ADAPTIVE SHIELD

SaaS Security Survey Report 2021

Contents

Background

In 2020, Gartner named a new category of cloud security — SaaS Security Posture Management (SSPM). Not covered by existing tools such as CSPM or CASB, the most recent addition to the hype cycle can continually assess security risks from the SaaS app estate.

Often left unsecured or handed over to less-trained employees who manage Marketing, Product, or Sales, SaaS errors such as misconfigurations, inadequate authentication protocols, insufficient identity checks, credential access, and key management leave companies at risk.

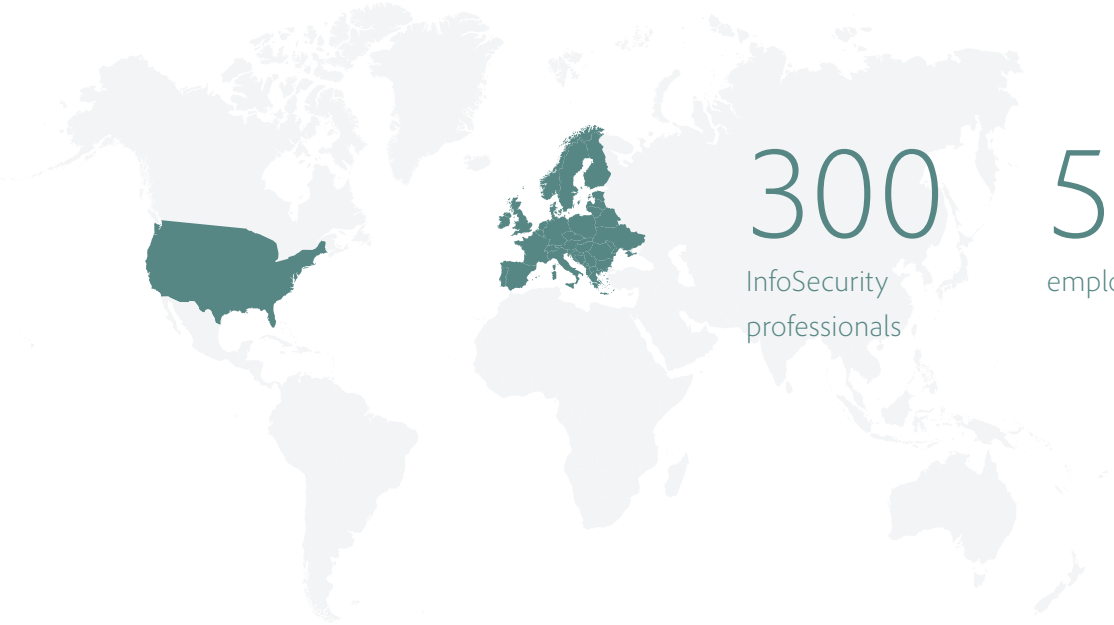
SSPM fills this gap by continuously assessing security risks and identifying misconfigurations across the organization's SaaS estate. The right solution can equip security teams with continuous SaaS security hygiene through deep visibility, detection, and remediation. With these benefits in mind, it's not surprising that SSPM has risen to the top of the conversational agenda.

Executive Summary

To understand how teams are currently dealing with their SaaS security posture, and what their main concerns are in handling SaaS tools, we surveyed 300 InfoSecurity professionals from North America and Western Europe, in companies of 500+ employees. (See full breakdown in demographics section.) The survey was completed by Global Surveyz, an independent survey company, and the responses were recorded in May, 2021.

The results present a picture of the urgent and growing need to secure this landscape. Security professionals recognize the issue at hand, and SaaS misconfigurations are a top concern. The more applications organizations onboard, the harder it becomes to keep them in check. However, with so much complexity, security owners can't help but hand over management to stakeholders with far less experience and know-how. As monitoring and maintenance spreads across departments, this creates an even greater risk of human error.

The data indicates that SSPM has risen to the top of the operational agenda and that it has become a top priority for CISOs and security professionals.



300
InfoSecurity professionals

500+
employees

Key Findings & Insights

85%

consider SaaS misconfigurations one of the top 3 threats

Cloud Risk Ranking

SaaS Misconfigurations are Considered a Top Threat

SaaS misconfigurations were reported among the top three risks that today's organizations are aware of, with 85% of companies calling out the threat. Interestingly, many of the other threats that are mentioned as a risk to today's security posture can also come as a result of misconfigurations, showing that indirectly, the threat level is even greater.

12%

of companies check for SaaS misconfigurations weekly

The SaaS Security Paradox

As SaaS Use Grows, Security Checks Lessen

With SaaS misconfigurations considered a top threat, you would expect that the more SaaS apps a company has, the more regularly they would check them. In reality, the opposite is true. The more apps a company has, the less they check security settings and permissions for misconfigurations. Only 12% of companies with 50-99 applications check them weekly.

60%

report high concern with more than 25% of their SaaS app configurations

Overcoming the Impossible

Companies Struggle with Maintaining Continuous SaaS Security Hygiene

Despite the majority of survey respondents (60%) reporting high concern with more than 25% of their SaaS app configurations, their frequency of reported checks remains low. One of the biggest challenges for security teams is the ability to configure the settings of all internal SaaS apps. Each app has different settings, a different user interface, its own terminology and its distinct complexities. Manually configuring settings for these disparate apps for hundreds to thousands of users is an impossible task.

52%

delegate responsibility over app security to the SaaS owner

The Dispersal of Delegation

App owners find themselves responsible for security

52% of companies report delegating responsibility over app security to the SaaS owner, who may be in departments such as Sales, Marketing, or Product, and is unlikely to be trained in security and compliance.

2021 Planning

SSPM is Now a TOP Priority for Security Teams

Security professionals recognize that securing the SaaS estate without a solution in place is not maintainable as SaaS apps become the system of record for most companies across all industries.

63%

of organizations know the way forward, and are already either using SSPM tools, or are planning to do so in the near future.

ADAPTIVE SHIELD

The Security Blindspot of SaaS Stack Misconfigurations

Cloud Risk Ranking, 2021

85% of companies recognize that SaaS misconfigurations are a risk to their organization.

Respondents report that SaaS misconfigurations put their organization at risk and rate them as one of the top 3 threats. This is without taking into account that many of the additional risks listed below, such as account hijacking, data leakage and limited visibility can also be caused by misconfigurations.

figure 1 Cloud Risk Ranking

Risk	High	Medium	Low	None
Account hijacking	45%	35%	17%	3%
Data leakage	44%	27%	18%	10%
SaaS misconfigurations	**32%**	**29%**	**24%**	**15%**
Insufficient identity, credential, access and key management	32%	28%	21%	18%
Insecure interfaces and APIs	32%	26%	25%	17%
Phishing	32%	21%	24%	25%
Ransomware	30%	27%	24%	20%
Insider threats	29%	31%	26%	15%
Limited cloud usage visibility	29%	26%	28%	16%
Metastructure and applistructure failures	27%	38%	23%	13%
Weak control plane	26%	28%	31%	15%

The SaaS Security Paradox

As a result of the growth in adoption of SaaS apps and the constant changes within an organization, companies are checking their SaaS applications for security weaknesses. Problematically, 73% of security professionals report that they only check on a monthly, quarterly or even annual basis.

Additionally, one might expect to see that the more apps the organization has, the more concerned the security team, and therefore they would increase the frequency of security checks. But in reality, we see the opposite. **The more SaaS applications a company has, the less frequently a company checks its security. Growth seems to cause security teams to lose control over their SaaS environment security.**

figure 2 SaaS Security Weaknesses Configuration Checks Frequency

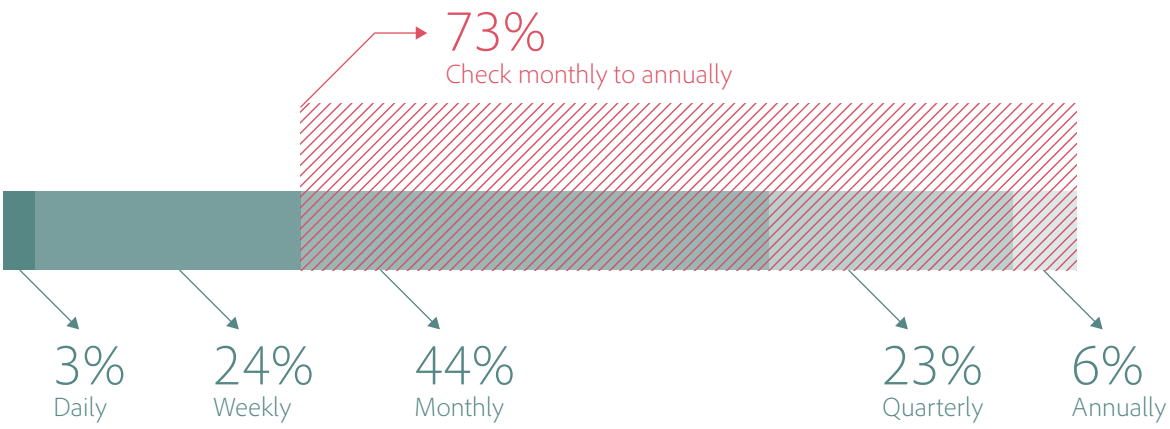
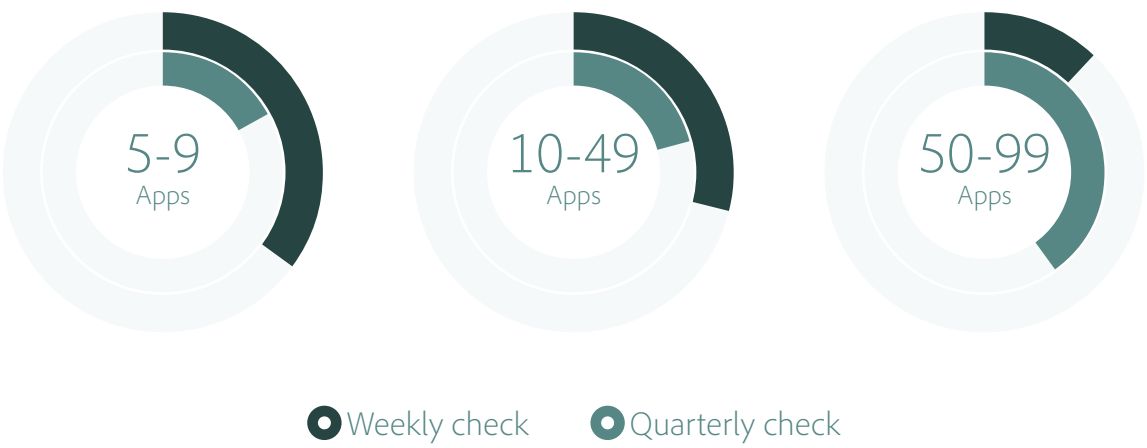


figure 3 Configuration Checks' Frequency by Number of SaaS of Applications



SaaS Apps' Configuration Concerns

Most companies are worried about over a quarter of their SaaS application security configurations.

The concern over SaaS apps and their configurations could be attributed to the constant changes in the SaaS apps themselves — from native software updates and adding new users to the systems (internal, 3rd parties, and employee turnover), to defining roles and permissions, and more. As a result, one might expect to see the frequency of checks increase with the reported concerns.

If 60% of companies are worried about the security posture of so many apps, surely that would lead to more frequent checks. However, as seen in figure 5, the rate of frequent checks (weekly basis) remains almost consistent between 23%-27%.

figure 4 SaaS Apps with Configuration Concerns

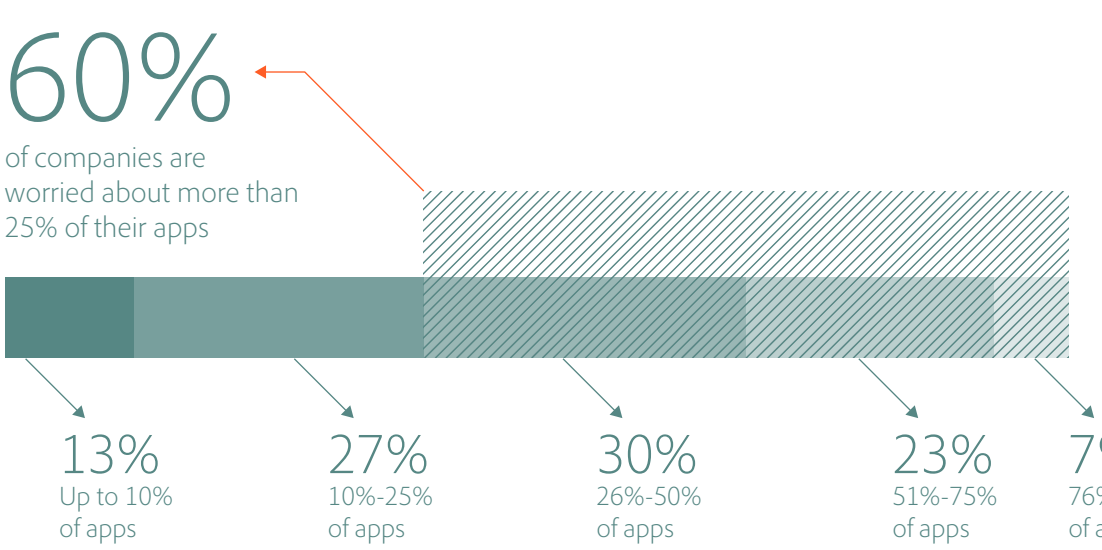
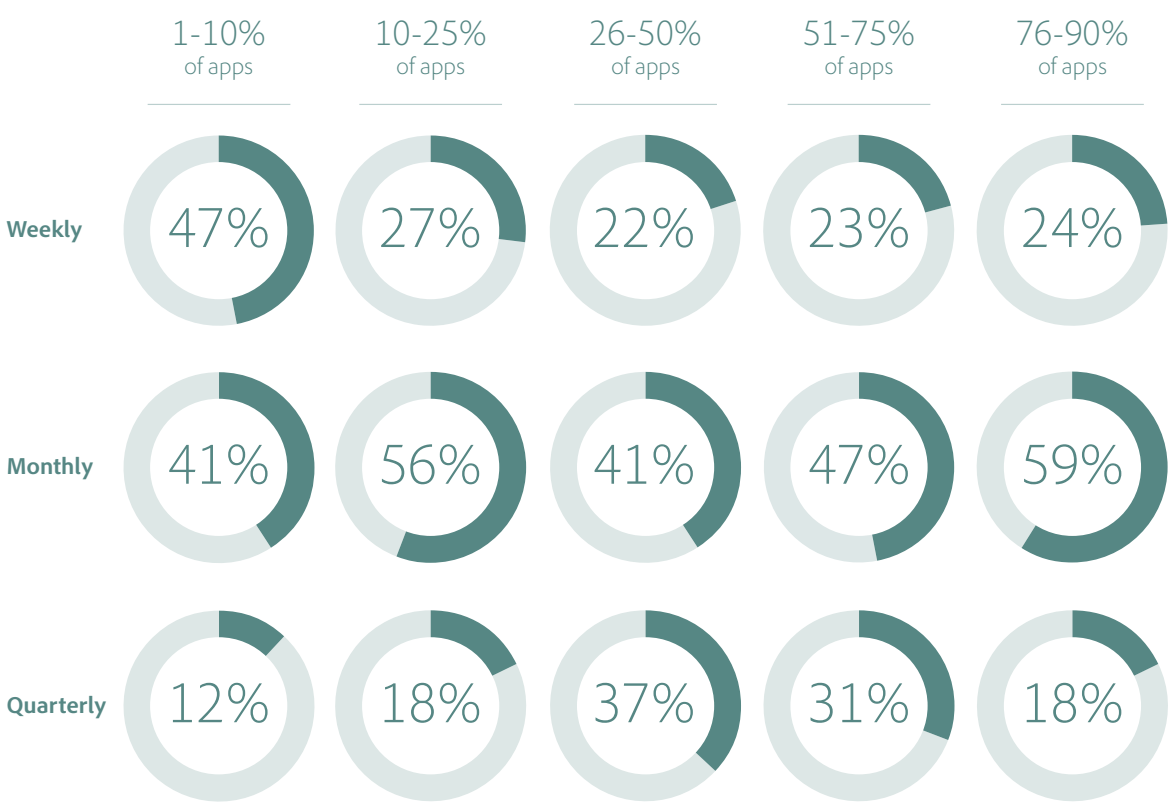


figure 5 Frequency of Checking for SaaS Configurations by Percentage of SaaS Applications Companies are Worried About



SaaS Security Responsibility is Spread Out Across Departments

Responsibility for Monitoring Security Settings

One of the biggest challenges for security teams is being able to manage the many disparate and complex settings and configure them correctly for all of their SaaS apps. Each app has unique settings, a distinct UI, and its own 'language'. **More than half of the companies report delegating the responsibility for monitoring the SaaS apps' security settings to the SaaS owner.**

Even in larger companies (5K+ employees), IT takes responsibility for monitoring the security settings at a rate of 53%. **Half of the surveyed organizations delegate security to less–trained staff who sit outside the security department's day-to-day purview.**

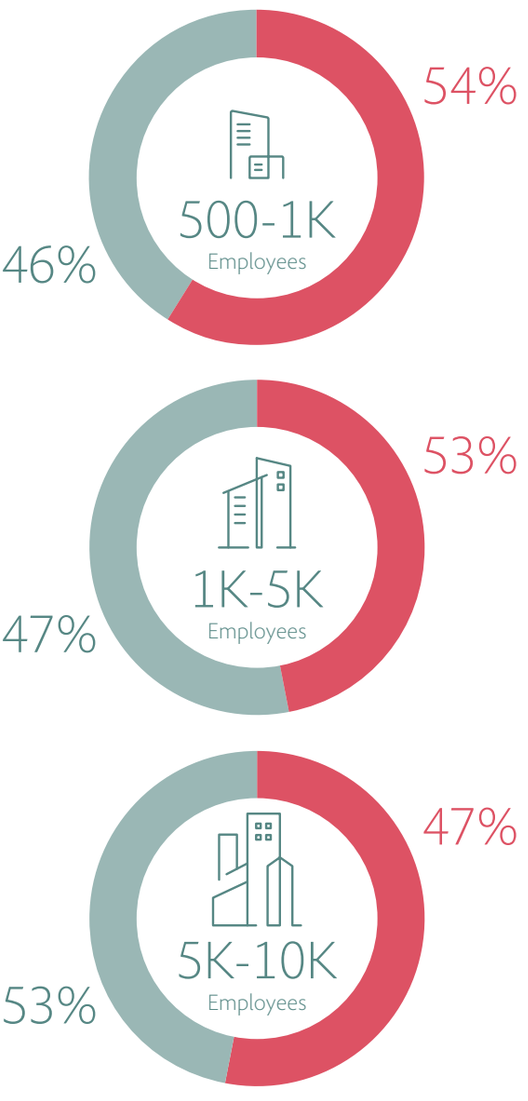
48%

report that Security Settings are managed by **IT or Security**

52%

report that Security Settings are managed by the **SaaS owner**

figure 6 Responsibility for Security Settings by Company Size



Access to SaaS Security Settings by Departments

One in four companies allow department owners (e.g. Sales, Marketing) to access SaaS security settings.

54%
IT

43%
InfoSec

24%
Saas App department owner

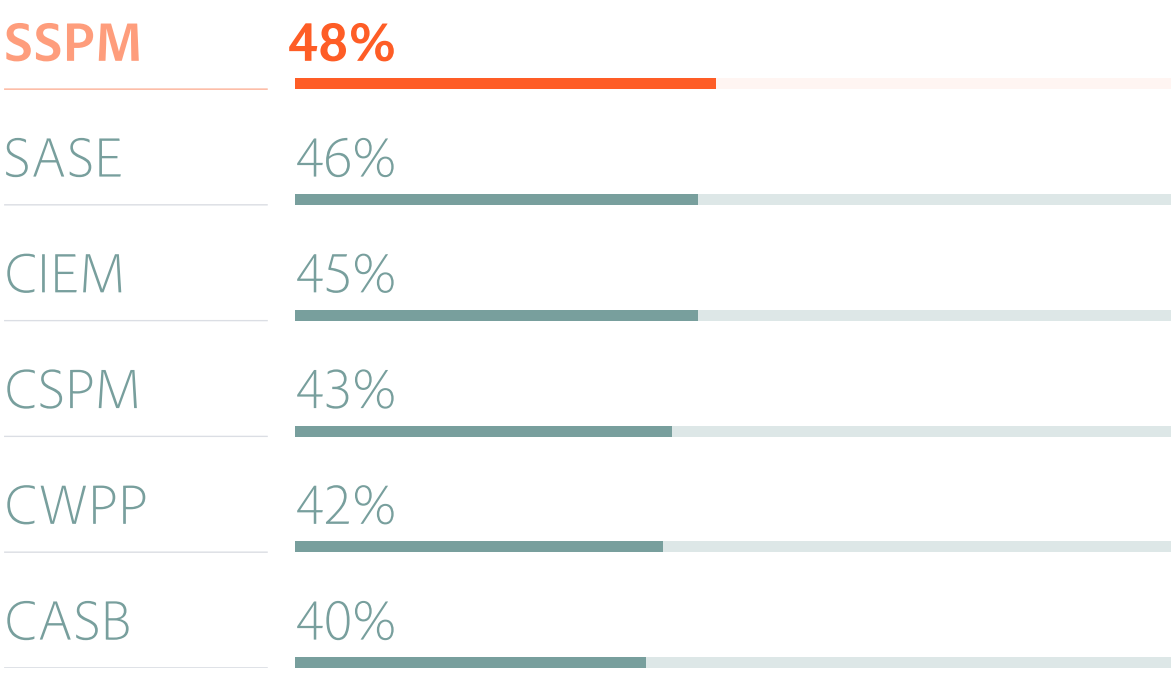
Any human error by the SaaS owner, who is often not trained in security, can lead to an increase in SaaS security misconfigurations, a reported high concern of CISOs and security professionals. Yet, in another paradox, one in four companies reports that departments outside of security have access the SaaS app security settings.

SaaS Security Planning and Priorities

2021 Security Priority Investments and SSPM Proliferation

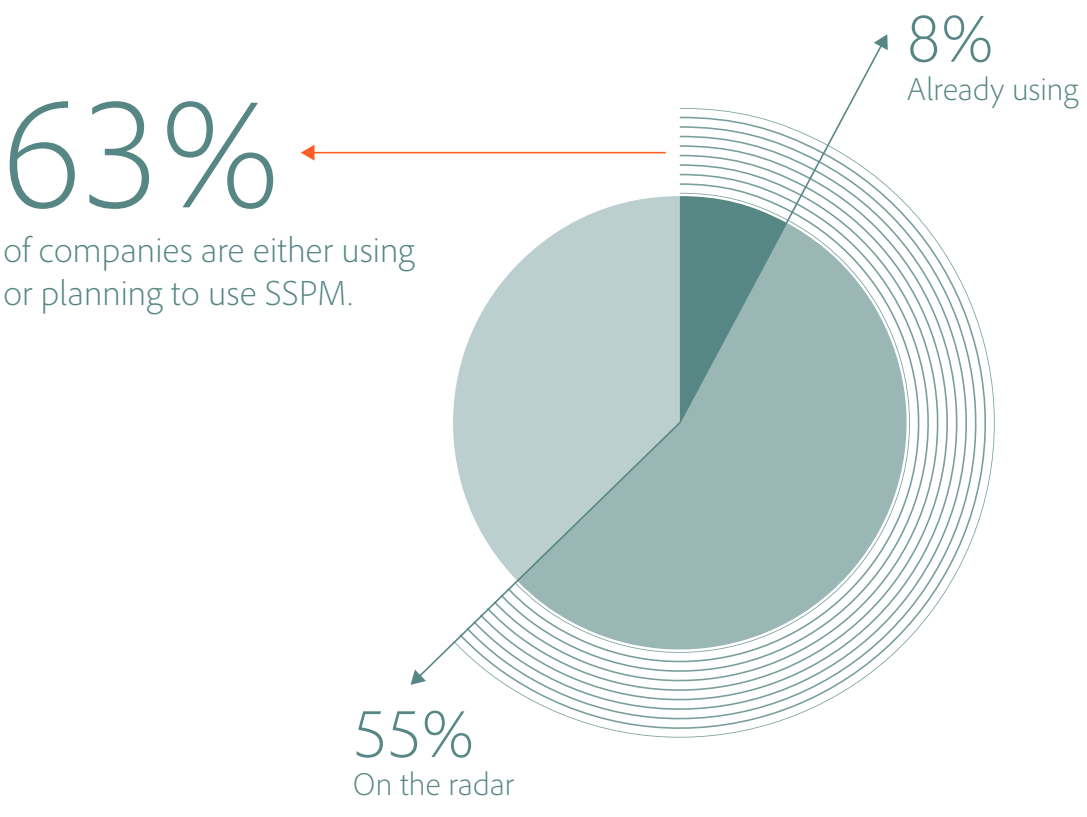
Facing this challenge head-on is at the top of the enterprise agenda. As opposed to the other cloud security solutions in the market, today, there are no real tools in wide usage that enable security teams to have full and continuous visibility of SaaS security settings and configurations. The survey results show that **SSPM has become THE TOP priority for 48% of companies in 2021.**

figure 7 Security Priority Investments, 2021



With the high risk posed by a lack SSPM, and this technology being reported as the #1 priority for investment, it should come as little surprise that 63% of companies are either using, or planning to use SSPM.

figure 8 SSPM Use and Plans



Demographics

Country of Residence

60%
US

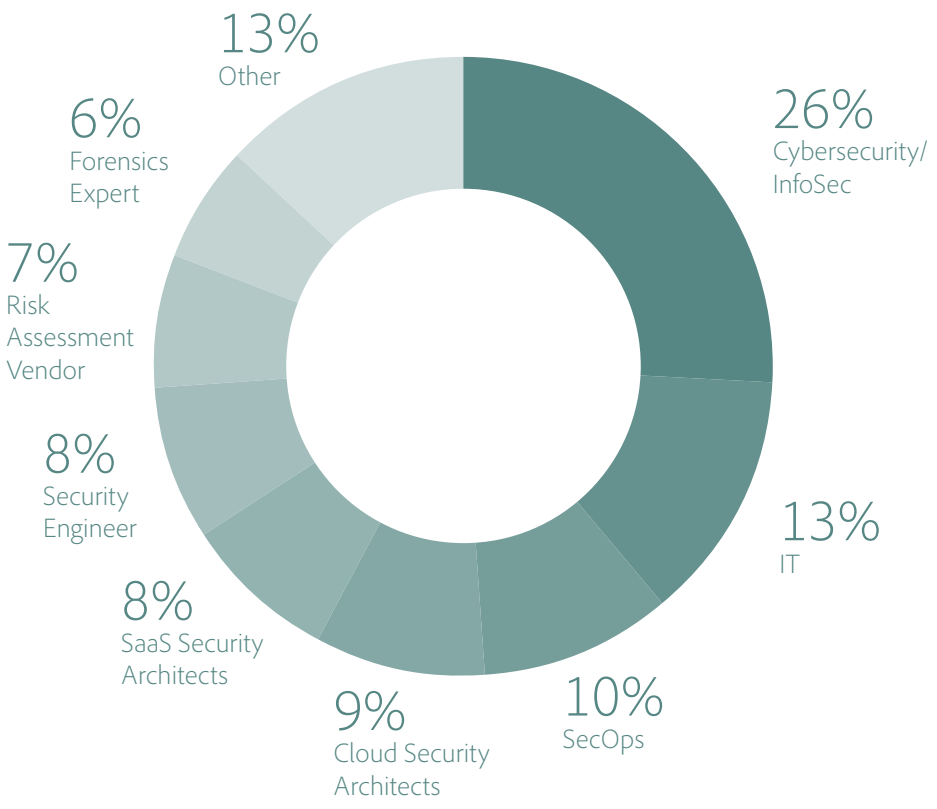
10%
Canada

30%
UK

Company Size

500-1K	41%
1K-5K	36%
5K-10K	18%
10K+	18%

Job Function



Job Seniority

23%
Manager

22%
Director

18%
Senior Director

16%
VP

10%
Architect

5%
CXO

6%
Other

Industry

Financial Services	12%
Technology	11%
eCommerce & Retail	10%
Energy & Utilities	10%
Industrials	9%
Banking	7%
Professional Services	6%
Health & Pharma	6%
Telecom	6%
Insurance	4%
Media	4%
Transport & Logistics	4%
Agriculture & Mining	3%

About Adaptive Shield

Adaptive Shield provides misconfiguration and vulnerability management with deep visibility for a company's SaaS security posture. With Adaptive Shield, security teams can easily see and fix configuration weaknesses quickly, ensuring compliance with company and industry standards.

Adaptive Shield works with many Fortune 500 enterprises to help them gain control over their SaaS threat landscape. Our management team has vast experience in cybersecurity leadership, delivering cybersecurity solutions and cloud enterprise software.

Request your SaaS Security Assessment

ADAPTIVE SHIELD