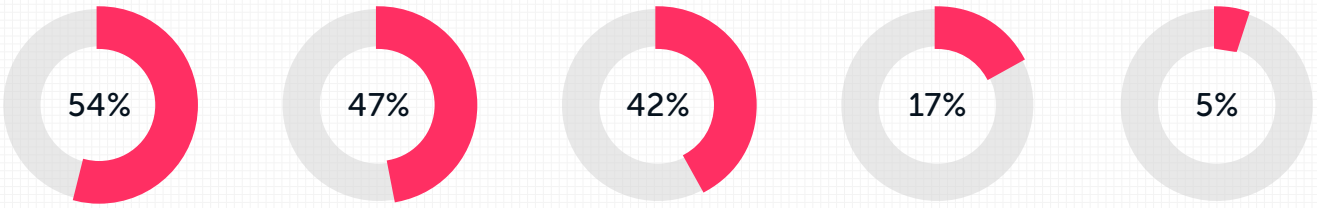


Is your security team able to identify and manage users with multiple user names



Monitoring devices that access SaaS applications

My organization's policies and processes for monitoring devices that access SaaS applications include



- 54% Check the device hygiene (vulnerabilities and updates agents) of SaaS privileged users only
- 47% Check the device hygiene (vulnerabilities and updates agents) of each and every SaaS user
- 42% Identify unmanaged devices accessing the SaaS stack
- 17% I don't have a process/ I'm unable to monitor devices that access our SaaS
- 5% Our process does not include any of the above

Detection and response capabilities for SaaS threats

My organization's SaaS threat detection and response capabilities include

- 58% Detect attacks through threat intelligence
- 47% Detect MFA flood attacks
- 44% Identify and respond to user and entity behavior anomalies
- 36% Detect brute force attacks
- 6% I don't have SaaS threat detection and response capabilities
- 2% Other

Data loss prevention regarding SaaS security

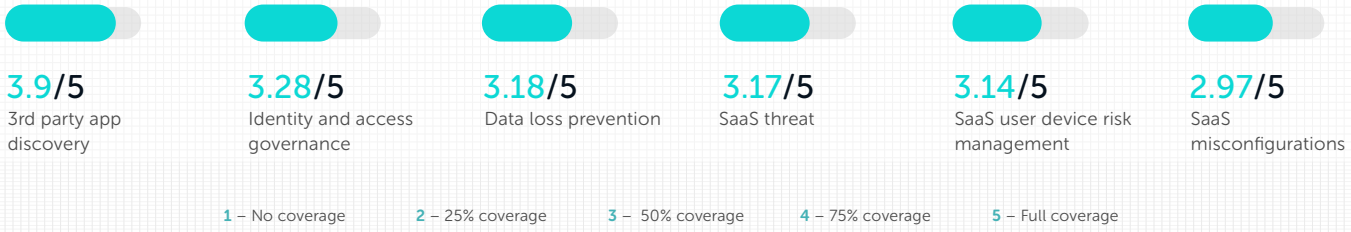
My organization's policy and processes for data loss prevention (DLP) regarding SaaS security include

- 51% Establish policy limiting data access by group or role
- 44% Alerts for excessive data download
- 42% Password protection for externally shared data
- 34% Alerts for excessive access to data
- 28% Expiration date for access to externally shared data
- 2% Training on SaaS DLP

SaaS Threats

CASB coverage for SaaS

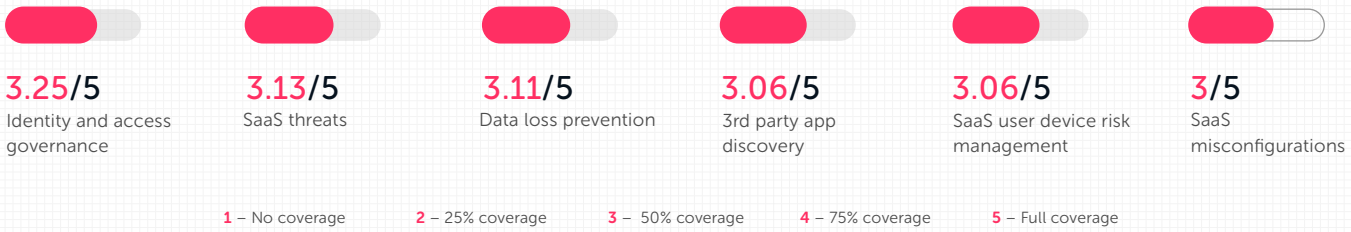
If you are using CASB to secure your SaaS, what level of coverage do you receive from this solution in the following areas



1 – No coverage 2 – 25% coverage 3 – 50% coverage 4 – 75% coverage 5 – Full coverage

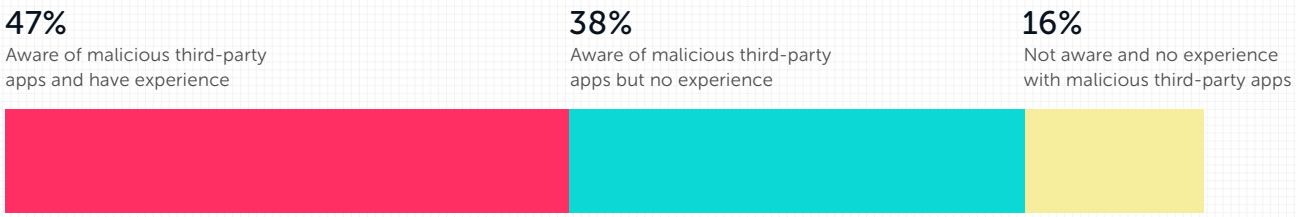
Manual audits' coverage for SaaS applications

If you are running manual audits on your SaaS application, how much coverage do you achieve in the following areas



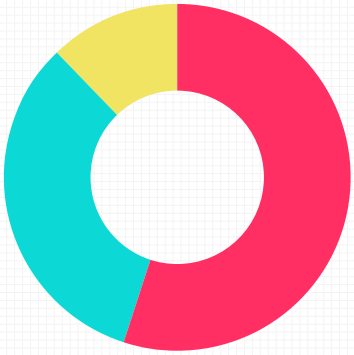
1 – No coverage 2 – 25% coverage 3 – 50% coverage 4 – 75% coverage 5 – Full coverage

Have you had any experience with malicious third-party applications



SaaS application security incidents

Has your company experienced a SaaS application security incident within the past two years



55% Yes

32% No

12% Unsure

What type of security incident(s) have you experienced

Data Leakage

Malicious Apps

Data Breach

SaaS Ransomware

Corporate Espionage

Insider Attack

SSPM Use and Benefits

Currently using or planning to use SSPM

Are you currently using or planning to use a SaaS Security Management (SSPM) platform

- 44% Currently using
- 36% Plan to use in the next 18 months
- 19% No current plans

Top benefits from using an SSPM

- 35% Improved control over the SaaS landscape
- 34% Increase SaaS security
- 19% Time savings in management and maintenance
- 8% Cost savings
- 3% Ability to adapt to new conditions or challenges

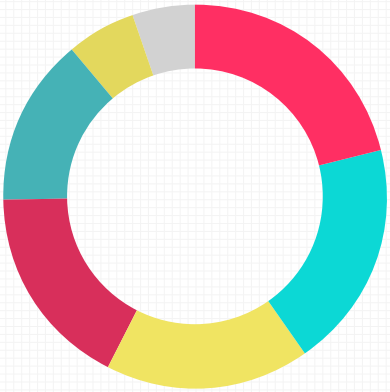
Top expected benefits from an SSPM solution

- 31% Mitigate SaaS threats
- 29% Increase SaaS security posture
- 23% Time savings in management and maintenance
- 10% Cost savings
- 7% Ability to adapt to new conditions or challenges

Results from respondents planning on implementing an SSPM solution within next 18 months.

Reasons for not implementing an SSPM

What is the top reason your company has no plans to implement an SSPM



21%
Not a top priority for my organization

19%
Lack of budget for purchasing the solution

17%
Lack of staff and knowledge to implement

17%
Lack of staff and knowledge to manage

14%
Covered by other solutions

6%
This kind of solution does not meet my security concerns

5%
Other

Acknowledgements

Lead Author

Hillary Baron

Contributors

Josh Buker

Marina Bregkou

Ryan Gifford

Sean Heide

Alex Kaluza

John Yeoh

Designer

StudioYael

Special Thanks

Hananel Livneh

Arye Zacks

Caroline Rosenberg

Eliana Vuijsje

About the Sponsor

Adaptive Shield, leader in SaaS Security, enables security teams to secure their entire SaaS stack through threat prevention, detection and response. With Adaptive Shield, organizations continuously manage and control all SaaS and 3rd-party connected apps, as well as govern all SaaS users and risks associated with their devices. Founded by Maor Bin and Jony Shlomoff, Adaptive Shield works with many Fortune 500 enterprises and has been named Gartner® Cool Vendor™ 2022.

www.adaptive-shield.com Follow us on LinkedIn REQUEST A DEMO