AppOmni

The State of SaaS Security

2024 REPORT

Table of Contents

Foreword

We are excited to share our second annual State of SaaS Security Report, which examines the industry's understanding of and attitudes toward SaaS security, as well as organizations' maturity and goals for their cybersecurity programs. SaaS has come a long way from its early days of use in isolated departments, and now underpins modern businesses across every function.

Last year's report highlighted the disconnect between actual SaaS risks and security self-assessments at many enterprises. This year, we gathered unique insights from security decision makers and managers from 644 organizations to gain a better understanding of the real-world security challenges that arise from prolific SaaS usage. Nearly half of the sample came from enterprise-sized companies with over 2,500 employees. Our respondents were from six countries including the United States, France, Germany, the United Kingdom, Japan and Australia. Respondents spanned across multiple security roles with 25% belonging to leadership and management roles and 75% to IT and security specialist roles.

Our survey findings, conversations, SaaS war stories over the last year, and the current regulatory environment make it clear that SaaS security must mature. Even as we write this report, our industry is dealing with the sobering reality of yet another major SaaS security breach, this time involving the databases of over 165 customers of Snowflake. Attackers continue to wreak havoc by stealing data, holding companies ransom, disrupting business operations, and damaging organizations' reputations. This year's survey found that more SaaS incidents are being exploited, with 31% (up 5 points from last year) of respondents indicating that their organizations suffered a data breach.

Fortunately, SaaS security is now getting the attention it requires. But initial deployment policies and ad hoc strategies don't lead to repeatable best practices, collaboration, or the continuous vigilance required to maintain a robust and comprehensive SaaS security program. Our study surfaced the challenges posed by decentralized governance and the confusion around shared responsibilities for SaaS security, both of which are exacerbated by a complex web of connected applications.

As attacker TTPs and preventable security issues are becoming more widely-known, there are signs that CISOs and their teams are prioritizing SaaS risks among their cloud security initiatives—even as budget pressures intensify. The days of waiting on SaaS vendors as the primary security providers for your SaaS estate are over. As the operating system of business, your SaaS estate requires a well-structured security program, organizational alignment on responsibility and accountability, and continuous monitoring at scale. We structured this year's report to share important insights from the survey and key takeaways that you can use to make informed decisions as you build your SaaS security program.

Brendan O'Connor

CEO and co-founder, AppOmni

Key Findings

#1

DISPERSED DUTIES AND DOMAINS

Decentralization of SaaS security responsibilities has blurred lines among the CISO, business owner of the SaaS application, and the cybersecurity team. The gap between accountability and responsibility contributes to organizational tension.

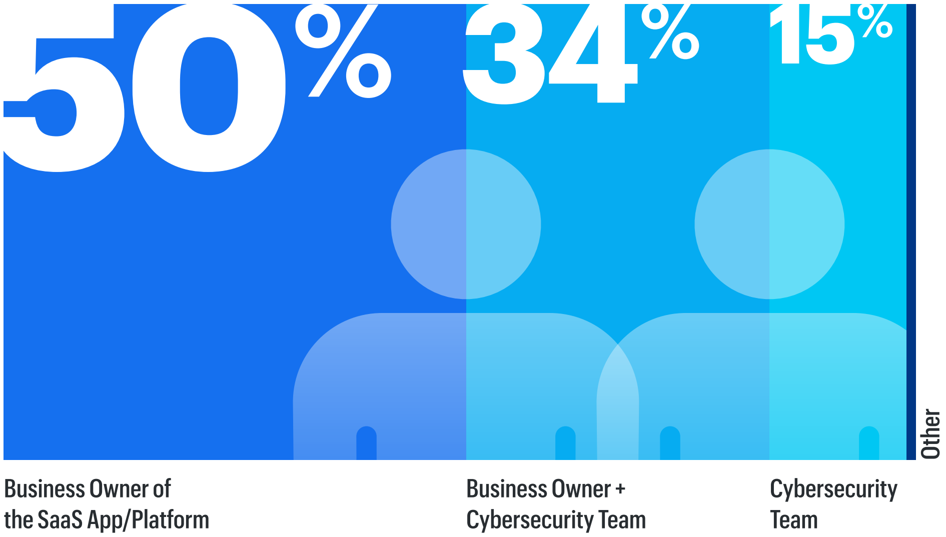
Survey data indicates that the responsibility over SaaS security controls and decision-making has grown unclear. What was once a centralized affair in which computing infrastructure was hosted on-site and offline security measures were used (e.g. badges, guards, and cameras), IT and security governance of SaaS applications have now dispersed across the cloud, different devices, and various personas.

Because SaaS apps are easy to adopt and deploy at the business unit level, these apps have empowered departments outside of traditional IT purview to independently purchase and implement solutions that cater to their needs. Additionally, each department within large enterprises is increasingly operating as its own tech hub.

While decentralization of SaaS app procurement and use enables streamlined productivity, it dilutes centralized control that once mitigated security risks and makes it difficult to recognize deviations from their policies and governance model.

These changes have reshaped the CISO's domain, contributing to ambiguity around responsibility and authority over SaaS security.

Who carries SaaS Cybersecurity responsibility?



What's more, 50% of respondents indicated that, in their organization, the responsibility for securing SaaS rests entirely on the business owner or stakeholder. Only 15% of organizations indicated that responsibility for SaaS security is centralized in the organization's cybersecurity team.

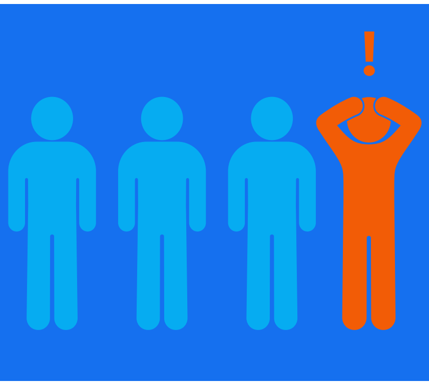
Only 15%

of organizations indicated that **responsibility for SaaS security is centralized in the organization's cybersecurity team**.

But despite the shift in SaaS security responsibilities, accountability and governance structures haven't kept up. When SaaS data breaches occur, stakeholders still look to the Chief Information Security Officer (CISO) for answers and solutions. They bear the brunt of the fallout, not the individual business units who've adopted and implemented the SaaS apps.

This disconnect between responsibility for security and accountability for failures introduces organizational tension. CISOs are placed in a precarious position in which they're held accountable for cybersecurity breaches in systems that they neither completely controlled nor implemented.

Regulatory Pressure for CISOs



25%

of survey respondents believe that the increasing **regulatory pressure for CISO level accountability** will be among the most important cybersecurity discussions in the coming months.

Key Takeaways

Because the decentralization of SaaS security controls has largely flown under the radar, many do not understand how SaaS security has been influenced by:

1. **Competing business goals**
   The foundational changes required for comprehensive SaaS security governance oftentimes took a backseat to other goals such as improving revenue potential, agility, and operational efficiencies.

2. **Slow, incremental changes to governance structures**
   Even though SaaS adoption has been swift and widespread, cybersecurity governance—or the set of policies, procedures, and processes that help an organization protect its crown jewels and to manage cyber risks—has been comparatively slow to evolve.

3. **Standardized cybersecurity practices across SaaS apps**
   While business owners or department heads are increasingly autonomous in their use of digital tools, they often lack the knowledge to implement security controls to manage their organization's attack surface. And because there is so much autonomy at the app-owner level regarding security controls, it's difficult to implement consistent cybersecurity measures to protect against app-specific vulnerabilities.

Key Findings

#2

ADOPTION ≠ AWARENESS

Organic adoption of SaaS apps does not automatically mean widespread awareness of associated risks. The extent of risks associated with SaaS-to-SaaS connections is unclear.

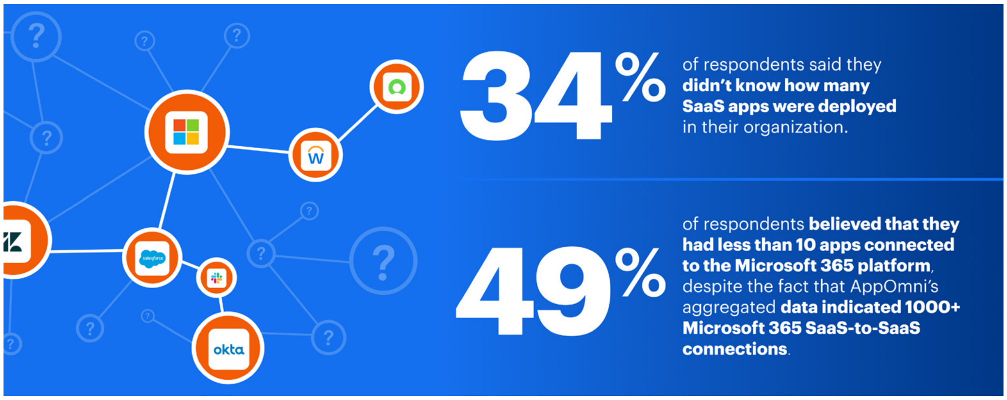
Just as organizations naturally adopt more SaaS apps, they also see a surge in essential third-party app integrations which offer numerous benefits: extended functionalities, automated workflows, unified and remote access to data, and improved collaboration.

Research indicates that the **number of SaaS-to-SaaS connections** is, most likely several orders of magnitude, in the **tens of thousands**.

Business units or individuals often bypass traditional IT procurement processes to adopt new third-party SaaS apps that seamlessly integrate with their core SaaS platforms. Think Salesforce integration with Slack or connecting Gong with Zendesk.

However, most organizations don't have the ability to see into their entire SaaS-to-SaaS footprint, therefore underestimating the inherent risks of third-party integrations to any enterprise. Case in point:

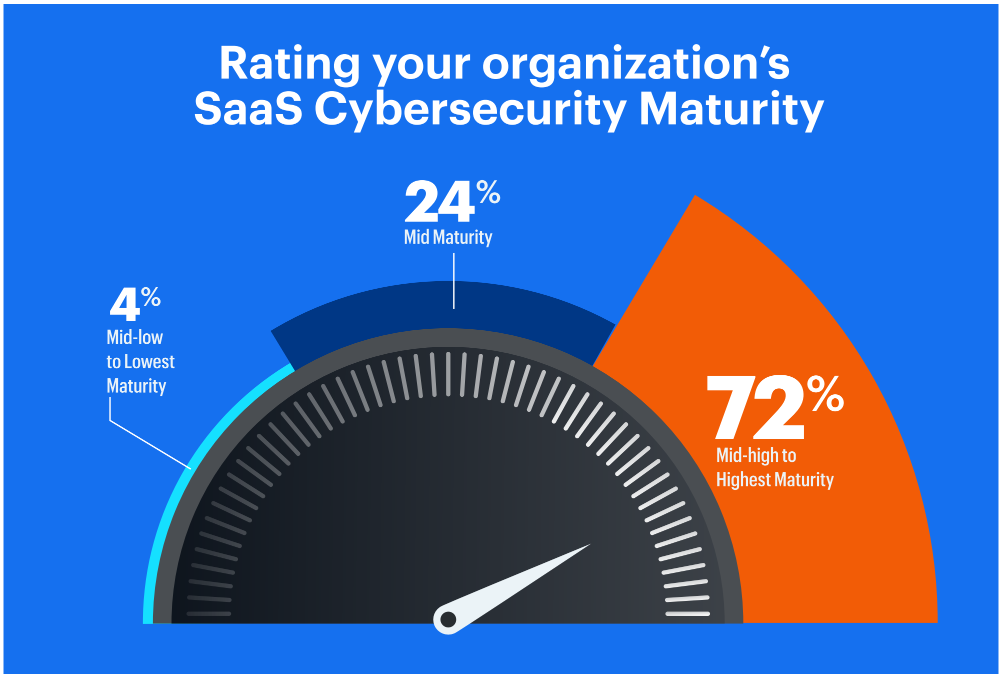
- 34% of respondents said they didn't know how many SaaS apps were deployed in their organization.
- 49% of the respondents who frequently used Microsoft 365 believed that they had less than 10 applications connected to the platform, despite the fact that AppOmni's aggregated data indicates that there are 1,000+ Microsoft 365 SaaS-to-SaaS connections on average per deployment.



34% of respondents said they **didn't know how many SaaS apps were deployed** in their organization.

49% of respondents **believed that they had less than 10 apps connected to the Microsoft 365 platform**, despite the fact that AppOmni's aggregated **data indicated 1000+ Microsoft 365 SaaS-to-SaaS connections**.

Respondents' declared lack of visibility into SaaS app risks might explain why 72% of survey respondents rated their organization's SaaS security maturity at a mid-high to highest level. Despite numerous high-profile SaaS related data breaches that made headlines in 2023, respondents gave their organization the same maturity rating as last year.



Key Takeaways

1. **Getting visibility into the entire SaaS attack surface**
   is a critical first step in an organization's SaaS security journey.

2. **Managing third-party SaaS risks**
   involves continuously monitoring SaaS connections and maintaining strict security controls, such as blocking unsanctioned third-party apps from connecting to business-critical apps that hold sensitive customer data.

3. **Cultivating a SaaS-aware security culture**
   in an organization involves ongoing collaboration between the CISO and their security team.

Key Findings
#3

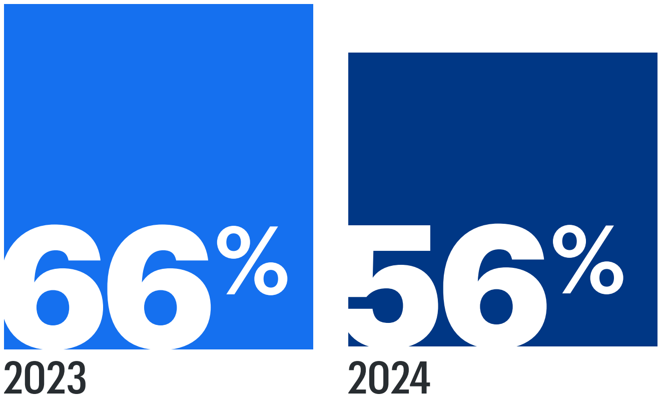
PRACTICAL ENFORCEMENT OF POLICIES IS LAGGING

Organizations overestimate how broadly and effectively their policies are being implemented.

The lack of visibility into SaaS risk extends beyond a lack of visibility into SaaS-to-SaaS connections and encompasses security policy enforcement for SaaS apps. Even with policies to regulate the use of SaaS applications in place, their practical enforcement often falls behind.

90% of respondents declare that their organizations have policies in place to allow the use of only sanctioned apps. However, 34% believed that their organization's policies, which allow only the use of sanctioned SaaS apps, are not strictly enforced at a practical level. This percentage rose by 12 points since 2023, highlighting the significant challenge in enforcement.

Organizations with strictly controlled SaaS app usage policies



Significantly fewer respondents indicated this year that their company's security policy that allows only the use of sanctioned SaaS apps is strictly controlled by the organization's cybersecurity team.

Unsanctioned SaaS apps don't undergo the same rigorous security vetting as those deployed by IT teams, nor do they always conform to the organization's data governance policies. Consequently, unsanctioned SaaS apps and lax enforcement have turned SaaS apps into an expansive and largely invisible attack surface that can result in security issues such as data leaks and regulatory non-compliance.

Survey data suggests that, while individuals are now less confident that their organizations consistently enforce SaaS app security policies, individuals still generally overestimate the strength and efficacy of their organization's existing SaaS security measures.

Key Takeaways

Historically, organizations focused primarily on managing the use of unsanctioned SaaS applications, but survey data suggests that not enough effort has gone into consistently managing policies even for security-approved apps. SaaS apps vary widely in how they handle policies, events, and controls to manage access and permissions. Therefore, ad hoc management of policies on a per application basis can lead to inconsistent implementation.

To ensure that policies are implemented consistently, organizations should:

1. **Set up the correct baseline policies**
   for all business-critical SaaS apps.

2. **Understand who has access to what data**
   in those apps, and see how permissions have changed over time.

3. **Monitor SaaS applications for policy drift over time**
   as SaaS vendors provide software updates and users are added or decommissioned.

Key Findings

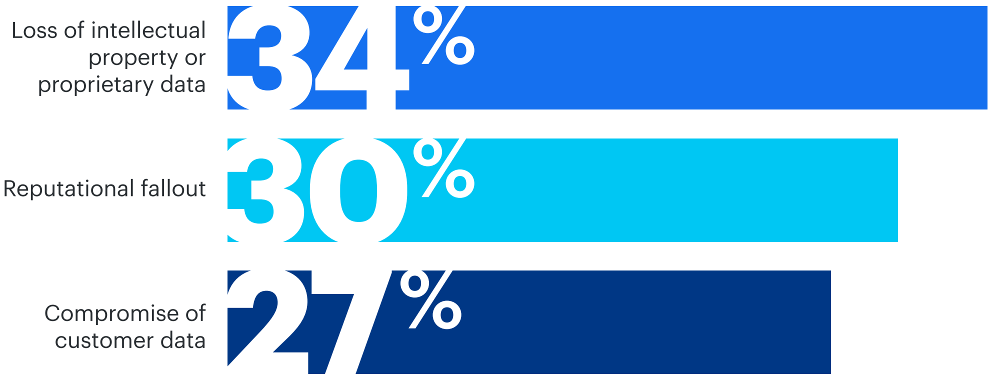
#4

SECURITY OF SANCTIONED APPS: CONFIDENCE IN DECLINE

High-profile data breaches have shaken organizations' confidence, but many remain unaware of ongoing incidents.

Cybersecurity leaders and practitioners stated that [1] the loss of intellectual property or proprietary data, [2] reputational fallout, and [3] compromise of customer data are their most pressing concerns in 2024. These issues highlight that, although customer data breaches are damaging, the theft or compromise of company-owned intellectual property represents a severe threat to any company's future.

What, if any, are your top 2 concerns around the security of SaaS Applications?



Considering the amount of SaaS data breaches that made headlines due to their scope and severity—e.g. the Sisense incident that triggered an alert from the U.S. Cybersecurity and Infrastructure Agency (CISA)—the resulting reputational damage not only undermines market trust but also has long-term financial consequences including a dip in stock prices, expensive legal battles, and higher insurance premiums.

These factors could also contribute to the decrease in reported confidence (27%) regarding security levels of sanctioned apps—or those that went through a traditional security procurement and vetting process; down from 32% in 2023. There's also a marked decline in confidence regarding the security of their company's or customers' data stored in SaaS apps, from 43% in 2023 down to 32% in 2024.

But surprisingly, almost a quarter of respondents (24%) declared that their organization experienced no SaaS cybersecurity incidents that they're aware of. This is consistent with last year's findings, which showed a notable overestimation of SaaS cybersecurity maturity levels and a concerning lack of understanding on where the responsibility for securing SaaS applications begins and ends. This is in sharp contrast to the number of organizations (31%) that declared having experienced a cyberattack resulting in a data breach, an increase from 26% in 2023.

Key Takeaways

SaaS usage is growing but so is the percentage of sensitive data in SaaS apps that, if compromised, can cause business disruptions, loss of customer trust, and damaged organizational reputation. SaaS needs to be actively secured and deserves to be on the list of CISO priorities. The good news is that while SaaS is easy to attack, some basic security controls can go a long way to securing these applications. To get started with SaaS security, make sure to:

1. **Follow your data: Where does your sensitive data reside?**
   Understanding where sensitive data sits in your organization can help you visualize your attack surface and decide which sources of risk to prioritize.

2. **Implement strong policy controls across those apps with sensitive data.**
   Access controls like SSO and MFA should never be optional.

3. **Monitor applications continuously to prevent configuration drift.**

Key Findings

#5

VIGILANCE ERODES AFTER DEPLOYMENT

Excessive emphasis on proprietary tools and initial SaaS vendor credibility hinders SaaS risk evaluation; due diligence often wanes after installation.

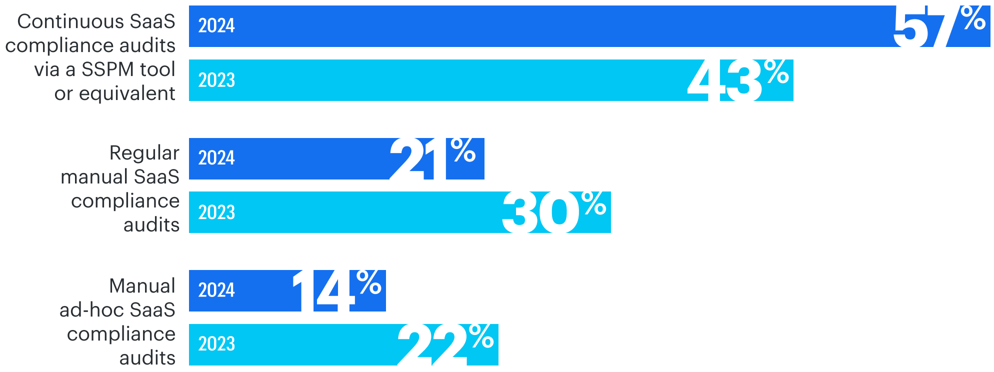
A smaller fraction of respondents **(18%) lean on their managed service providers**, and fewer still choose to engage in independent cybersecurity audits.

According to the survey, one in five respondents find it challenging to evaluate cybersecurity risks associated with adopting a new SaaS app—even with dedicated security teams. These teams could include specialists in endpoint security, network security, data security, audit and legal support, and more.

This struggle can be attributed to an overreliance on manual, periodic audits. Case in point: when introducing new SaaS applications or services, 87% of respondents perform audits, with the majority conducting them in-house.

Most audits are internally-led using proprietary risk assessment tools, independent industry frameworks (e.g. NIST, CIS Critical Controls, or ISO 27000 or similar), or are conducted by Managed Service Providers.

Tools in Place to Ensure SaaS Cybersecurity Compliance, 2024



Leaders understand the importance of securing their SaaS environments during the procurement phase, but survey data reveals that this diligence often diminishes post-install, and maintaining continuous SaaS security is not consistently prioritized.

Some organizations (8%) place too much emphasis on a vendor's initial credibility, declaring that they do not conduct audits because they rely on trusted SaaS companies. Over-reliance on one-time security processes is also a concern for compliance.

One-third of respondents indicated that their organizations relied on manual audits to ensure adherence to a myriad of regulations—from GDPR, HIPAA, to CCPA. While this number is lower than in 2023—one in two of respondents indicated that they used manual audits for compliance last year—it still represents a significant risk of noncompliance.

Key Takeaways

A shift from manual, one-time checks to proactive and automated processes is essential for early detection of SaaS threats and timely corrective actions. Why?

1. **SaaS applications are highly configurable.**
Imagine them as Lego blocks, giving businesses the flexibility to construct, adjust, and grow their software solutions to meet specific requirements, one piece at a time. However, similar to working with Legos, adding more pieces increases the risk of errors or instability unless managed carefully.

2. **Keeping up with the sheer volume of changes in settings can be overwhelming**
for even the most experienced security teams. It also makes it nearly impossible for security teams to be experts in every application.

3. **Technical knowledge is required to configure and secure an app and its resident data**
because critical security configurations are dependent upon how the app is used. Once a SaaS app is customized to deliver the most value and the desired custom functionality for the team using it, default settings don't provide optimal security and may conflict with compliance requirements.

4. **SaaS warrants regular audits and reviews of customizations to address any weaknesses**
and thwart potential data leaks. Audits can be a time sink and, if done manually or ad hoc, can leave organizations non-compliant.

Key Findings

#6

UNCERTAINTY OVER THE OPTIMAL SOLUTION

SSPM is gaining recognition but lacks a unified definition, leading enterprises to use multiple solutions simultaneously to secure their SaaS applications.

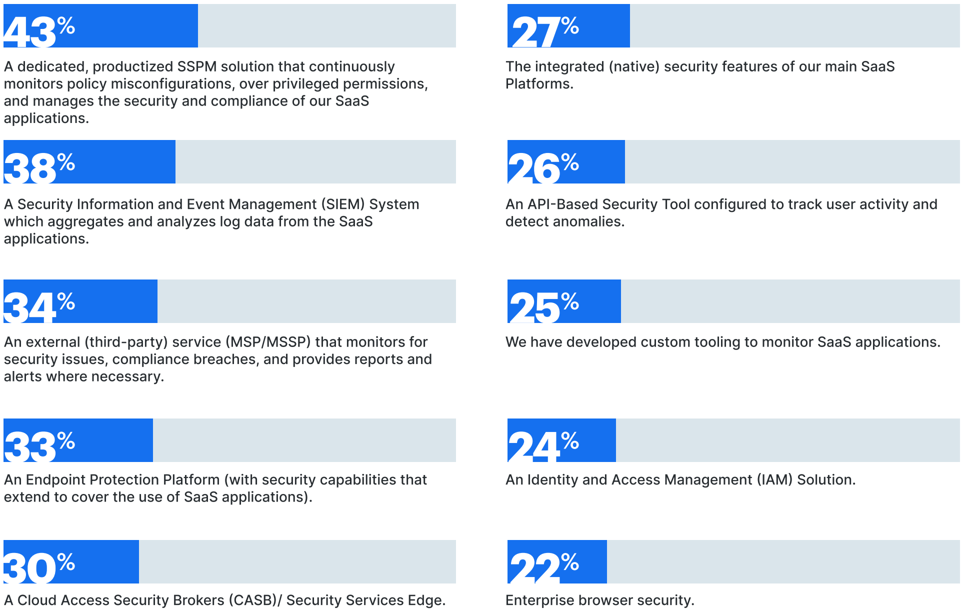
The SaaS security market has yet to agree upon a standardized list of capabilities that encapsulates SaaS security posture management. The resulting confusion over definitions means that some organizations are not getting the breadth or depth of SaaS security functionality they need to secure their data or workloads.

It's not always clear which solution is needed to ensure SaaS security. When asked how they detect and monitor third-party apps that connect to their corporate SaaS environments, the wide range of answers given indicates that there is still confusion over what types of solutions provide robust and comprehensive protection over SaaS applications.

This year we dug deeper to better understand what type of tools or processes companies have in place. Although 43% state that they have a dedicated SSPM solution in place, organizations continue to rely on a variety of security tools including SIEM (38%), Endpoint Protection Platform (38%), CASB/SSE (28%), and API-based security tools (26%).

Others even declared having developed custom tooling to monitor SaaS usage and, again, rely on an external Managed Service Provider to monitor for security issues, compliance breaches, and provide reports and alerts where necessary.

Types of Solutions Organizations Have in Place, 2024



Definitions:

SSPM manages and secures SaaS app configurations and connections to maintain regulatory compliance and reduce risk. It enables continuous monitoring of audit logs for policy misconfigurations and over-privileged permissions.

CASBs protect access from on-prem (or managed network) users/devices to cloud environments but lack visibility and security of SaaS apps, and usually don't monitor SaaS-to-SaaS connections or third-party integrations.

CSPM is another tool that secures data stored and used exclusively in cloud architectures, but doesn't address the security posture of SaaS apps or the sensitive data stored in those apps.

Key Takeaways

Enterprises are deploying a diverse set of tools and checklists to secure SaaS estates. CASBs, SASE, SWGs, CSPM shaped initial network-based SaaS access security or IaaS cloud security strategies. But they are limited in their ability to secure against modern SaaS security challenges. CASBs, for example, primarily inspect network traffic but cannot offer deep visibility or control over user activity—such as fine-grained access controls or real-time activity monitoring.

The lack of a standard definition for SSPM means that these tools can vary dramatically in capability, leaving companies to navigate a complex landscape of features and, eventually, inadequate protection of SaaS. A complete and robust SSPM solution will include the following capabilities:

1 Configuration and Drift Management

Review and update the settings necessary to maintain policy baselines, security, and access controls.
Question to ask: Does my solution provide a snapshot of my enterprise's ideal state?

2 Data Access Exposure

Identify vulnerabilities that can compromise sensitive data.
Question to ask: Does the solution flag the most common misconfigurations that lead to data exposure?

3 Threat Detection

Identify and analyze anomalies and potential threats from human and machine identities and SaaS events.
Question to ask: Does the solution integrate with SIEM, SOC tools, and security data lakes?

4 SaaS-to-SaaS Security

Get visibility into third-party connections to SaaS apps and protect the attack surface.
Question to ask: Can I identify if a specific app or user has create, read, update, and delete (CRUD) privileges?

5 Compliance

Streamline compliance and reporting with on-demand compliance assessments.
Question to ask: Can I monitor my SaaS apps by a specific compliance framework?

Key Findings
#7

COMPETING PRIORITIES AND BURDEN OF PROOF FOR ROI

Cybersecurity teams will need to invest wisely and demonstrate ROI through measurable risk reduction.

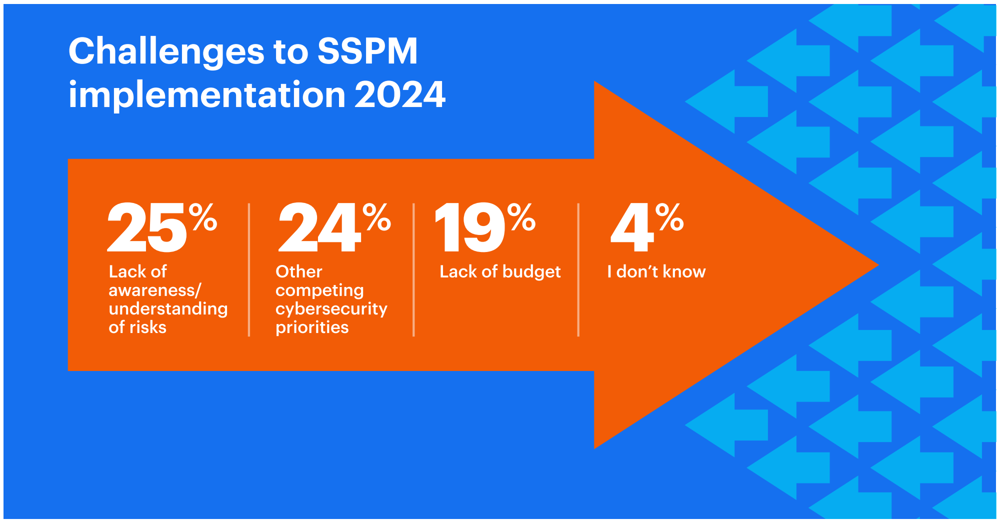
Survey data shows that 69% of respondents anticipate increased cybersecurity spending in the next 12 months, but they are unclear beyond that timeframe.

19% of respondents cited budget pressures as the main challenge in implementing SaaS Security Posture Management (SSPM) solutions.

Also a combined 49% reported that competing cybersecurity or business priorities hinder SSPM adoption. Many organizations that have implemented SSPM are unsure if they can maintain these solutions next year or afford the full range of necessary SaaS security functionalities.

38%

expressed concerns about **data risks and IP protection related to GenAI**. Meanwhile, nearly 40% believe that leveraging AI to enhance cybersecurity will be a key topic of discussion in the coming months.



Challenges to SSPM implementation 2024

25% Lack of awareness/ understanding of risks

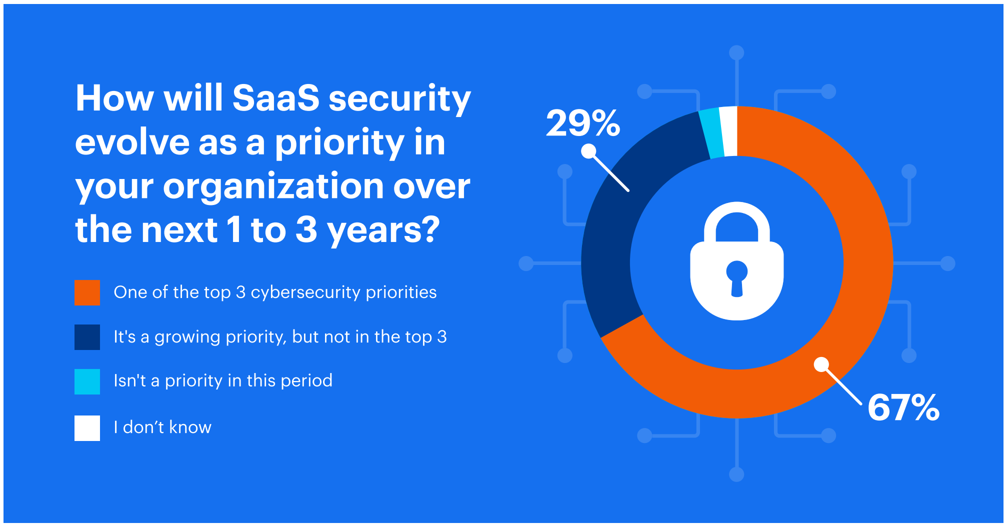
24% Other competing cybersecurity priorities

19% Lack of budget

4% I don't know

Cybersecurity teams face pressure to prove ROI on their spending. Our interviews reveal that CISOs and their teams are preparing for growing cybersecurity needs without proportional budget increases. As the digital infrastructure becomes more complex and SaaS sprawl continues to swell, the attack surface expands but budgets may not keep pace, especially next year.

Teams must "spend smarter, not harder," focusing on cost efficiency in their security programs. Already, 29% of survey respondents see this trend, expecting ROI on cybersecurity investments—measured by quantifiable risk reduction—to become a key discussion point in the next 12 months. Such risk reduction levers could include number of data exposures discovered, effort (hours) for compliance and audit, or mean time to issue resolution.



How will SaaS security evolve as a priority in your organization over the next 1 to 3 years?

Key Takeaways

Competing business and budget priorities may be hindering SSPM implementation, but the challenge of securing SaaS applications is now clearer and better understood. Today, more CISOs/CSOs are paying attention to high-profile data breaches such as Snowflake, GitHub, or MOVEit Cloud. They are also expressing eagerness to establish a SaaS security program that identifies, assesses, and prioritizes potential threats based on the likelihood and impact of their occurrence.

To address scale and resource concerns while building out their SaaS security program, organizations should follow a multi-phased, risk-based approach. This involves starting a program rollout by first identifying where sensitive data is stored in the organization's SaaS apps, determining which of those apps are business-critical, and evaluating the potential impact on business operations if a breach involving those apps occurred. This process enables organizations to allocate time and budget towards the apps with the highest criticality and potential business impact, thereby allocating time and budget as effectively as possible.

Here are five key questions to consider for each SaaS app as you move towards a risk-based SaaS security strategy:

1. **Asset identification**
   What is the functional role of the asset to the organization?

2. **Criticality**
   What is the value of the information or data that is processed or stored by the asset?

3. **Impact**
   What is the likely impact of a breach and the impact of the asset and its data being compromised? This is also referred to as blast radius and business impact.

4. **Resource allocation**
   How can you allocate security resources based on the prioritization of assets and ensure that the cost of protection is proportional to each asset's value?

5. **Prioritization**
   How can you prioritize security based on results of the risk assessment, with a focus on protecting the most critical assets first? Assets deemed of high value should be given a higher level of prioritization and protection.

With a SaaS security program and comprehensive security tooling in place, security teams are enabled to conduct continuous risk assessments, identify over-provisioned users, monitor configuration drift, comply with legal, regulatory and security standards, and establish a Zero Trust architecture.

Bold Moves for 2025 and Beyond

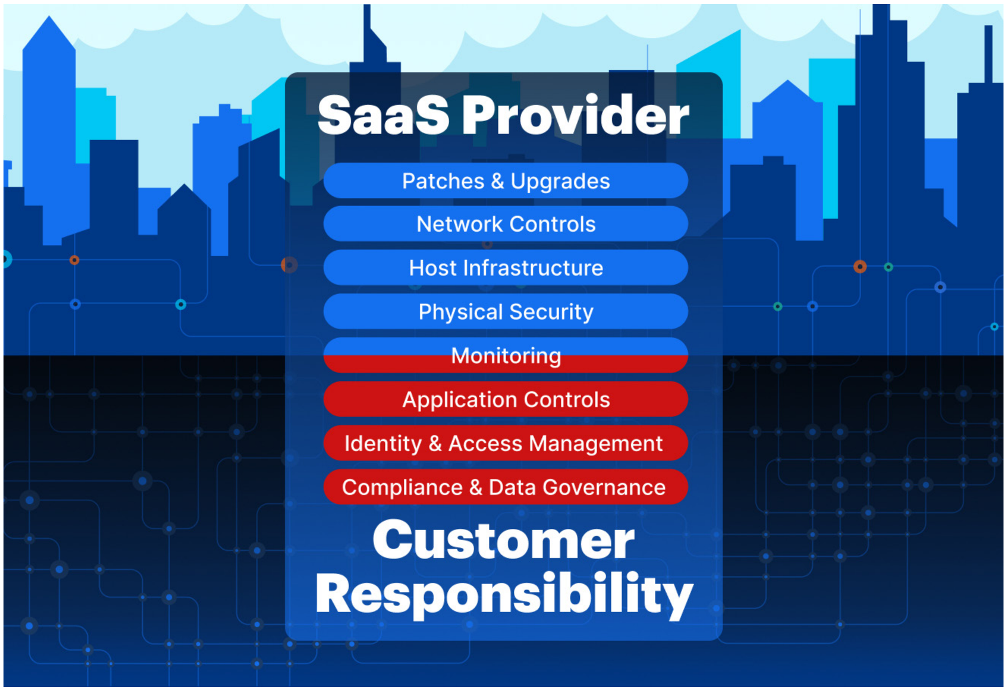
As SaaS app adoption grows, SaaS security becomes increasingly decentralized and therefore more challenging to enforce. To manage these risks, organizations must first prioritize resource allocation and security of their crown jewels (and those that will have the largest blast radius or the most business impact). Then leverage the right technology to gain visibility on who has access to what, app permissions, and proper configurations. Lastly is to ensure that security principles, such as Zero Trust, are not only applied to app access, but are also intricately woven within the applications themselves.

But these changes cannot be successfully adopted without a culture of SaaS security awareness among all employees in the organization. One of the best ways to cultivate this culture is through continuous end-user cybersecurity education, in which employees learn about the importance of identity verification and cybersecurity best practices. With this knowledge, employees can feel empowered to apply and adhere to their internal policies and avoid unintentionally becoming a SaaS attack vector.

The shared responsibility model for SaaS security is still widely misunderstood.

The shared responsibility model is meant to delineate the division of security responsibilities among cloud service providers, SaaS platforms, and customers, ensuring all parties understand their roles in data protection and risk management. While collaboration is essential for this model to work, this year's survey shows it remains widely misunderstood regarding SaaS security.

Shared Responsibility Model



But what is out of sight is frequently out of mind.
Or in the case of SaaS, thought to be covered by the SaaS Provider.

Additionally, the CISO, cybersecurity or IT team, and SaaS app business owners also have their own set of duties and responsibilities within the organization.

From the surface, it seems that SaaS platforms have compliance, identity and access management, and app controls fully covered. But in reality:

- **Compliance**
  While the provider ensures the infrastructure meets certain standards, the customer must ensure their use of the SaaS application is compliant with industry and regulatory requirements.
- **Identity & access management**
  Customers must enforce multi-factor authentication (MFA), integrate single sign-on (SSO), create, manage, or delete user accounts, and proactively monitor user access logs and audit trails to detect and respond to any unauthorized or suspicious activity.
- **Application controls**
  Customers are responsible for configuring default security settings, but also for defining and enforcing access control policies (granularly determining who has access to what).

A comprehensive SaaS security program must include continuous monitoring, scalable processes, and widespread support.

SaaS security is not a one-and-done process. Instead, it requires a risk-based approach that continuously monitors and prioritizes the most critical security issues in business-critical SaaS apps.

To build a SaaS security program, organizations should follow the steps below:

1 Identify your SaaS attack surface.

Not all SaaS apps pose an immediate security risk. Prioritize the apps that store and process your business-critical information. Audit your SaaS estate to understand the overall data criticality in SaaS and who has access to what.

2 Work with business owners.

Establish the RACI (Responsible, Accountable, Consulted, Informed) between the security team and business owners and standard operating procedures for SaaS security in your organization from onboarding new apps, setting policy baselines, to adding and offboarding users.

3 Establish a virtuous cycle with robust posture and accurate threat detection.

SaaS security posture and threat detection should work side by side. Often entire classes of threats can be prevented with the right posture and permissions, preventing noisy alerts (from threat detection) to busy SOC analysts. And threats identified should lend themselves to systemic fixes.

4 Address the long tail of SaaS apps and OAuth connected apps.

Plan to address the posture needs of SaaS apps beyond your core apps. Use the open source SaaS Event Maturity Matrix to review supported events for your preferred apps to know detections and policies to consider. Proactively set approval policies for connected apps and monitor all OAuth connections to managed apps.

5 Formulate an incident response strategy that prioritizes responding to SaaS risks and incidents.

Make SaaS a standard part of your overall incident response plan whether it is insiders or external actors. From scoping and investigating to securing and reporting, a clear SaaS incident response plan will help you save significant time and money.

Organizations that cultivate a SaaS-security aware culture and implement technology such as SSPM are well positioned to improve their overall security posture, reduce the risk of data breaches, and ensure compliance, all while streamlining the management of their SaaS environments.