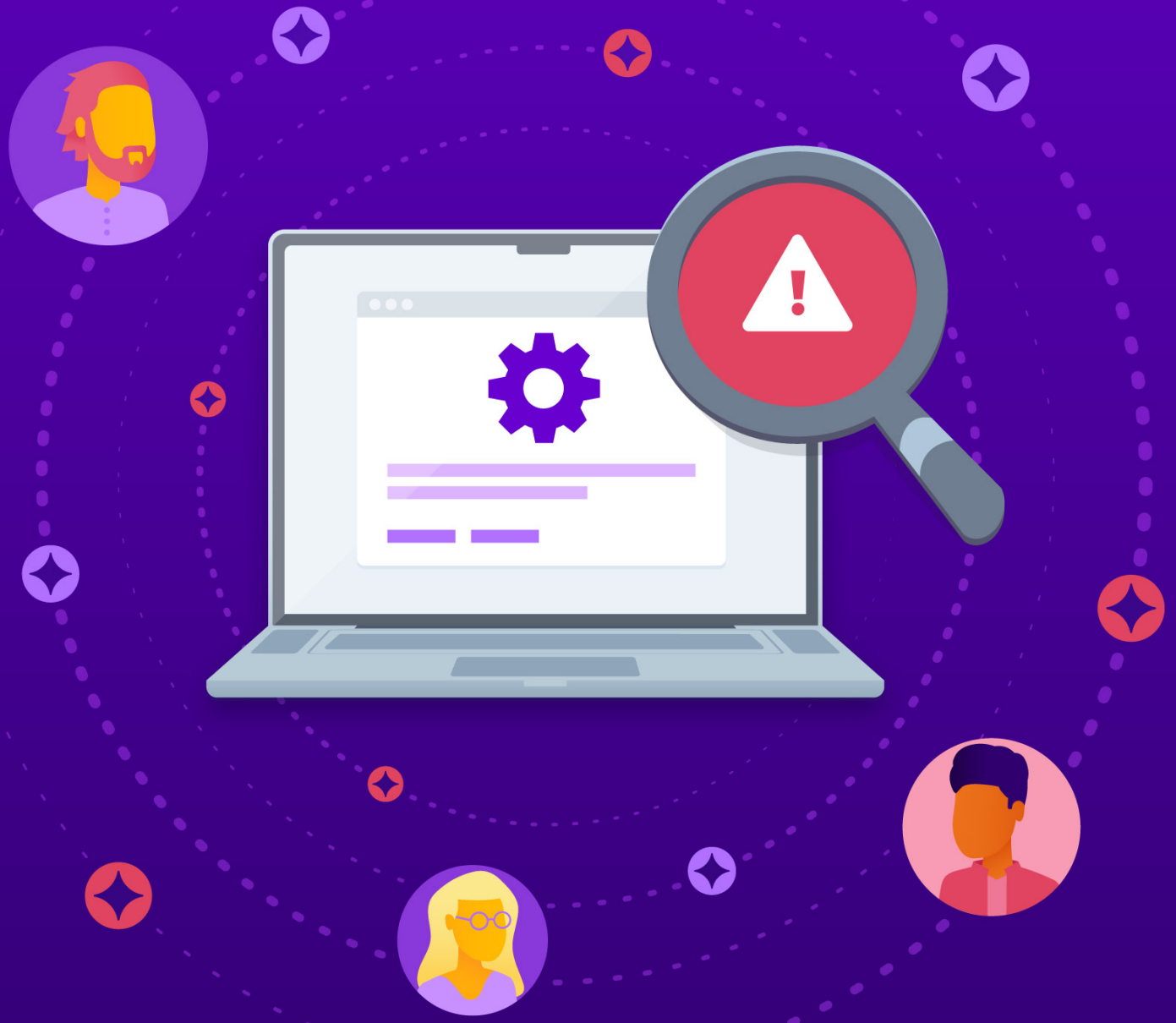
SaaS AI-Risk for Mid-Market Organizations

2025 Survey Report



WING Security

CSA cloud security alliance®

Acknowledgments

Lead Author

Hillary Baron

Contributors

Josh Buker
Marina Bregkou
Ryan Gifford
Sean Heide
Alex Kaluza
John Yeoh

Graphic Design

Claire Lehnert
Stephen Lumpe

Special Thanks

Ran Senderovitz and Brian Fravel

About the Sponsor

Wing Security is dedicated to protecting organizations from SaaS-related threats. With comprehensive SaaS Security Posture Management (SSPM) and Identity Threat Detection and Response (ITDR), Wing's platform provides continuous visibility and control over critical apps, SaaS configurations, and app-to-app connectivity. Designed to simplify SaaS security management, Wing equips security teams with essential context and flexible remediation capabilities to address SaaS risks effectively, ensuring smooth business operations and continuity.

https://wing.security/

Table of Contents

Acknowledgments 3
Executive Summary 5
- Key Findings at a Glance 5

Key Findings 6
- Key Finding 1: Security Teams Are Struggling with a Growing Attack Surface and Tracking Application Use 6
- Key Finding 2: Mid-Market Organizations Prioritize Critical Apps Protection Resulting in Security Gaps 7
- Key Finding 3: AI-Related Risks Are a Growing Concern, but Organizations Lack a Formal Plan 9
- Key Finding 4: SaaS Security Strategy Is Hindered by Insufficient Tooling and Reliance on Manual Processes 10
- Key Finding 5: SaaS Security Embedded and Growing Through Current Security and IT Initiatives 12

Full Survey Results 15
- Overview 15
- SaaS Risks 16
- AI Risks and Concerns in SaaS 19
- Budget and Plans for the Future 21

Demographics 23
Survey Methodology and Creation 24
- Goals of the Study 24

Executive Summary

Mid-market organizations are facing a growing challenge: managing an expanding Software as a Service (SaaS) environment with fewer resources than larger enterprises. This report explores how these organizations are addressing SaaS security risks, from managing misconfigurations and artificial intelligence (AI)-driven threats to overcoming budgetary constraints and limited tooling. The findings highlight the gaps in their current strategies and provide actionable insights for improving their security posture.

Key Findings at a Glance

1. A Growing Attack Surface

Mid-market organizations are grappling with managing the large volume of SaaS applications, both sanctioned and unsanctioned, with actual numbers often exceeding expectations. Limited visibility into these applications creates significant security gaps. Specialized tools and automation are essential for securing this expanding digital footprint.

2. Prioritizing "Crown Jewels" While Leaving Gaps

Many companies are concentrating their configuration management efforts on their most critical applications like Google Workspace and Identity Provider/Identity Access Management (IdP/IAM) service. Doing so is a foundational step in maintaining a strong security posture. However, while prioritizing these core systems is essential, broader SaaS environments should not be overlooked. To fully mitigate risks, organizations must expand automation and ensure comprehensive coverage across all applications, including those perceived as lower priority and application-to-application connections.

3. AI Risks Without a Formal Plan

AI-related risks, particularly to data and intellectual property, are a growing concern, but only half of organizations have dedicated teams addressing them. The absence of a unified strategy and clear accountability leaves organizations vulnerable to evolving threats and compliance challenges.

4. Reliance on Manual Processes and Insufficient Tooling

Smaller security teams often rely on manual processes and general-purpose tools like Cloud Access Security Broker (CASB), which are insufficient for SaaS security needs. Many organizations are planning to adopt specialized solutions like SaaS Security Posture Management (SSPM) and Data Security Posture Management (DSPM) to enhance visibility and address critical risks.

5. Growing SaaS Security Through Current Initiatives

Nearly 90% of organizations plan to expand IT budgets or enhance existing security initiatives—such as risk management, configuration management, and risk detection and response—to address SaaS security. However, only 3% have a dedicated line-item budget specifically for SaaS security. Dedicated funding and aligned priorities across teams remain critical for building an effective SaaS security strategy.

Conclusion

Mid-market organizations are making progress in recognizing and addressing SaaS security risks, but significant gaps remain. To build a robust security posture, these organizations should prioritize adopting specialized technologies that enhance visibility, automate processes to improve the posture and SaaS misconfiguration and address critical security gaps like Identity, Access, and Data leaks to 3rd parties and AI applications that may train on the company data. Relying on manual processes not only increases costs but also fails to provide comprehensive risk coverage. Aligning priorities across IT, security, and business units will also be critical to achieving a unified and proactive approach to SaaS security. By addressing these challenges, mid-market organizations can better safeguard their assets and navigate the evolving SaaS landscape.

Key Findings

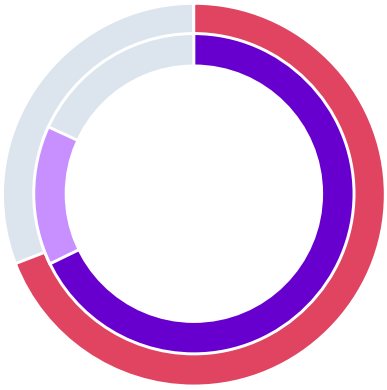
Mid-market organizations face a unique balancing act: defending a growing digital footprint without the deep pockets and vast resources of larger enterprises. This survey dives into the strategies these companies are using to protect their high-value assets, from navigating SaaS security gaps to tackling AI-related risks—often with leaner budgets and manual processes. By highlighting real-world challenges and priorities in risk management, the report uncovers critical insights for mid-sized security teams striving to stay resilient in an increasingly complex threat landscape.

Key Finding 1:

Security Teams Are Struggling with a Growing Attack Surface and Tracking Application Use

For many mid-market organizations, managing the sheer volume of both sanctioned and unsanctioned SaaS applications has become a major challenge. While 69% of companies report having 50 or fewer sanctioned applications, 68% estimate a similar number of unsanctioned ones, with 14% unsure of the exact figure. However, research from Wing Security paints a more concerning picture: organizations with around 1,000 employees actually average close to 700 SaaS applications in total (both sanctioned and unsanctioned)—far exceeding the perceived 100. This disparity underscores a significant visibility issue that could lead to potential security gaps. As the saying goes, you can't secure what you can't see.

Perceived number of sanctioned and unsanctioned SaaS application in organizations' environments



Sanctioned

69% 50 or fewer

Unsanctioned

68% 50 or fewer

14% Unsure

The survey further found that only 44% of organizations prioritize protecting all their sanctioned applications, while a mere 17% include unsanctioned ones in this priority. This points to an urgent need for stronger application management across the board. Although nearly half of respondents rely on Cloud Access Security Brokers (CASBs) to manage app security, CASBs alone are often insufficient for managing app-to-app interactions, leaked credentials, identity risks, access permissions,

Organization's approach when protecting SaaS applications

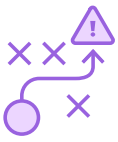
Prioritize protecting all sanctioned apps

44%

Prioritize protecting both sanctioned and unsanctioned apps

17%

misconfigurations, and unsanctioned applications. Mid-market organizations may need greater support through automated configuration management and SaaS-specific security tools to gain the visibility and control essential for managing application security risks. By bridging the gap between IT resources and security priorities, these companies can better secure their expanding digital footprint.



Key Finding 2:

Mid-Market Organizations Prioritize Critical Apps Protection Resulting in Security Gaps

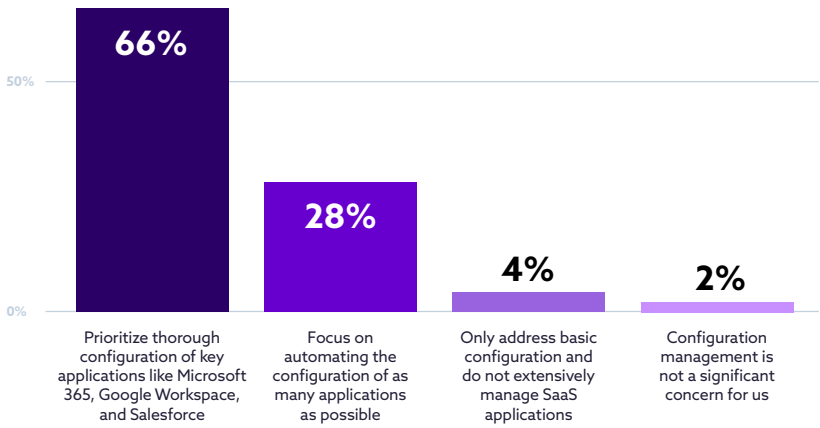
Mid-market organizations recognize the critical role of configuration management in securing their SaaS environments, with 43% identifying misconfigurations as their biggest SaaS security risk. However, constraints in resources and tooling mean that efforts to address these risks are often limited to the most critical applications, leaving less critical apps at risk.

Biggest perceived SaaS risks

43% Misconfigurations	**24%** Data breaches	**15%** Supply chain attacks
42% Unauthorized access	**24%** Data leakage	**9%** Insider risks (malicious or negligent)
27% Compliance and regulatory concerns		

While only 2% of respondents believe configuration management isn't a concern, most focus on high-priority apps rather than achieving full coverage across their SaaS environments. In fact, 66% of organizations plan to prioritize configuration management for critical applications like Microsoft 365, Google Workspace, and Salesforce—a practical and impactful starting point for strengthening their SaaS security strategy. By focusing on these "crown jewels," organizations can ensure their most essential systems are safeguarded with minimal operational disruption. At the same time, unsanctioned applications require attention to prevent potential risks. These applications should

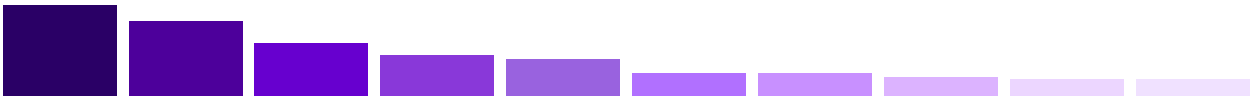
Approach to configurations management for SaaS applications



be monitored to confirm they do not store sensitive data, access critical systems through tokens or application programming interfaces (APIs), or inadvertently expose employee credentials. While only 28% of organizations currently plan to automate configuration management across all applications, balancing the protection of critical apps with better visibility into unsanctioned applications will help organizations build a more secure and resilient SaaS environment. Even these lower risk applications can potentially be a high risk decision.

The survey also revealed that API integrations (45%) and cross-department collaboration (37%) are among top priorities when it comes to SaaS security, with visibility and insights (26%) following closely. However, only 20% of organizations focus on in-depth configuration management for key apps. This is consistent with the prioritization of configuration management for just the most critical applications.

Most important features in SaaS security solutions



45%	Number of API integrations to SaaS Apps	**18%**	Threat detection capabilities	**8%**	Workflow automation
37%	Supports collaboration and shared responsibility among business units and employees	**11%**	Breadth of configuration management across many apps	**8%**	Quality of dashboard and reports
26%	Visibility and insights	**11%**	Automated remediation		
20%	Depth of configuration management in critical apps	**9%**	Ease of use		

In fact, a mere 11% extend these efforts broadly across their app ecosystem. This limited scope suggests that mid-market organizations may be prioritizing their resources and attention to the applications deemed most critical to their work. However, this could lead to overlooking the risks associated with less critical but still vulnerable applications. They're also often working with fewer resources than large organizations which may force them to make difficult decisions; however, this could leave them vulnerable.

Additionally, the rise of shadow IT, with unsanctioned applications operating outside of IT's control, often goes unaddressed. This oversight further weakens their security posture. These applications hold the identities and credentials of organizational entities. Furthermore, they may be connected through APIs to other, more critical SaaS platforms without proper vetting of their security, and accounts take over risks. To mitigate these risks, organizations should consider expanding their configuration management to include all critical SaaS applications, ideally through automated solutions, and enhance visibility into shadow IT. By broadening their approach, mid-market organizations can create a more resilient security framework that addresses vulnerabilities beyond their core applications.

Key Finding 3:

AI-Related Risks Are a Growing Concern, but Organizations Lack a Formal Plan

As AI features become increasingly embedded within SaaS applications, organizations are expressing growing concerns over the risks these features bring, particularly regarding data and intellectual property (IP) protection. The majority of organizations show a moderate to high level of concern about AI-related risks in SaaS, with 55% moderately and 20% highly concerned about potential AI risks. More specifically, data risks (41%) and IP risks (45%) are identified as top priorities, signaling that organizations are acutely aware of AI's potential threats to their critical assets. In contrast, only 6% see compliance as a pressing issue, reflecting an imbalance in risk prioritization that could lead to long-term challenges as AI regulations evolve.

Biggest concern with AI use in SaaS stack

AI risk management is further complicated by a fragmented distribution of responsibilities across departments. SaaS management, especially configuration management, is handled by IT (51%), legal teams (27%), business units (24%), and risk management (52%), with emerging AI threats being overseen by a mix of security (52%), IT (45%), and legal teams (29%). This division of responsibility makes it difficult for organizations to establish consistent AI security practices, as different teams may have conflicting priorities or insufficient expertise to address AI-specific risks effectively. Moreover, while 51% of organizations rely on their security teams to manage AI risks, 33% either lack a dedicated role or are unsure who holds responsibility for AI risk management. This

Responsibility distribution for SaaS applications

lack of clear accountability introduces significant vulnerabilities, as AI risks remain unchecked and unmanaged without a structured plan.

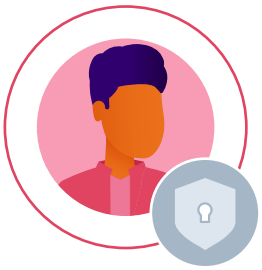
While organizations recognize the potential risks AI poses to data and IP within SaaS applications, the absence of a unified AI risk management strategy leaves critical gaps in security and compliance. To address these vulnerabilities, organizations should work toward formalizing their AI risk strategies, clearly designating accountability, and enhancing focus on regulatory compliance. Without addressing these gaps, mid-market organizations will remain exposed to emerging AI risks and evolving regulatory requirements, jeopardizing their security posture in the long run.

Key Finding 4:

SaaS Security Strategy Is Hindered by Insufficient Tooling and Reliance on Manual Processes

Mid-sized organizations are increasingly aware that their current security tools and manual processes are not keeping pace with the complexity and risks posed by SaaS applications. While security teams are often smaller than IT teams—55% of security teams have only 6-10 members compared to IT teams with 44% with 6-10 members and 25% with 11-15 members—these teams are tasked with managing a growing number of both sanctioned and unsanctioned SaaS applications. This imbalance leaves security teams stretched thin, facing challenges in maintaining visibility and control, which increases the risk of misconfigurations and unauthorized access.

How many members are on your organization's security team vs IT team?



Security team

55% 6 - 10 members

7% 11 - 15 members

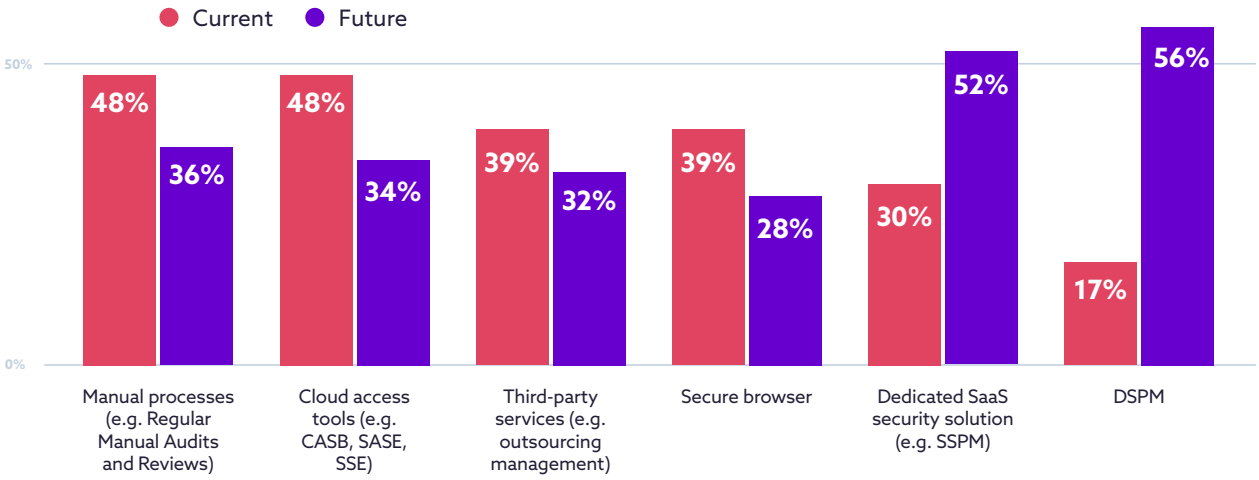
IT team

44% 6 - 10 members

25% 11 - 15 members

Security teams in many of these organizations are performing dual roles, often handling both security and IT responsibilities. This overlap may blur the lines between functions, but it doesn't reduce the growing demands of SaaS security. Currently, 48% of organizations rely on manual processes to manage SaaS risks, and another 48% utilize Cloud Access Security Brokers (CASB) for oversight. However, fewer organizations use more specialized tools like SaaS Security Posture Management (SSPM) or Data Security Posture Management (DSPM), with only 30% and 17% adoption, respectively.

Current and planned use of tools for managing risk and threats for SaaS supply chain



This reliance on manual oversight and general-purpose tools like CASB reflects a gap in the SaaS security strategy for most organizations. Recognizing these limitations, many organizations plan to utilize SSPM (52%) and DSPM (56%) solutions to enhance visibility, automate critical processes, and address high-priority risks, such as data protection and misconfigurations some time in the future. The planned shift toward specialized tools underscores an understanding that SSPM and DSPM solutions are better suited to meet the specific demands of SaaS security.

Additionally, many organizations struggle with basic SaaS security management functions due to a lack of centralized tracking (36%), notifications for app updates (30%), control over update frequency (27%), and the sheer volume of applications (22%). These pain points illustrate that, while organizations desire more robust SaaS security tools, their current tooling falls short, and manual processes only provide reactive security measures rather than proactive risk management.

Most challenging aspects of tracking terms and conditions for SaaS applications

36% Lack of tools to centralize tracking	**22%** Number of applications	**15%** Tracking third-party data sharing
30% Notification of updates in timely manner	**20%** Resource contraints	**13%** Difficulty understanding complex legal language
28% Frequency of updates	**17%** Diversity of data use policies	**12%** Vendor transparency

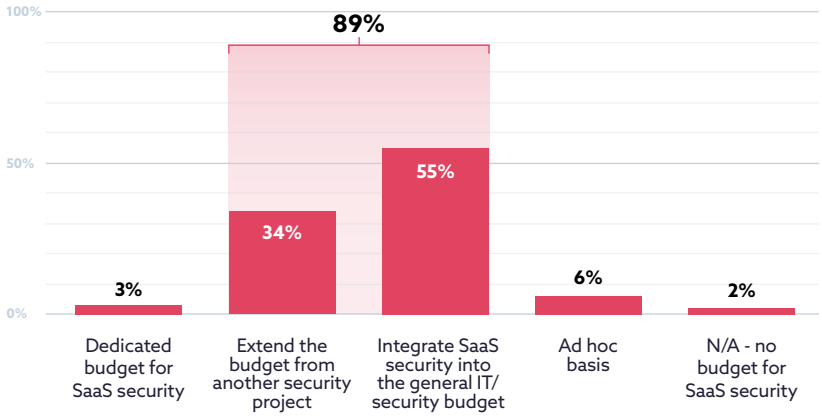
As mid-sized organizations move toward adopting SSPM and DSPM tools, they will be better positioned to protect critical assets, minimize risks, and build a more comprehensive security posture. However, until these specialized tools are fully in place, organizations will continue to face challenges in keeping up with the evolving SaaS landscape, impacting their ability to stay agile and innovate securely to avoid falling into a reactive security posture.

Key Finding 5:

SaaS Security Embedded and Growing Through Current Security and IT Initiatives

While organizations recognize the importance of securing their SaaS environments, and 52% plan to utilize SSPM tools in the future, due to budget constraints and a lack of dedicated funding, this creates significant barriers to implementing effective SaaS security strategies. Only 3% of organizations report having a dedicated budget for SaaS security, reflecting that very few view it as a standalone priority. Instead, most organizations (89%) integrate SaaS security into broader initiatives like risk management, compliance, and Identity posture. This approach extends existing priorities into the SaaS domain, reflecting an increasing focus on addressing SaaS-specific risks within the context of overall security efforts. However, relying on general IT or security budgets (55%) or reallocating funds from other projects (34%) can lead to reactive, patchwork investments that fail to fully address the unique risks SaaS applications pose. As SaaS security becomes more integrated into organizational priorities, extending these efforts thoughtfully will be key to building a comprehensive and effective strategy.

Budget for SaaS security



Security domains that currently have security budget

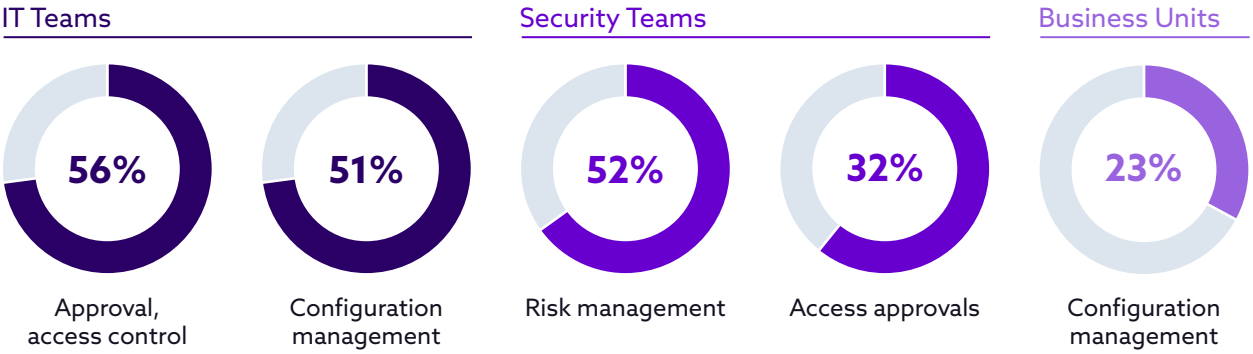
53%	Risk Management	**28%**	Threat Detection and Response	**14%**	AI Governance
40%	Compliance	**26%**	Data Protection and Data Loss Prevention (DLP)	**9%**	Dedicated SaaS Security/ SSPM Project/ Platform
29%	Identity Management	**25%**	Configuration Management		
28%	Asset, Software, and Services Supply Chain Management	**23%**	Non-Human Identities		

Risk management (53%) and compliance (40%) dominate funding priorities, both of which are critical for SaaS security. However, bundling SaaS security into these broader initiatives can dilute focus and prevent targeted investments in specialized tools like SaaS Security Posture Management (SSPM) or

Data Security Posture Management (DSPM). This lack of specificity leaves critical gaps in the security posture, particularly in areas like configuration management and data protection, where SaaS-specific risks require tailored solutions.

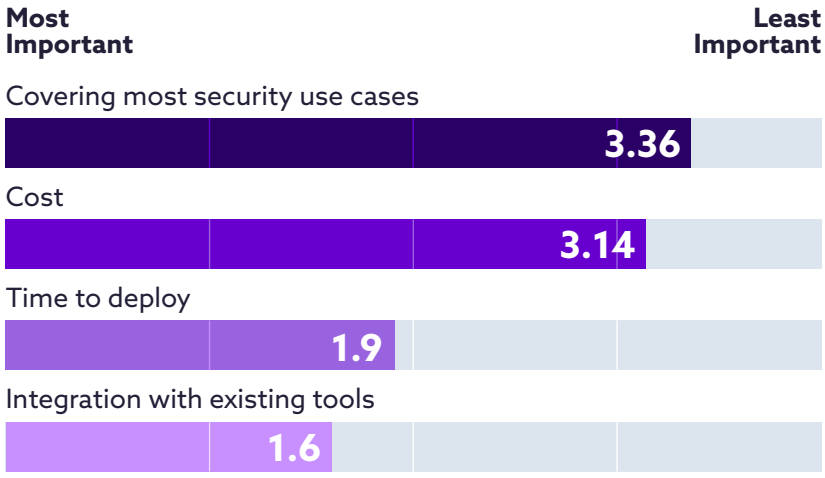
Additionally, SaaS security responsibilities are fragmented across departments. IT teams are heavily involved in phases like approval, access control (56%), and configuration management (51%), while security teams lead risk management (52%) and access approvals (32%). Business units are also involved in critical tasks like configuration management (23%). This distributed responsibility makes it difficult to consolidate resources and prioritize security investments, further contributing to the reliance on general IT funds and the challenges of orchestrating efforts across teams.

Responsibility distribution for SaaS applications



Cost is the second most important consideration when selecting SaaS security tools, rated at 3.14 on a scale of 1-4 (where a higher average ranking indicates more important), just behind coverage of security use cases (3.36). This cost-conscious mindset explains why many organizations lean on general-purpose tools or manual processes, which are often insufficient for addressing the specific challenges of SaaS environments. While cost considerations are necessary, overreliance on low-cost or less-specialized solutions can leave organizations vulnerable to risks like data breaches, misconfigurations, and compliance violations.

Order of most important aspects of SaaS security tools



Organizations are beginning to extend their budgets in targeted areas, including risk management (33%), asset, software, and services supply chain management (27%), configuration management (26%), and data protection and loss prevention (25%). These planned investments suggest that while SaaS security may currently lack dedicated funding, organizations are starting to acknowledge its importance within their broader security strategy.

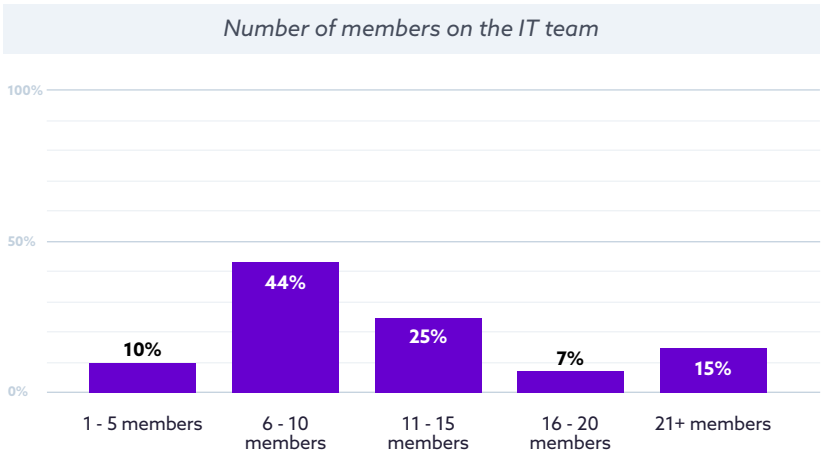
Security domains that will receive additional budget in the next 12 months

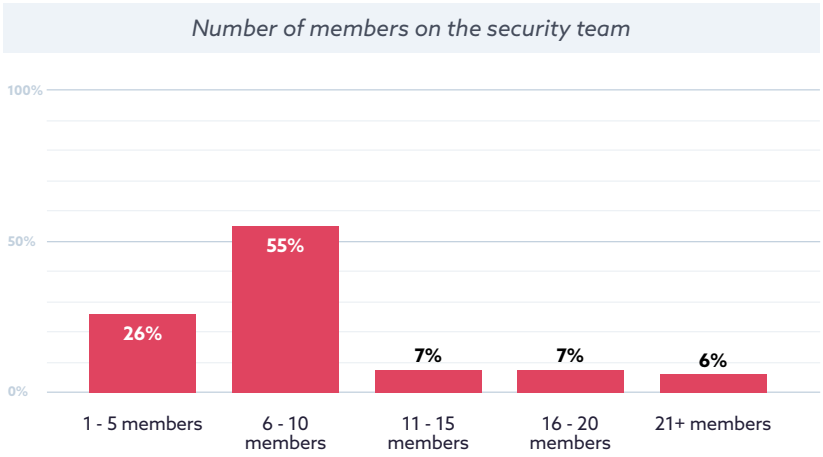
33%	Risk Management	**21%**	Compliance	**14%**	Non-Human Identities
27%	Asset, Software, and Services Supply Chain Management	**20%**	Identity Management	**14%**	Threat Detection and Response
26%	Configuration Management	**19%**	AI Governance		
25%	Data Protection and Data Loss Prevention (DLP)	**15%**	Dedicated SaaS Security/ SSPM Project/ Platform		

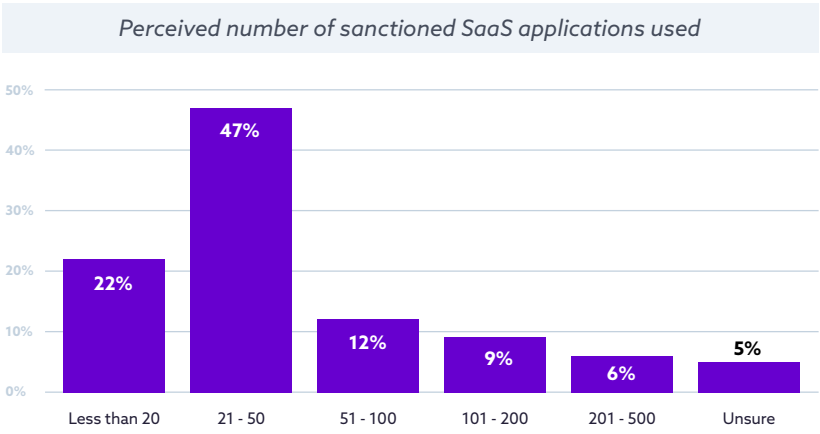
Mid-sized organizations face significant challenges in balancing cost, ownership, and coverage of use cases while addressing the unique demands of SaaS security. To strengthen their security posture, organizations must prioritize dedicated investments in specialized tools like SSPM and DSPM. Equally critical is aligning teams across IT, security, and business units to consolidate efforts and resources, ensuring a more cohesive and proactive approach to SaaS security. By addressing these barriers, organizations can build a more robust and cost-effective security strategy tailored to the complexities of SaaS environments.

Full Survey Results

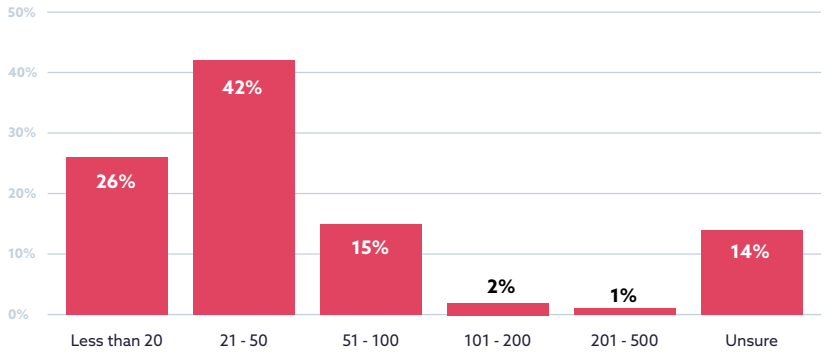
Overview







Perceived number of unsanctioned SaaS applications used



Most important features in SaaS security solutions

45% Number of API integrations to SaaS Apps

37% Supports collaboration and shared responsibility among business units and employees

26% Visibility and insights

20% Depth of configuration management in critical apps

18% Threat detection capabilities

11% Breadth of configuration management across many apps

11% Automated remediation

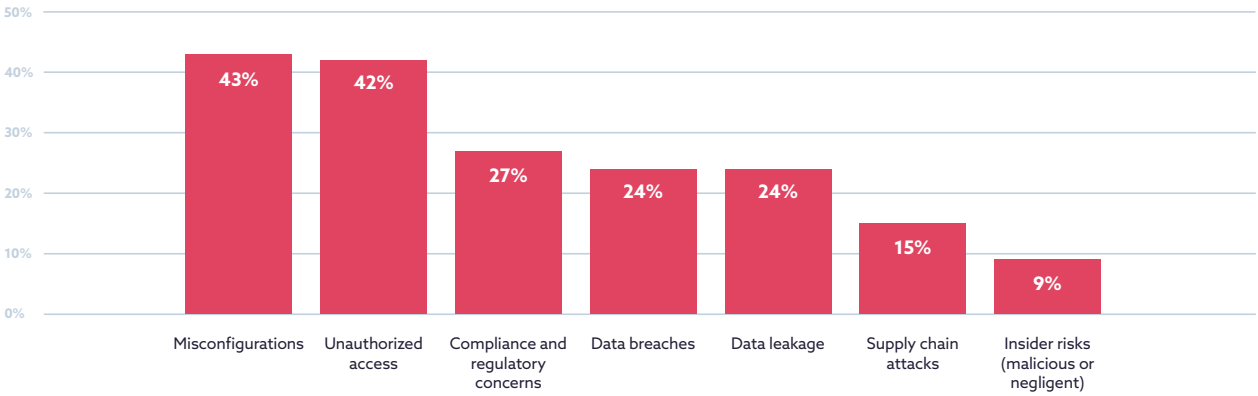
9% Ease of use

8% Workflow automation

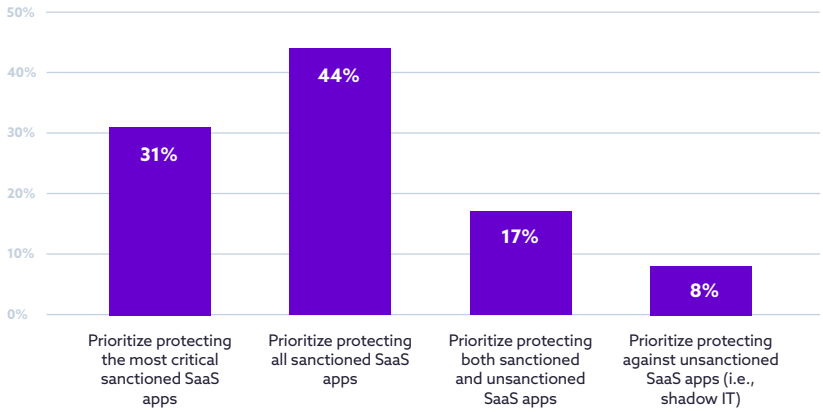
8% Quality of dashboard and reports

SaaS Risks

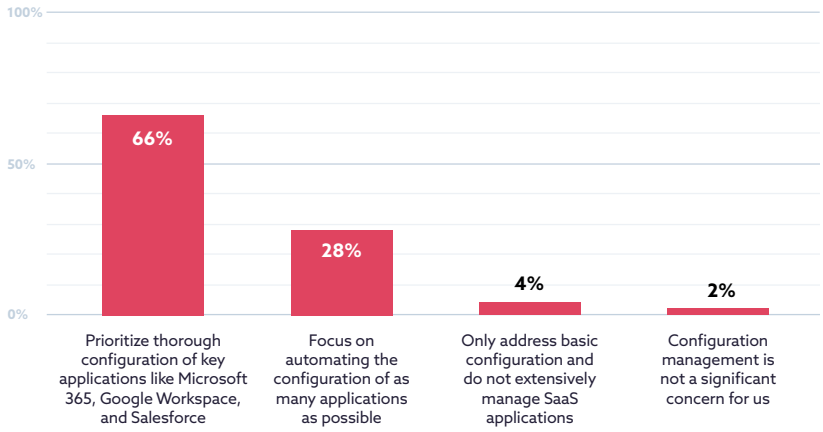
Biggest SaaS security risks



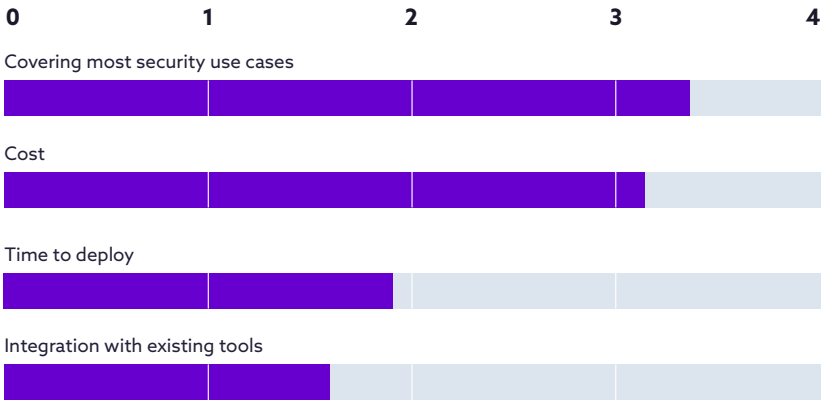
Priorities when protecting SaaS applications



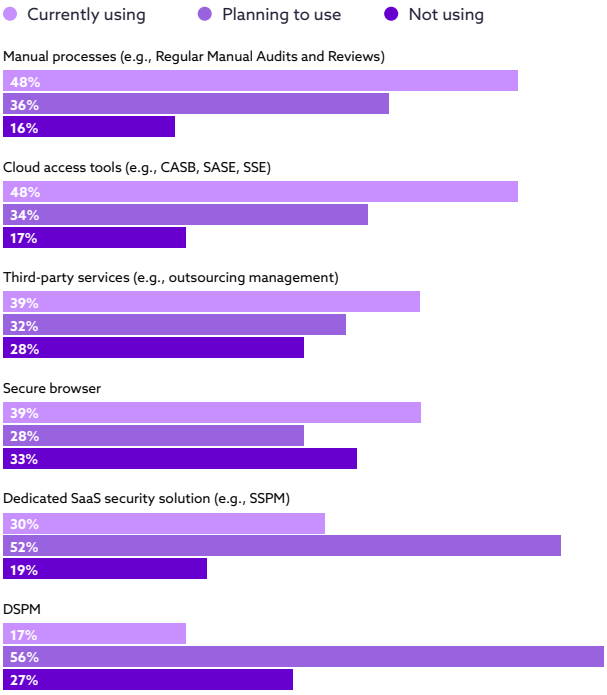
Approach to configurations management for SaaS applications



Order of most important aspects of SaaS security tools
(Most important = 1, least important = 4)

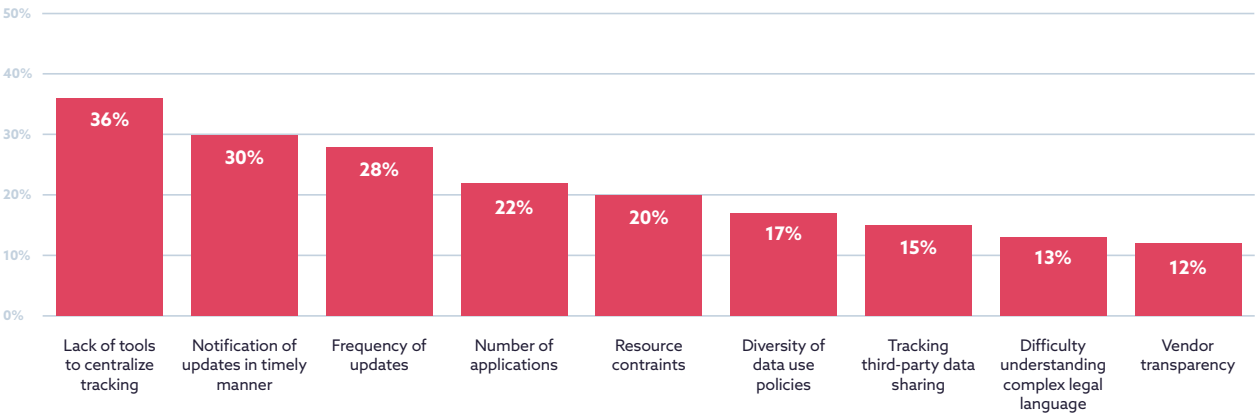


Current and planned use of tools for managing risk and threats for SaaS supply chain



Responsibility distribution for SaaS applications

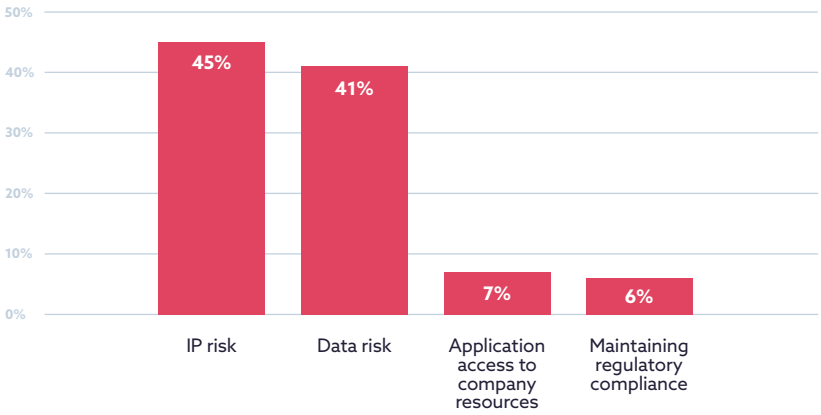
Most challenging aspects of tracking terms and conditions for SaaS applications



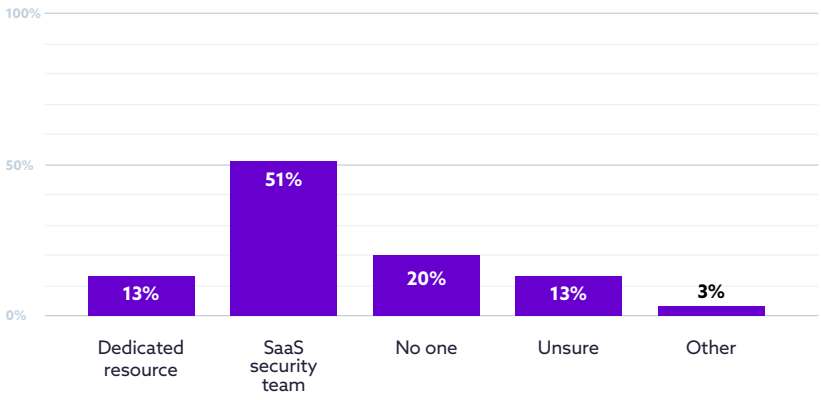
AI Risks and Concerns in SaaS

Sentiments of security experts toward AI features launching in SaaS applications

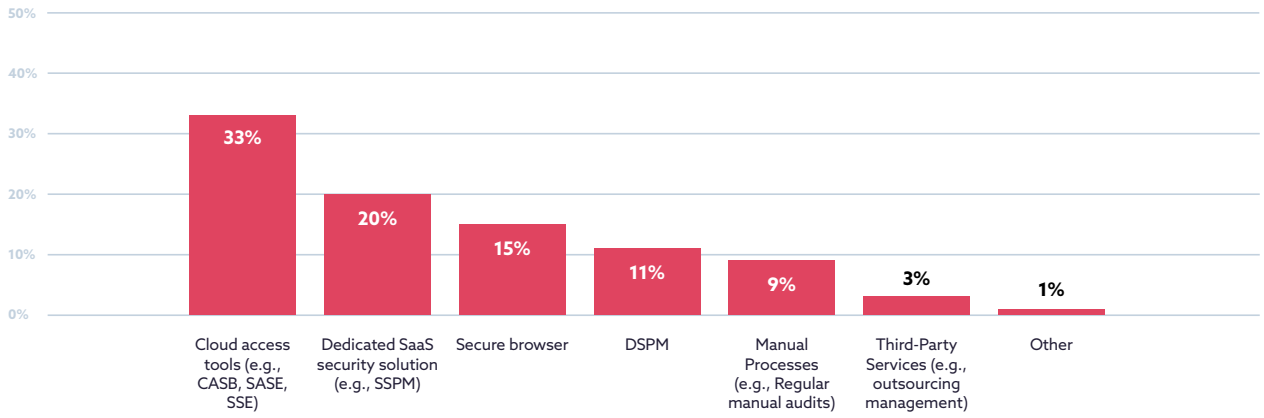
Biggest concern with AI use in SaaS stack



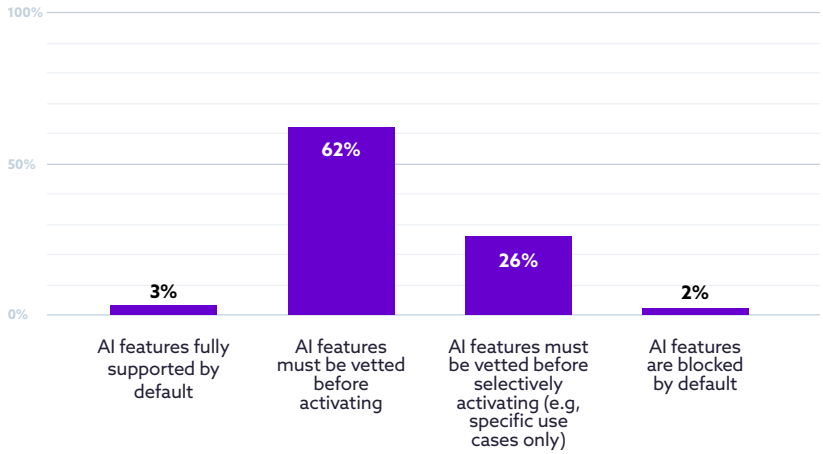
Responsibility for tracking SaaS AI risk



Tools and strategies for discovering and monitoring AI risk

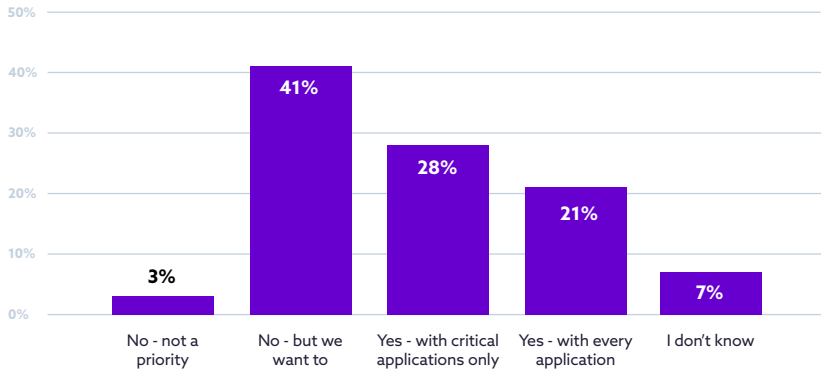


Plan to handle AI features in SaaS applications



Does your organization prioritize productivity or data protection when it comes to AI-based apps?

Tracking tool for SaaS applications' use of data for training AI

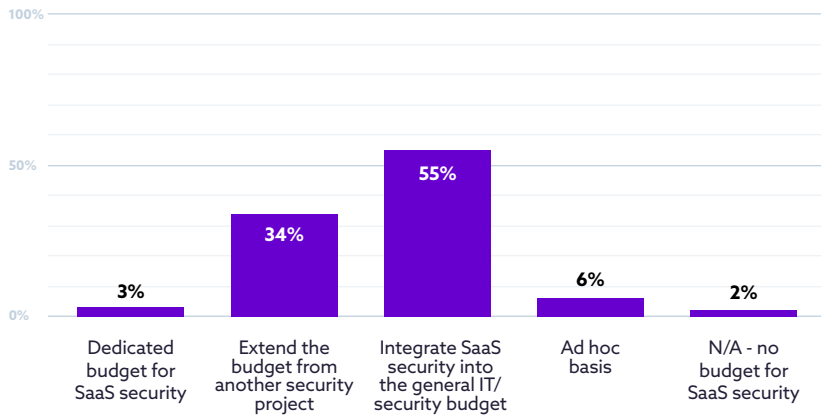


Plans to protect IP and data in AI-based applications

42%	AI-Specific security tools	20%	Risk-based approach	15%	Integrated AI security framework
34%	Behavior monitoring	18%	Compliance monitoring	12%	Strict policy enforcement
25%	Employee training and awareness	18%	Regular audits	3%	N/A - we won't use AI-based apps
24%	Data access controls	17%	Configuration monitoring	2%	Other
24%	Data anonymization techniques	16%	Third-party security services (i.e., outsourcing)	1%	Not a concern

Budget and Plans for the Future

Budget for SaaS security



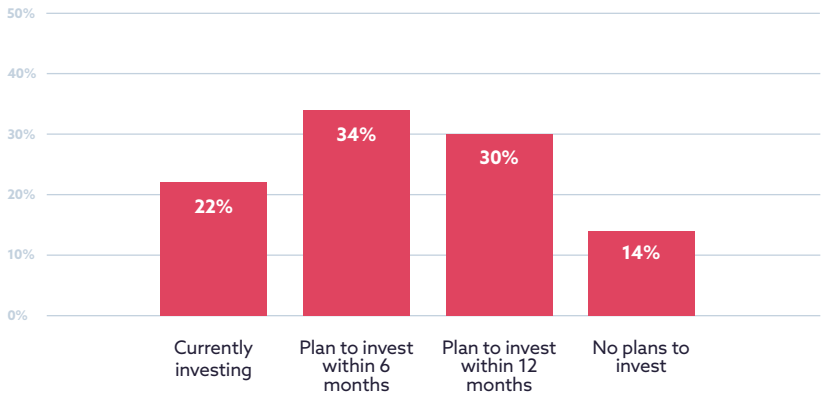
Security domains that currently have security budget

53%	Risk Management	28%	Threat Detection and Response	14%	AI Governance
40%	Compliance	26%	Data Protection and Data Loss Prevention (DLP)	9%	Dedicated SaaS Security/ SSPM Project/ Platform
29%	Identity Management	25%	Configuration Management		
28%	Asset, Software, and Services Supply Chain Management	23%	Non-Human Identities		

Security domains that will receive additional budget in the next 12 months

33%	Risk Management	21%	Compliance	14%	Non-Human Identities
27%	Asset, Software, and Services Supply Chain Management	20%	Identity Management	14%	Threat Detection and Response
26%	Configuration Management	19%	AI Governance		
25%	Data Protection and Data Loss Prevention (DLP)	15%	Dedicated SaaS Security/ SSPM Project/ Platform		

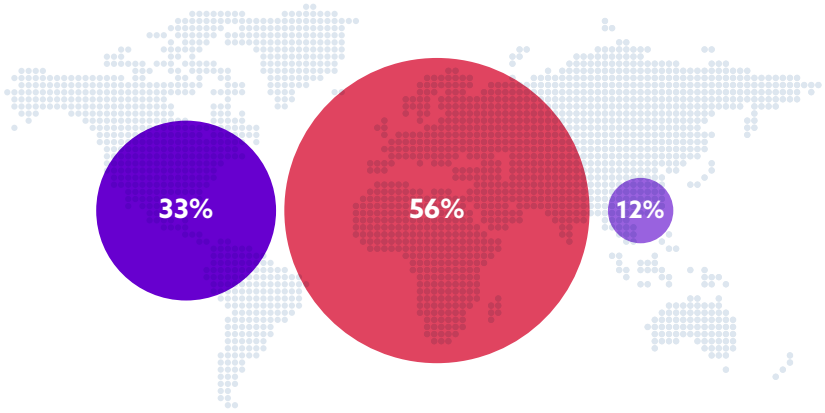
Plans to invest in solutions or features to protect SaaS from AI-based risk



Demographics

What region of the world are you located in?

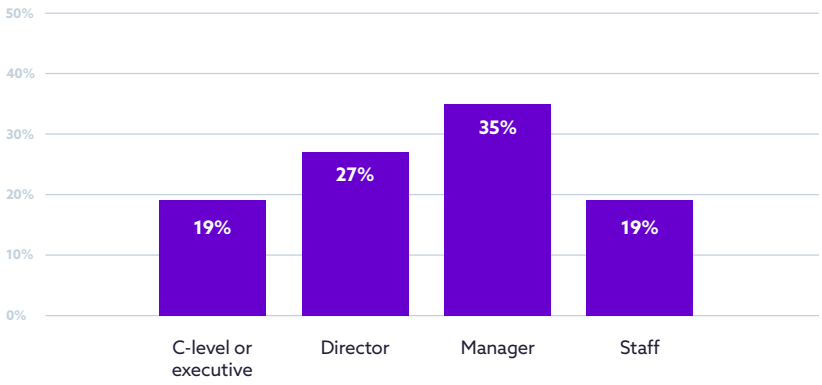
- Americas
- Europe, Middle East, Africa (EMEA)
- Asia Pacific (APAC)



What is the size of your organization?

100%
251 - 2500 employees

Which best describes your job level?



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

18%	Telecommunications, Technology, Internet & Electronics	6%	Education	1%	Food & Beverages
17%	Airlines & Aerospace (including Defense)	5%	Prefer not to answer	1%	Health & Fitness
15%	Advertising & Marketing	2%	Government	1%	Manufacturing
14%	Agriculture	2%	Healthcare & Pharmaceuticals	1%	Nonprofit
8%	Finance & Financial Services	1%	Business Support & Logistics	1%	Retail & Consumer Durables
6%	Automotive	1%	Entertainment & Leisure	1%	Transportation & Delivery

Survey Methodology and Creation

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices and ensure 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.

Wing Security commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding SaaS security and its challenges with AI features within the SaaS stack. Wing Security financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in October 2024 and received 406 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

This survey aims to provide a comprehensive understanding of the challenges and opportunities mid-market organizations face in securing their SaaS environments. The specific goals include:

1. **Understanding Strategies and Priorities for SaaS Security**
   Explore how organizations approach securing their SaaS applications, including the tools and methods they rely on, key focus areas, and the extent to which they prioritize visibility, configuration management, and automation.
2. **Examining Concerns Around AI Risks in SaaS**
   Assess the level of concern organizations have regarding the integration of AI within SaaS applications, particularly around data protection, intellectual property, compliance, and other emerging risks. Identify how these concerns influence current security practices and strategies.
3. **Evaluating Resources Available for SaaS Security**
   Analyze the resources organizations allocate to SaaS security, including the size and structure of security teams, the distribution of responsibilities across IT, security, and business units, and the extent of reliance on manual processes versus automation.
4. **Exploring Plans and Budgeting for SaaS and AI Security**
   Investigate future plans for SaaS and AI security, including budget allocation, adoption of specialized tools such as SaaS Security Posture Management (SSPM), and strategies for addressing gaps in visibility, risk management, and compliance.