2022 SaaS Security Survey Report

cloud security alliance®

Acknowledgments

Lead Authors:

Hillary Baron
Josh Buker
Sean Heide
Alex Kaluza
Shamun Mahmud
John Yeoh

Designers:

Claire Lehnert
Stephen Lumpe

Special Thanks:

Eliana Vuijsje and Caroline Rosenberg at Adaptive Shield

Table of Contents

Acknowledgements 3
Survey Creation and Methodology 5
Goals of the study 5
Executive Summary 6
- Key Finding 1: SaaS misconfigurations are leading to security incidents 6
- Key Finding 2: The leading causes of SaaS misconfigurations are lack of visibility and too many departments with access 6
- Key Finding 3: Investment in business-critical SaaS applications outpacing SaaS security tools and staff. 7
- Key Finding 4: Manually detecting and remediating SaaS misconfigurations is leaving organizations exposed. 8
- Key Finding 5: The use of an SSPM reduces the timeline to detect and remediate SaaS misconfigurations 9

SaaS Application Use in Organizations 10
SaaS Security Assessment 12
Misconfigurations in SaaS Security 15
SaaS Security Tools 17
Conclusion 17
Demographics 18
About the Sponsor 20

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 cyber security 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 actions 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 security and related misconfigurations. Adaptive Shield financed the project and co-developed the questionnaire by participating with CSA research analysts. The survey was conducted online by CSA from January to February 2022 and received 340 responses from IT and security professionals from various organization sizes and locations. CSA's research team performed the data analysis and interpretation for this report.

Goals of the study

The goal of this survey was to understand the current state of SaaS security and misconfigurations. Key areas of interest include:

- Use of SaaS applications with organizations
- Methods, policies, and tools for assessing SaaS app security
- Timeline for detecting and remediating misconfigurations in SaaS app security
- Awareness of new SaaS security related products

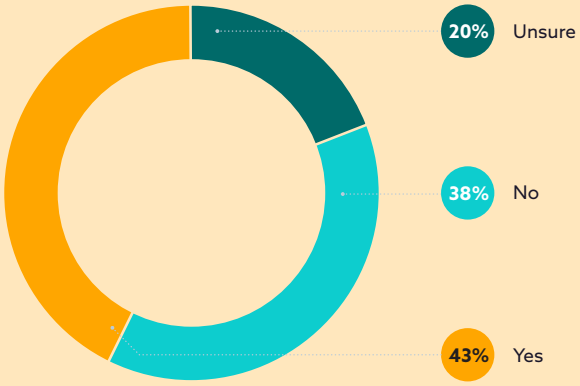
Executive Summary

Many recent breaches and data leaks have been tied back to misconfigurations causing it to be a top concern for many organizations. Most research related to misconfigurations has focused strictly on the IaaS layers and ignores the SaaS stack entirely. Yet, SaaS security and misconfigurations are equally crucial to the organization's overall security. For these reasons, CSA developed and distributed a survey to better understand the use of SaaS applications, timeline and tools for SaaS security assessments, a timeframe for misconfiguration detection and remediation, and awareness of security tools for SaaS applications.

Key Finding 1

SaaS misconfigurations are leading to security incidents

Misconfigurations have been a top concern for organizations since at least 2019[1]. Unfortunately, at least 43% of organizations dealt with one or more security incidents because of a SaaS misconfiguration. This number could be as high as 63% as a notable amount were unsure if their organization had experienced a security incident due to a SaaS misconfiguration. This fact is particularly striking when comparing similar data on IaaS misconfigurations; 17% of organizations experienced security incidents due to a misconfiguration[2].



Organizations need to embrace automation and continuous scanning for not just IaaS misconfigurations but also SaaS misconfigurations, to prevent such security incidents. Automation enables organizations to remediate the issue in real-time, so they aren't left vulnerable.

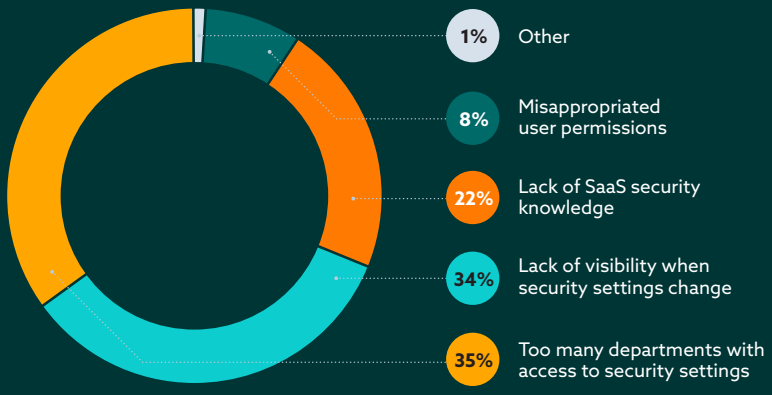
Key Finding 2

The leading causes of SaaS misconfigurations are lack of visibility and too many departments with access

The leading causes of the security incidents are two related issues: too many departments have access to the SaaS security settings (35%) and a lack of visibility into changes in the SaaS security settings (34%). This finding is not surprising for two reasons: 1. Lack of visibility into SaaS security settings was rated a top concern when adopting SaaS applications. 2. On average, organizations have multiple departments with access to security settings (see the section titled "Responsible for SaaS app security settings" for more details).

1 Top Threats to Cloud Computing: Egregious Eleven. (CSA) 2019.
2 State of Cloud Security Risk, Compliance, and Misconfigurations. (CSA) 2021.

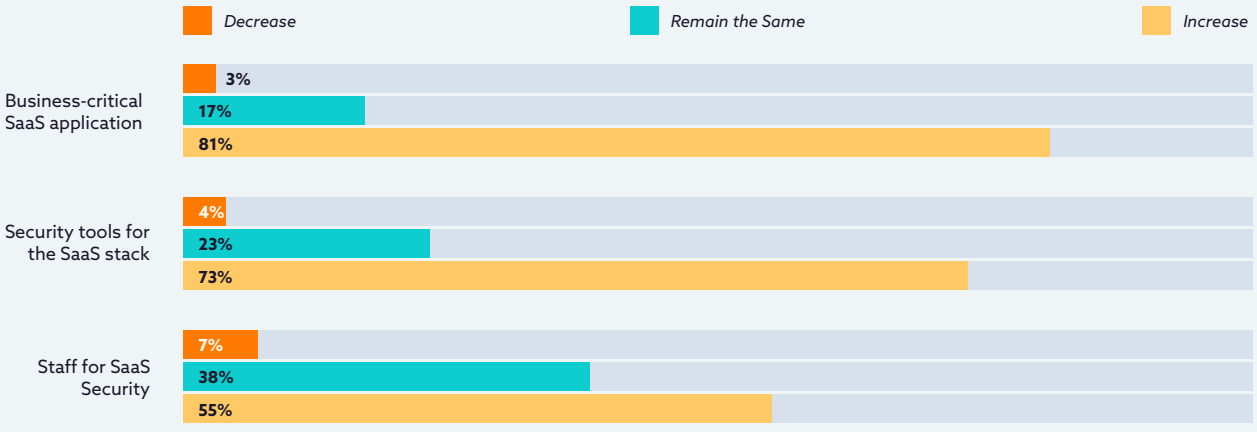
Forty percent of organizations report that departments with security access to SaaS apps are business departments (e.g., legal, marketing, sales) that are focused on performing job-related tasks. Often they lack the proper training and focus on security to be making changes to security settings. However, they need this level of access to the SaaS application to perform their job. This means organizations need to enable access for multiple departments and provide the security teams insight into security setting changes. Ultimately, this allows them to detect, prevent, and/or correct if an improper change has occurred.



Key Finding 3

Investment in business-critical SaaS applications outpacing SaaS security tools and staff

Over the past year, 81% of organizations have increased their investment in business-critical SaaS applications, but fewer organizations report increasing their investment in security tools (73%) and staff (55%) for SaaS Security. This change means there is an increasing burden on the existing security teams to monitor SaaS security. As seen in another key finding, the use of automation for monitoring SaaS security can help to decrease this pressure, but only 26% of organizations utilize this technology. Security teams are spending more time manually assessing security, detecting, and remediating misconfigurations. Organizations must consider this when investing in business-critical SaaS applications as the current investment pattern will be unsustainable long-term.

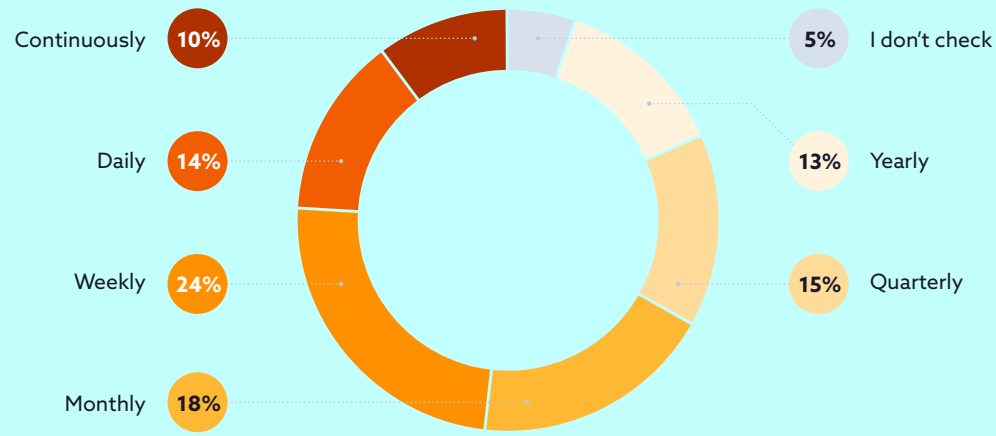


Key Finding 4

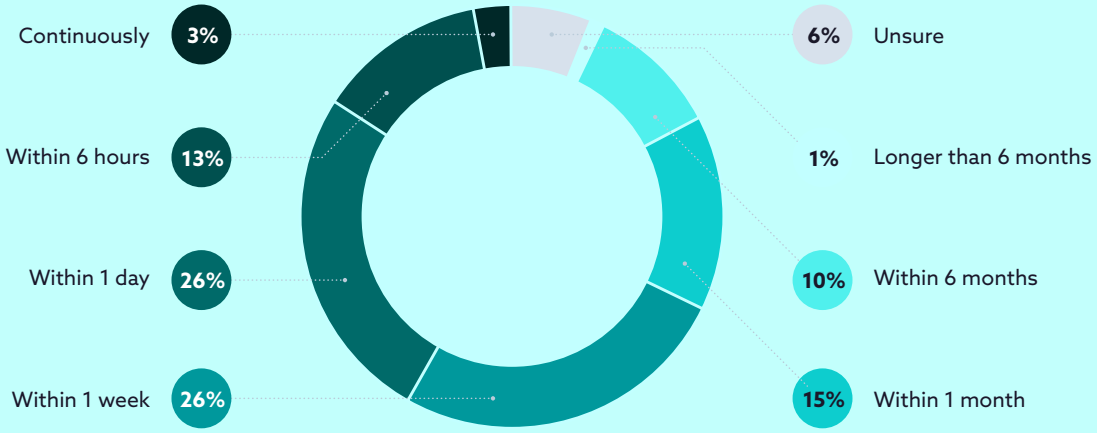
Manually detecting and remediating SaaS misconfigurations is leaving organizations exposed

When organizations manually monitor and remediate their SaaS security setting, it is taxing to the security teams and leaves the organization vulnerable. Nearly half (46%) can only check monthly or less frequently, and another 5% don't check at all. This data means that misconfigurations could go undetected for a month or longer. Then once the misconfiguration is found, it takes the security teams additional time to remediate. Approximately 1 in 4 organizations take one week or longer to resolve a misconfiguration when remediating manually. The bottom line, organizations are being left vulnerable. To prevent security incidents due to SaaS misconfigurations, organizations must explore automation and other such tools to shorten the timeline to detect and remediate these SaaS misconfigurations.

Frequency of SaaS Security Configuration Checks*



Length of Time to Fix SaaS Misconfigurations*



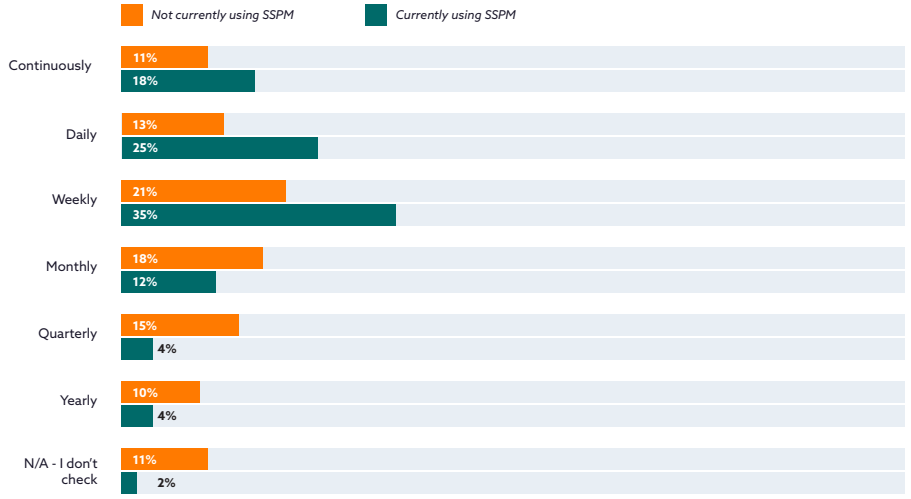
*Manual methods only

Key Finding 5

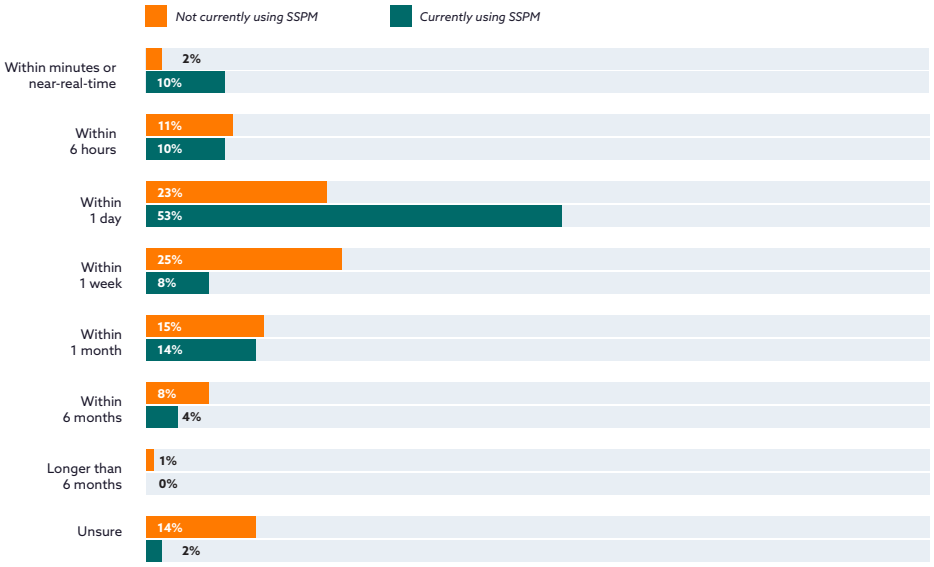
The use of an SSPM reduces the timeline to detect and remediate SaaS misconfigurations

Organizations that utilize an SSPM can detect and remediate their SaaS misconfigurations significantly quicker. Most of these organizations (78%) checked their SaaS security configurations weekly or more frequently. Compare this to organizations not utilizing an SSPM; only 45% were able to check weekly or more regularly. When resolving the misconfigurations, 73% of organizations using an SSPM resolved it within a day, and 81% resolved it within the week. Compare this to organizations that don't use an SSPM; only 36% resolve the misconfiguration within a day and 61% resolve it within one week. Take this information together, and SSPM users reduce the time their organization is exposed and likely to experience a security breach.

Frequency of SaaS Security Configuration Checks



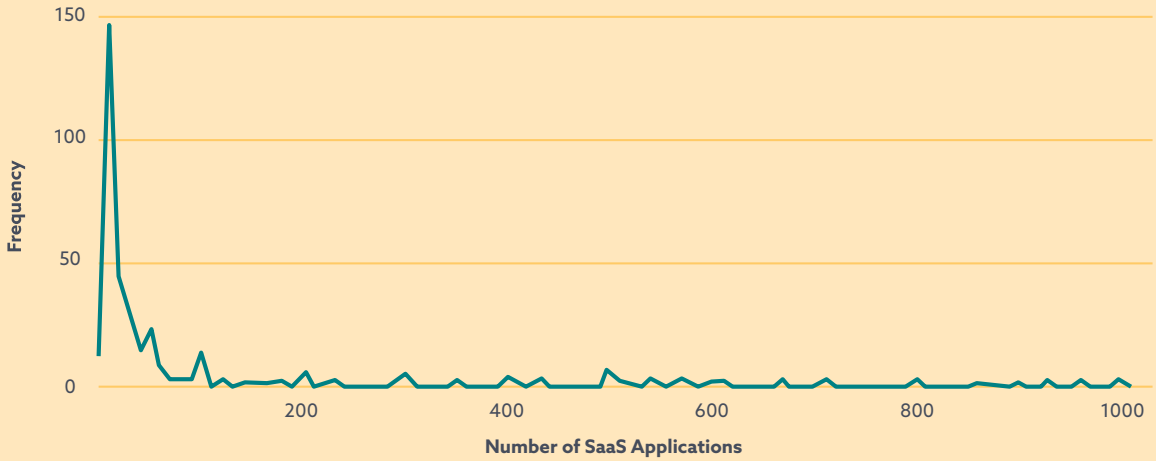
Length of Time to Fix SaaS Misconfigurations



SaaS Application Use in Organizations

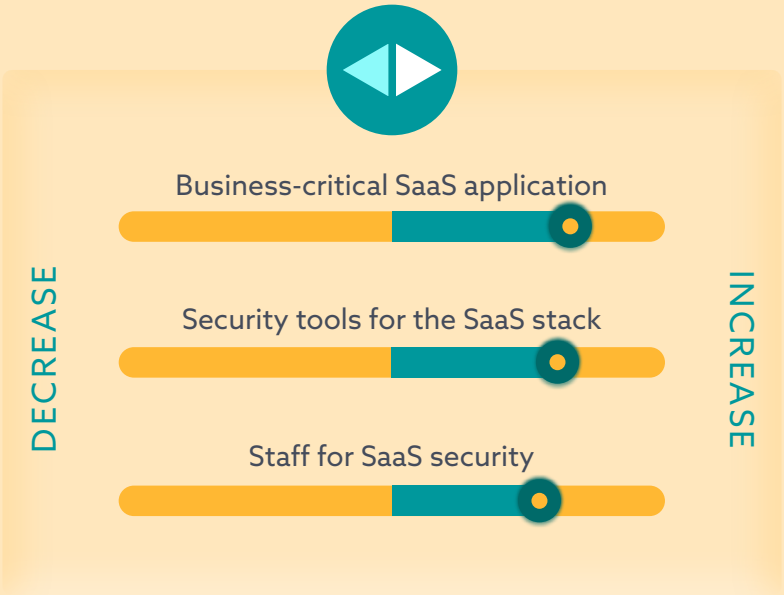
Estimated SaaS application use within organizations

On average, organizations report using 102 applications. The maximum number of applications reported was over 5000.



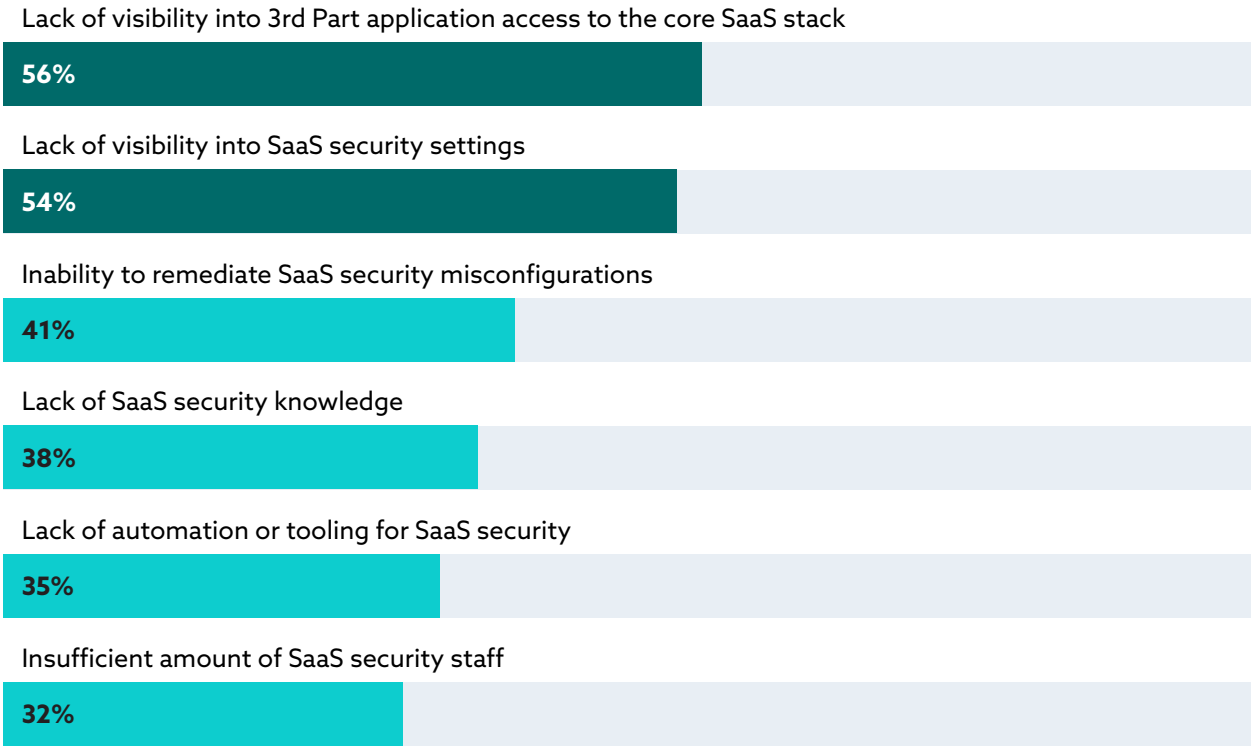
Changes to investments in SaaS application and security over the past year

Organizations have changed their investment in SaaS applications and security over the past year. However, investment in business-critical applications is outpacing investment in security tools and staff for SaaS applications. If this trend continues, organizations will continue to significantly overburden their security teams.



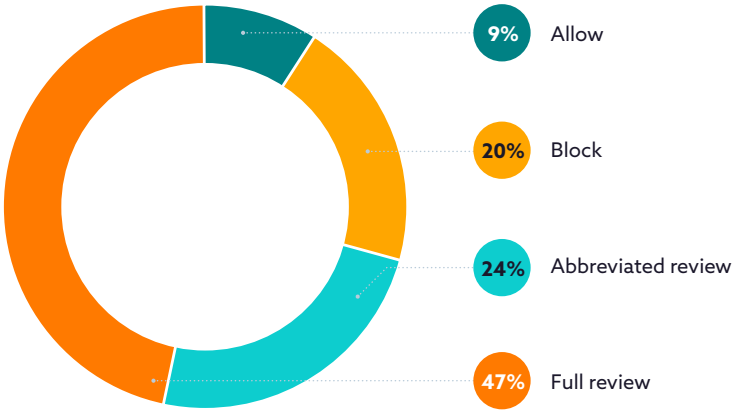
3rd party app access is a top concern when adopting SaaS applications

When organizations adopt SaaS applications, their top concerns regard a lack of visibility. Specifically, they are concerned with the lack of visibility into 3rd party application access to the core SaaS stack (56%) and SaaS security settings (54%). The least selected concern was an insufficient amount of Saas security staff (32%) which could explain the lower levels of investment found previously.



Policy when unsanctioned SaaS applications are discovered

When organizations discover unsanctioned SaaS applications, 47% perform a full security review. Approximately another quarter conduct an abbreviated review (24%).



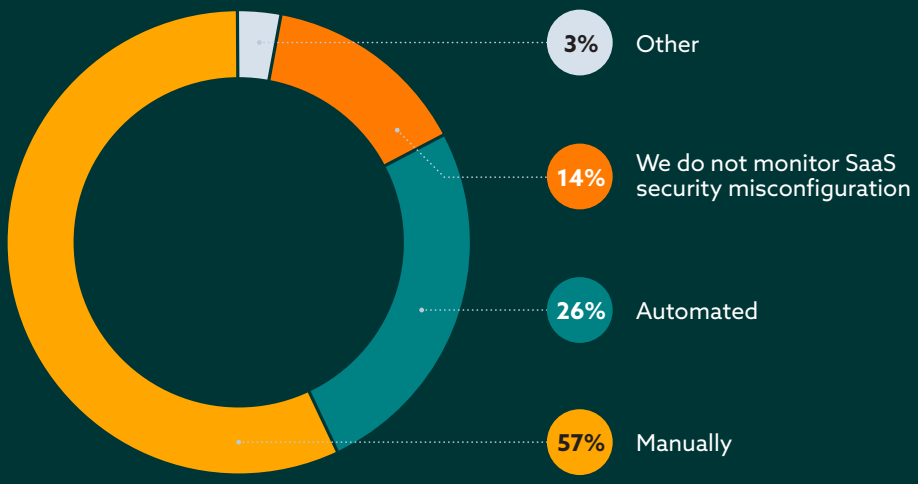
SaaS Security Assessment

Responsible for SaaS app security settings

Organizations, on average, report that more than the IT or security departments are responsible for SaaS app security settings. The top departments responsible are security (59%), IT (50%), and business application owners (40%), which signifies multiple departments that sit outside of security. While business application owners have valid reasons to have this level of access, these departments lack the proper knowledge of security and interest in maintaining the application's security. This ultimately can cause issues for the security and IT departments who do.

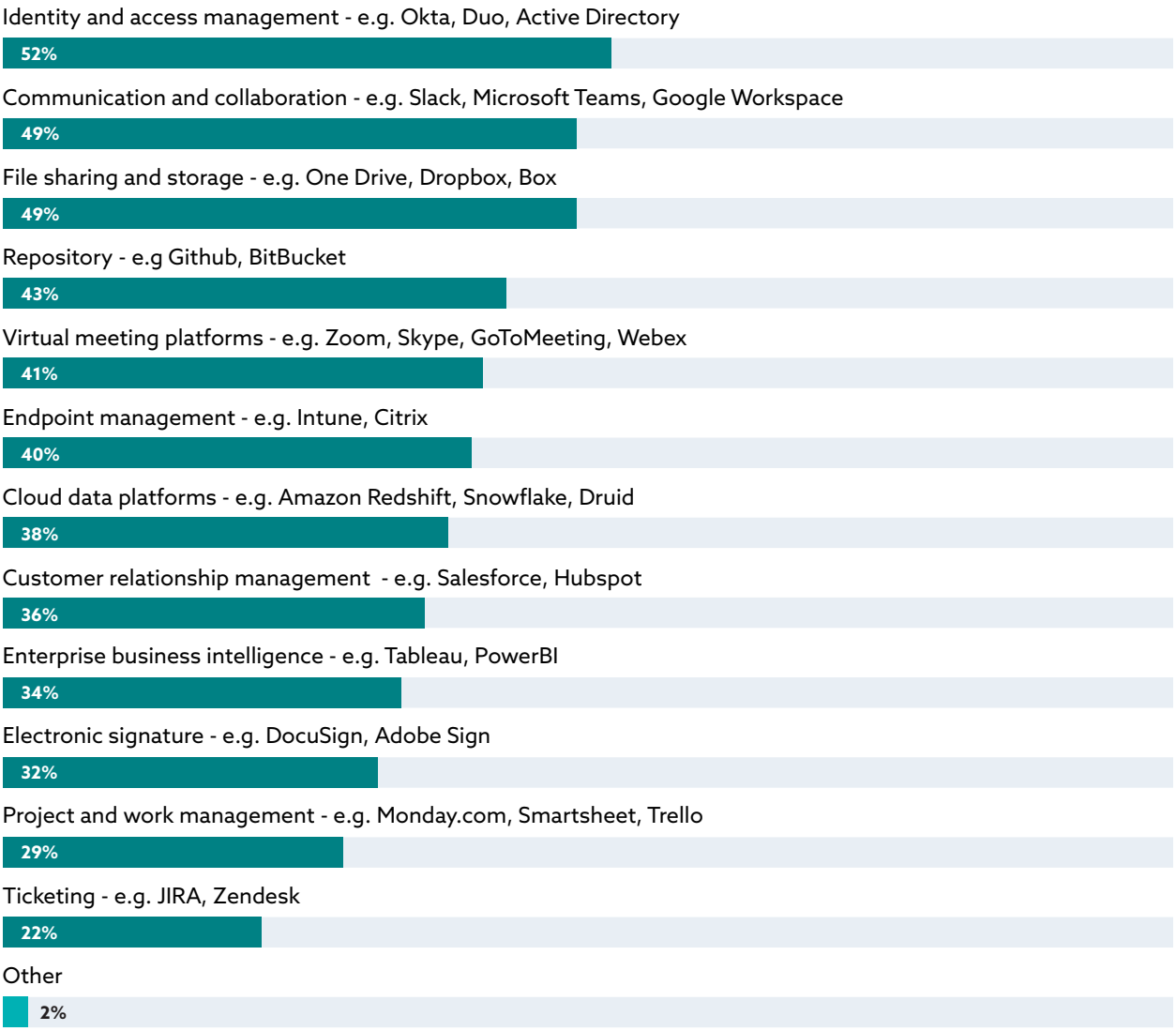
Method for monitoring SaaS security configuration

The most common method for monitoring SaaS security configurations is manually (57%). Of those organizations that monitor manually, 63% perform this assessment manually. This is not only a time-consuming task but also prone to human error. Approximately 1 in 7 organizations report not monitoring SaaS security configurations at all. This could be due to a multitude of reasons, one of which may be a lack of resources (e.g., tool to automate monitoring, staff to monitor manually).



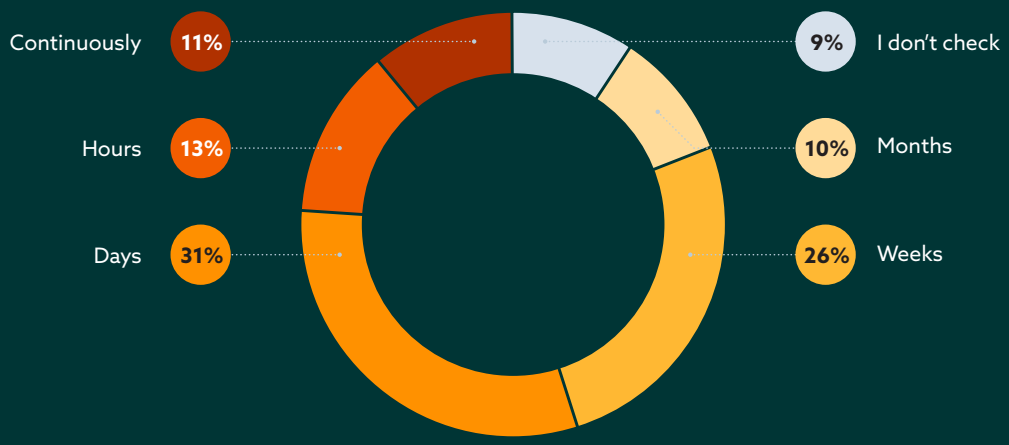
Applications assessed for misconfigurations

Organizations monitor a wide range of SaaS applications for misconfigurations. The most highly selected applications were IAM (52%), communication and collaboration platforms (49%), and File sharing/storage (49%). With small differences between concerns, it is clear that organizations are worried about their whole SaaS app stack.



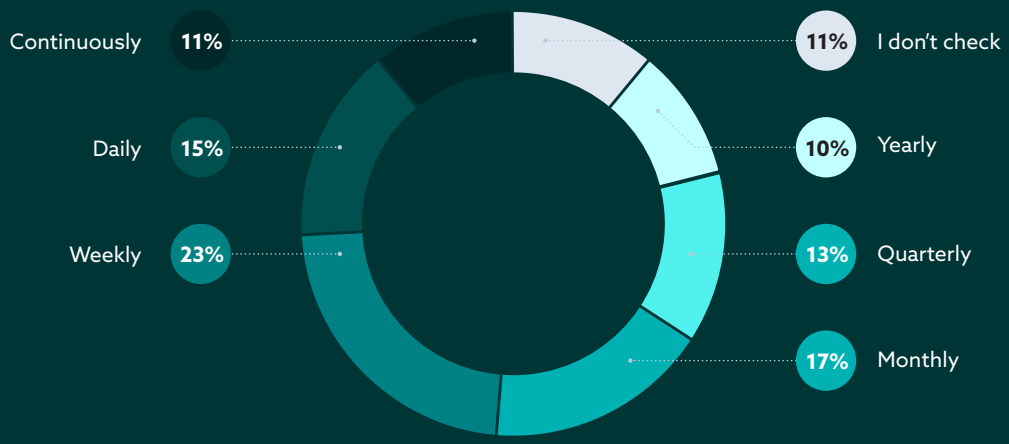
Length of time for SaaS security configuration assessment

It takes longer than a week for a third of organizations to assess SaaS security configurations. This could explain why some organizations are not monitoring their SaaS security configurations; it is a time and resource-intensive process.



Frequency of SaaS security configuration assessment

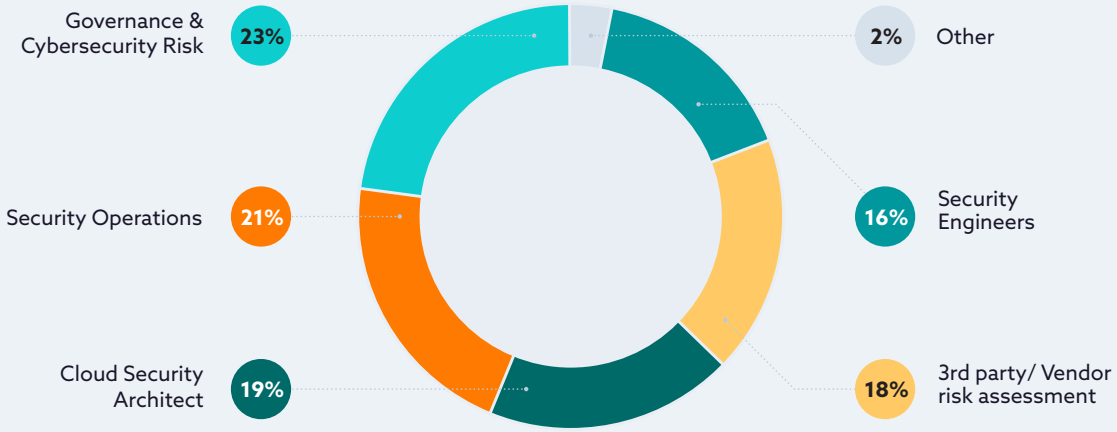
Forty percent of organizations check their SaaS security configuration monthly or less frequently; 1 in 10 organizations reported that they only checked yearly. The most common response, however, was weekly (23%).



Misconfigurations in SaaS Security

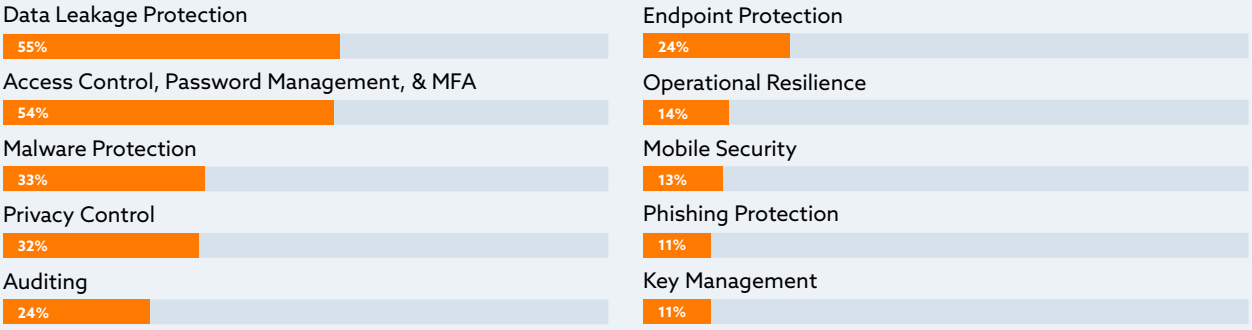
Responsible for detection and remediation of SaaS security misconfigurations

The primary role responsible for detecting and remediating SaaS security misconfigurations appears to vary from organization to organization. The most common responses were Governance & Cybersecurity Risk (23%) and Security Operations (21%).



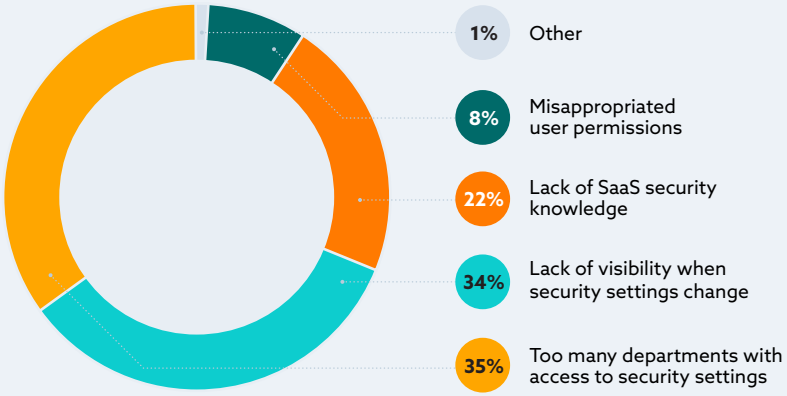
Top areas of concern related to SaaS security misconfigurations

The top areas of concern for organizations pertaining to SaaS security misconfigurations are data leakage protection (55%) and access control, password management, & MFA (54%). These concerns are complementary; they want to avoid access and exfiltration of essential company data.



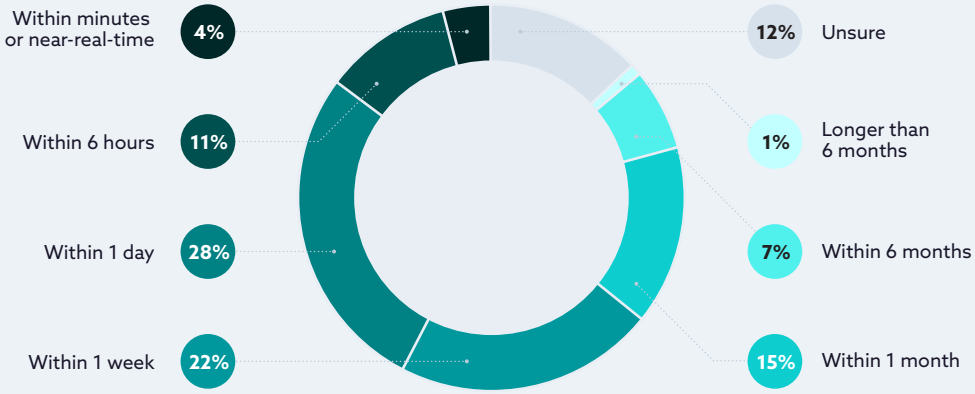
Main cause of SaaS misconfigurations

The two primary causes of SaaS misconfigurations stem from too many departments having access to security settings (35%) and lack of visibility when security settings change (34%). These causes represent two different views about the same problem. The security team responsible for detecting and correcting SaaS misconfigurations needs insight into security setting changes, particularly when other business departments have access. With this insight, the security team can work quickly with the other business departments to correct the security misconfiguration or prevent it from occurring altogether.



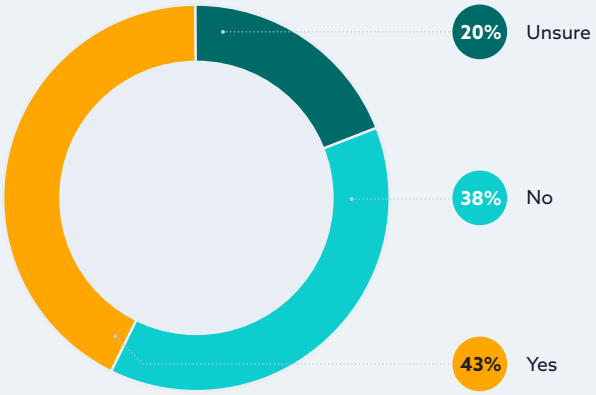
Length of time to fix SaaS security misconfiguration

Correcting misconfigurations takes about one day (28%) or one week (22%) for most organizations. A nearly equal number of organizations take a month or more (23%). For users of SSPM, however, the timeline is reduced. Nearly ¾ of organizations using an SSPM can resolve the misconfiguration within one day.



Security Incidents due to SaaS security misconfigurations within the past year

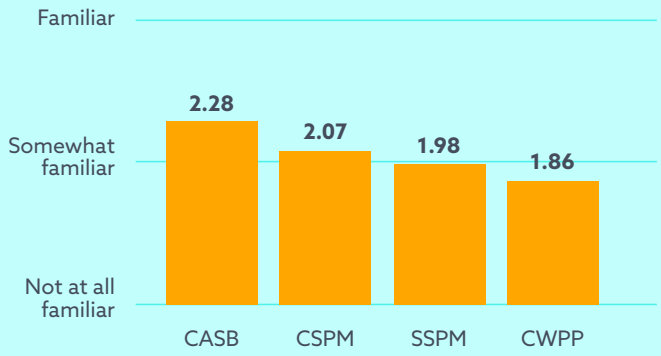
Reducing the timeline to detect and correct a SaaS security misconfiguration is crucial to preventing a security incident. Unfortunately for 43% of organizations, these misconfigurations did lead to a security incident. However, this could be as high as 63% due to the number of unsure respondents.



SaaS Security Tools

Familiarity with cloud security solutions and their benefits

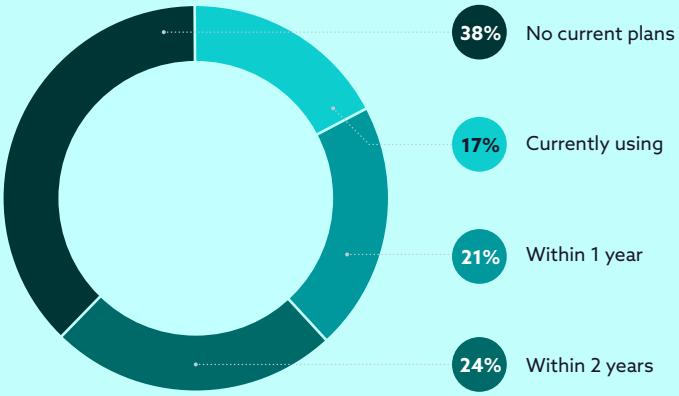
Familiarity with four cloud security solutions was assessed. Interestingly, SSPM received an average rating of "somewhat familiar." Despite only being introduced to the market approximately two years ago, the SSPM market appears to be maturing rapidly.



Current use or plans to implement SSPM

The percentage of organizations that plan to or currently use SSPM (62%) also point to rapid adoption and maturity in the market. The most common reasons cited for planning to implement an SSPM were the ability to detect and auto-remediate SaaS misconfigurations (54%) and visibility into policy violations in SaaS applications (23%).
Organizations who already use an SSPM reported their SaaS security improved (51%), and they saved time with SaaS security management and maintenance (33%)

Only 38% of organizations report having no current plans to implement an SSPM. The most common reasons for not planning to implement an SSPM were not being familiar with the capabilities (46%) and a lack of resources to implement a new solution (25%).



Conclusion

The key ways organizations can improve their SaaS security.

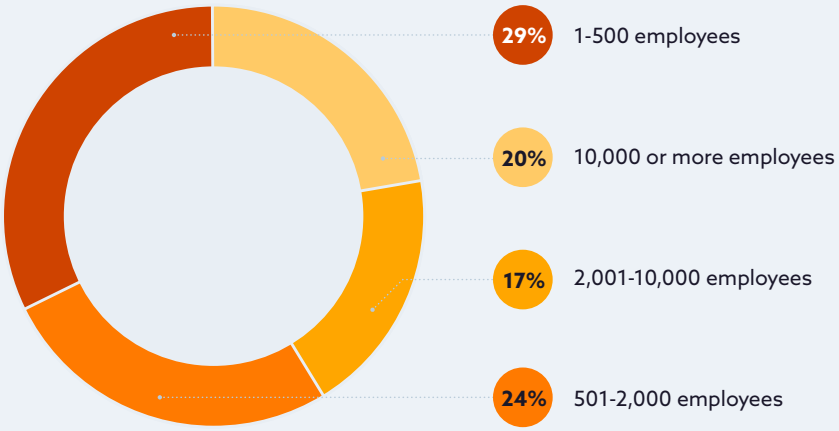
1. Provide security teams with proper visibility into SaaS app security settings, including 3rd party app access, and user permissions. This visibility allows multiple departments to maintain their access without risking improper changes that leave the organization vulnerable.
2. Utilize automated tools to monitor and remediate SaaS security misconfigurations like SSPMs. Automation allows security teams to fix these issues in near-real time, reducing the time the organization is left vulnerable or preventing the problem from occurring altogether.

These changes provide support to their security team while not preventing other departments from continuing their work and avoiding major security incidents.

Demographics

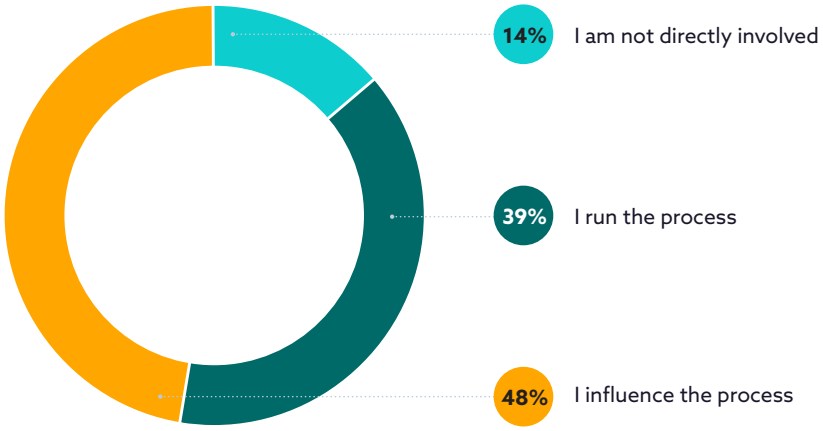
This survey was conducted from January to February 2022 and gathered 340 responses from IT and security professionals from various organization sizes, industries, locations, and roles.

What is the size of your organization?

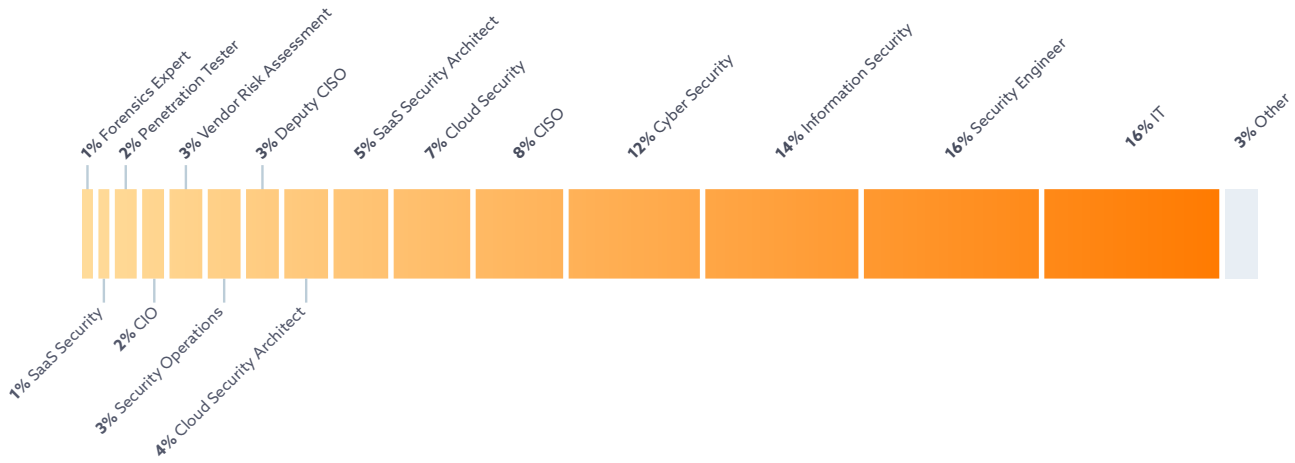


Which of the following best describes the principle industry of your organization?

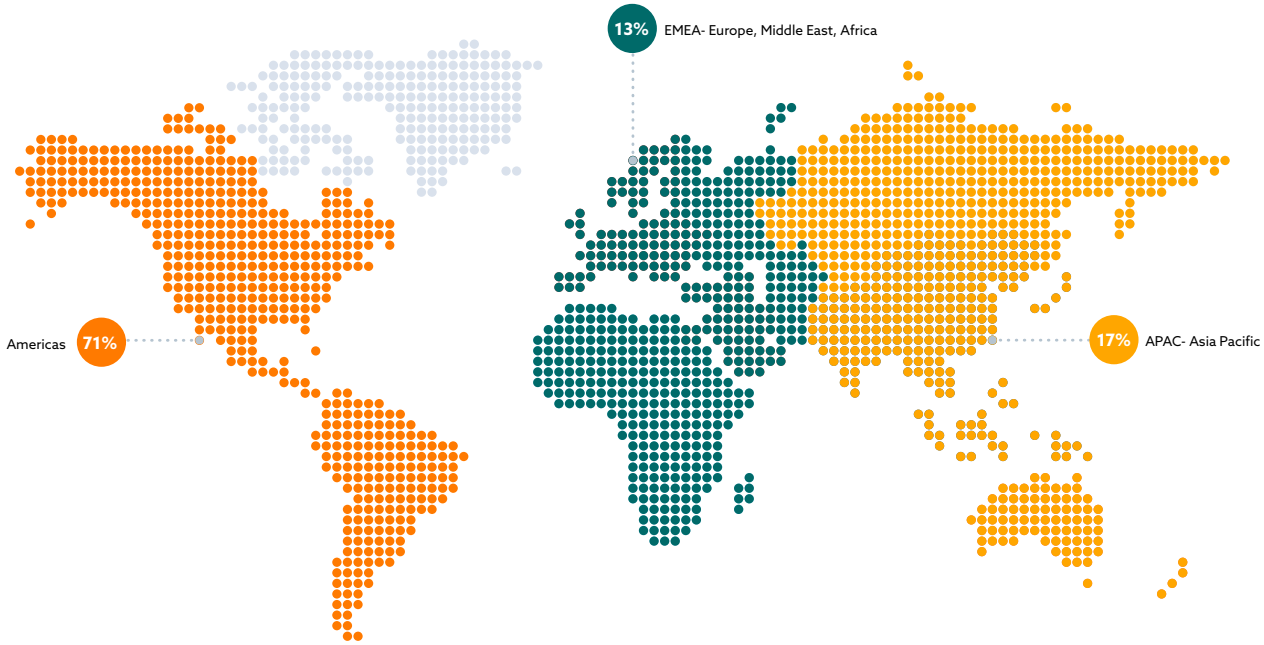
What is your role in the decision-making process of introducing new strategies?



Which of the following most closely matches your role?



What region of the world are you located in?



About the Sponsor

Adaptive Shield, the leading SaaS Security Posture Management (SSPM) company, enables security teams to see and fix configuration weaknesses quickly in their SaaS environment, ensuring compliance with company and industry standards. Adaptive Shield works with numerous Fortune 500 enterprises to help them gain control over their SaaS threat landscape. For more information, visit us at www.adaptive-shield.com or follow us on LinkedIn.

ADAPTIVE SHIELD