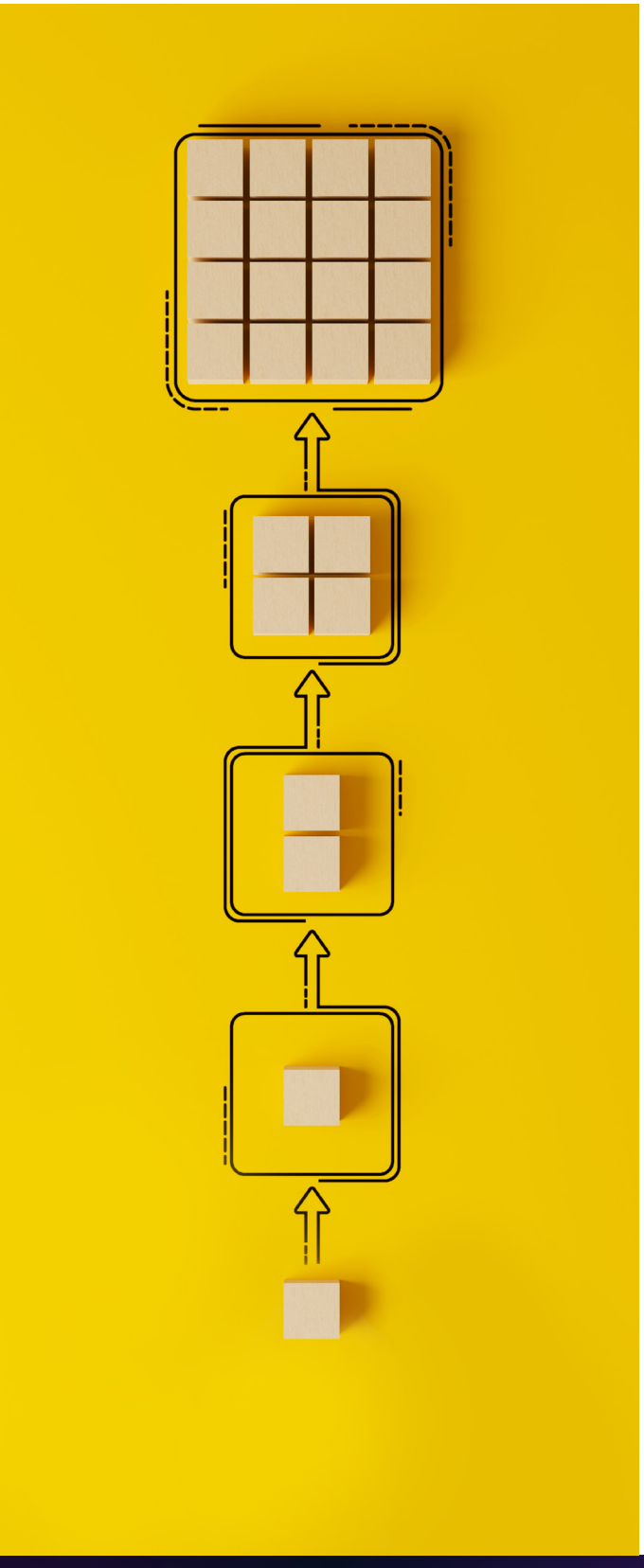
The AppOmni SaaS Security Posture Management Report 2023

An Analysis of the Top Mis-identified SaaS Security Gaps

AppOmni

Contents

Introduction



The only thing certain about cybersecurity is that it is constantly undergoing change.

When we find a new way to protect ourselves from recognized threats, new threats emerge. Nowhere is this truer than in SaaS cybersecurity. Navigating this landscape poses a challenge, as the target is constantly moving due to vendor and customer-side configuration changes. Adding to the complexity is the rapid expansion of the landscape itself, with new SaaS apps being introduced and new SaaS App admins and end-users entering the scene.

In the Summer of 2023, we surveyed over 600 security practitioners around the world to gain an understanding of their SaaS cybersecurity requirements. Our objective was to identify perception vs. reality in terms of SaaS cybersecurity gaps and to build an understanding of the general state of the SaaS cybersecurity market.

The findings of this survey are encouraging in that they suggest a high prioritization for SaaS cybersecurity initiatives, with 70% of respondents viewing it as a top 3 initiative. However, we can also gauge a degree of overconfidence and optimism in the degree that organizations feel they have adequately secured their SaaS applications. This optimism contrasts with our findings from real world deployments, identifying significant data leakage, critical security misconfigurations, elevated access privileges, SaaS-to-SaaS connections and threat detection gaps.

There are signs that recognition of the numerous cyber risks tied to large-scale SaaS app usage are still emerging, yet organizations remain unaware of the actual SaaS cybersecurity risk mitigation measures required to secure these applications. The results of our survey provide insights on potential gaps in understanding these security risks and how to raise awareness of key security practices that can be converted into useful practice.

Addressing SaaS cybersecurity risk is at the core of what we do at AppOmni. With our founders having previously worked as SaaS cybersecurity practitioners for decades, we are acutely aware that addressing SaaS cybersecurity risk cannot be done effectively manually or in a piecemeal fashion. Only through security automation via a purpose-built SaaS Security Posture Management (SSPM) solution like AppOmni, can organizations address SaaS cybersecurity effectively and at scale. Our mission is to create a safer SaaS world and it is why AppOmni is the top choice for Fortune 500 clients.

Key Takeaways

Awareness of SaaS cyber risk is growing, with 70% of organizations seeing SaaS cybersecurity as a top three security initiative within the next 1 to 3 years.

The volume of SaaS apps in use in the enterprise are also increasing, 68% of companies represented in the survey have 50+ sanctioned SaaS apps in use, and 40% have 100+. Larger enterprises have more SaaS apps deployed, with one in two having in excess of 100 apps deployed.

71% of organizations rated their SaaS cybersecurity maturity as mid to high, yet 79% suffered a SaaS cybersecurity incident in the past 12 months, with data exposure the leading incident, followed by over-permissioned end-users and app security misconfigurations.

Only 13% of organizations stated that it is impossible to use unsanctioned SaaS in their organizations. SaaS vendors may provide reassurance, but SaaS end-users may overlook certain cybersecurity responsibilities for securing their SaaS apps and the associated data. The Shared Responsibility model provides a guiding light.

52% of organizations still rely on manual SaaS cybersecurity audits and 60% have limited to no ability to monitor SaaS-to-SaaS connections. The only feasible way for companies to ensure a proactive and resilient SaaS cybersecurity posture is to implement a SaaS Security Posture Management (SSPM) solution with cybersecurity automation and continuous monitoring capabilities at the core. This entails proactively detecting and alerting on data exposure and misconfiguration risks as they arise.

SaaS Cybersecurity Misconceptions: Perceptions, Overconfidence, and Reality

85% of respondents don't think there is a SaaS security problem. Are they secure or just unaware?

The following survey data, while optimistic, represents the still "hidden" nature of SaaS cybersecurity and why it remains a critical problem for the bulk of organizations to solve today. Below, we present survey responses that suggest that by all measures, SaaS environments remain secure, and yet, our analysis from real world SaaS assessments paint a picture that is quite the opposite.

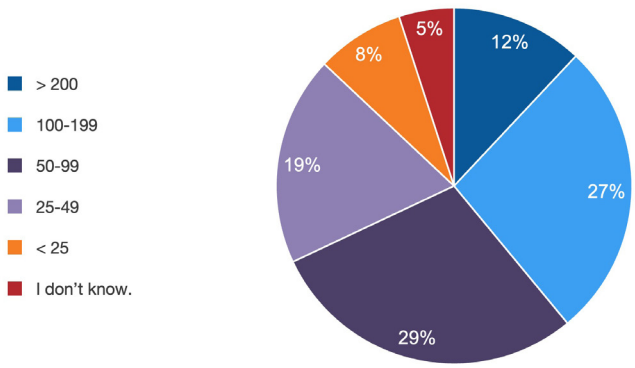
The very characteristics that make SaaS applications attractive to organizations, such as their flexibility and ease of deployment, also make them difficult to secure on an ongoing basis and at scale. At AppOmni, we identified three main problem areas that are commonly misunderstood, leading to avoidable cyber risks:

1. SaaS data security misconceptions
2. Overconfidence in the extent of SaaS cyber risk visibility
3. Misunderstanding the SaaS cyber threat model

As companies' daily operations are becoming increasingly dependent on cloud infrastructure, the need for solid SaaS application security is set to increase. The flexibility and customizability of SaaS, coupled with economies of scale, transform productivity. 68% of companies represented in the survey have 50+ sanctioned SaaS apps in use, and 40% have 100+. Larger companies (2500+ employees) tend to use more sanctioned SaaS apps, with almost one in two using 100+ apps.

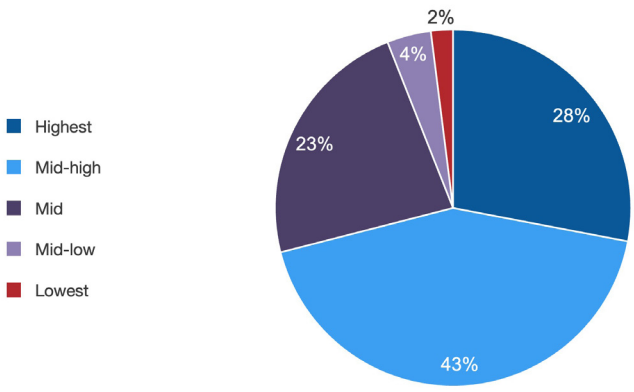
45% of organizations in North America using in excess of 100 SaaS apps, compared to Europe at 42% and APAC at 32%.

Number of Sanctioned SaaS Applications in Use



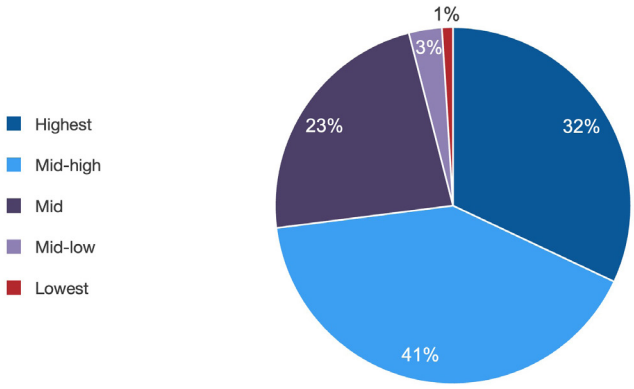
Respondents are generally optimistic about SaaS cybersecurity, and when rating the SaaS cybersecurity maturity level of their organizations, 43% of respondents report that their organization's SaaS cybersecurity is at a "mid-high" level, with 28% claiming to be at the "highest maturity" level.

SaaS Cybersecurity Perceived Maturity



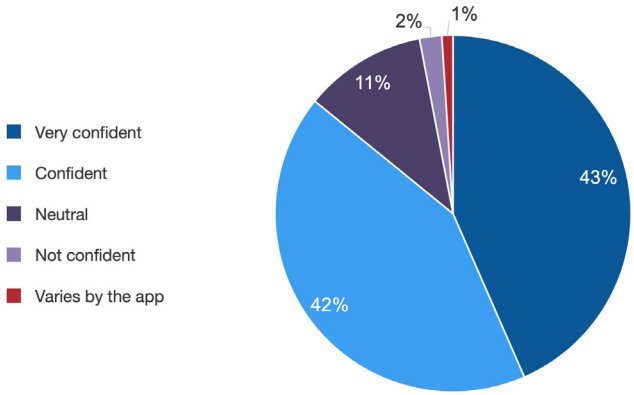
When questioned about the security levels of the authorized SaaS applications in their organization, 73% of respondents rated the application security as "mid-high" (for 41%) to "highest" (for 32%).

Perceived Levels of Security of Sanctioned SaaS Applications



A significant 85% of respondents indicated that they are confident that their company and customer data is secure in their organizations' SaaS applications.

SaaS Application Data Security Confidence



SaaS Data Security Misconceptions

Although the reported high levels of confidence in SaaS cybersecurity may initially seem reassuring, these results must be understood in the context of how companies currently approach SaaS cybersecurity vs. how many understand the actual cybersecurity risks and have consequently operationalized a SaaS security program.

For example, 85% of respondents were confident or very confident that their data is secure in SaaS compared to our real world assessments that have identified over 300 million exposed data records out of SaaS environments. In fact, in over 55% of our assessments, AppOmni has detected data leakage of customer data, PII and other data.

AppOmni has identified over 300 million exposed data records in real world assessments. Over 55% of SaaS risk assessments find data leakage of customer data, PII and other data.

In the case of one of the largest SaaS vendors globally, our analysis has shown that over 70% of internet facing instances are leaking data.

These scenarios have been further validated with documented data breaches such as these:

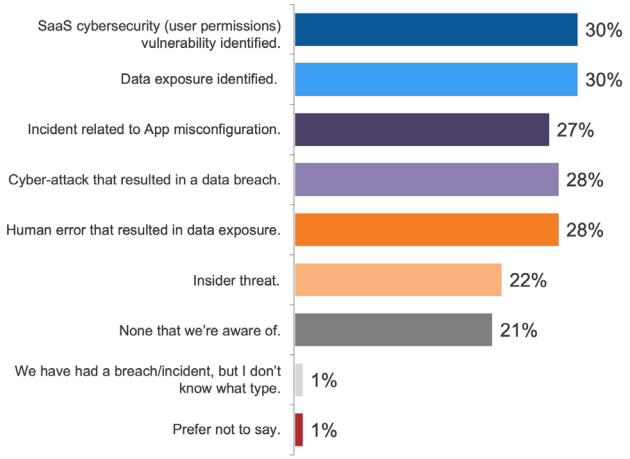
GitHub Microsoft 365 okta HubSpot

More recently, in the spring of 2023 we highlighted some targeted attacks that exposed data of of SaaS. Yet still, these SaaS-related breaches remain largely unknown to most organizations. The fact that the general public remains unaware is a core part of the disconnect between the 85% perception rate, compared to real world observations in SaaS security. The problem with awareness is that the industry and SaaS vendors consistently label these breaches as via a “third party.”

This definition, or lack thereof, of a “third party” is disturbing in that it hides the actual source and method of the breach. In fact, some of the largest data breaches in history can be traced to a SaaS application with critical misconfigurations, over-permissioning, and exposed data the leading threat vectors. The notion that the vast majority of organizations feel their SaaS data is secure directly contrasts with our own real world assessments and analysis.

Furthermore, 79% of respondents surveyed disclosed that their organization had identified SaaS cybersecurity incidents over the past 12 months. Of these incidents, approximately 30% of respondents confirmed that they had incidents related to data exposure, end-user permission vulnerabilities, and misconfigurations.

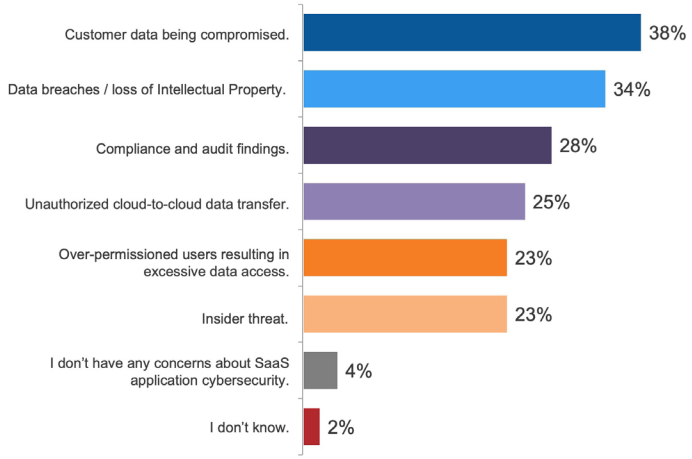
SaaS Cybersecurity Incidents in the Last 12 Months



This confirms that SaaS security incidents have been actively occurring, but may not be broadly publicized and provides further evidence that perception of SaaS cybersecurity posture is misaligned with real world observations and incidents.

In the same vein, the main concerns voiced by respondents about SaaS cybersecurity are focused on the potential compromise or loss of customer and company data, along with IP (for 38% and 34% respectively). Compliance and audit findings ranked third, at 28%.

Top SaaS Cybersecurity Concerns



When we consider that a large portion of respondents are concerned about SaaS data security, have confirmed data exposure or breach incidents, combined with our real world data identifying hundreds of millions of exposed data records, the notion that 85% of respondents are confident in their SaaS cybersecurity seems overly optimistic at best.

The reality is that SaaS monitoring and attack surface risk mitigation remains a blind spot for many organizations. They often focus only on initial risk assessments and "outside-in" audits, as opposed to looking at how SaaS applications are actually implemented and operationalized at scale across the organization.

As mentioned earlier, it is crucial to remember that cybersecurity teams may easily become overwhelmed with the challenging task of securing a diverse SaaS environment. The depth of expertise required for each application makes it difficult for them to ascertain if and when their SaaS environment has been compromised, and if it has, how it happened. The only way to maximize the probability that any abnormal or malicious activity such as suspicious logins, brute-force attempts, and data access or deletion are discovered, is through the use of a SaaS Security Posture Management (SSPM) solution.

Only by continuously monitoring each SaaS app across the SaaS estate can security and risk leaders proactively address SaaS misconfigurations or data exposure risks as they arise. Simply stated, trying to address SaaS app security on a piecemeal basis will leave organizations vulnerable to threat actors exploiting cyber risks.

Overconfidence in SaaS Cyber Risk Visibility

It is a well-known adage in risk management that it is easier to secure the known-knowns vs. the unknown-unknowns. Many companies have a procurement process for SaaS application/platform acquisition. These processes generally include extensive compliance audits and checklists established by an in-house or external cybersecurity team, such as reviewing a SOC2 audit and/or penetration test results.

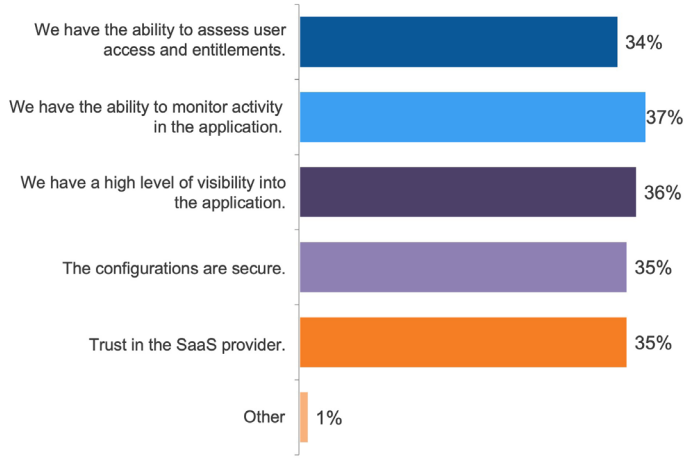
This is further evidenced by the fact that 89% of respondents state that they perform some type of audit before adopting a new SaaS application. However, this is often where security visibility into SaaS applications ends, and where the unknown-unknowns begin. Based on interviews conducted in conjunction with over 500 SaaS risk assessments, after the pre-procurement due diligence is completed, very few organizations have any continuous visibility into these applications. A smaller percentage may conduct a one-time or annual point-in-time assessment via a manual process.

Once the SaaS application is deployed, it is often left to business or application owners with limited security expertise to ensure that the SaaS applications are configured and functioning correctly. Configuring SaaS applications manually can be overwhelming, even for experienced security teams. Consequently, application owners may grant end-users excessive permissions, or misconfigure critical security settings, such as setting multi-factor authentication (MFA) to optional or leaving secrets stored insecurely.

The lack of consistency in settings across applications makes it impossible for security teams to master each application, leading to frequent and recurring misconfiguration-related vulnerabilities across the SaaS estate. The situation is further compounded by a lack of unified risk observability for SaaS app misconfigurations and data exposure across the SaaS estate.

In spite of these highly manual audit reviews and assessment processes, 50% of respondents claim they have full visibility and monitoring capability of the SaaS apps used in their organization. Here again, perception does not match reality. Industry analysts consistently measure adoption of SSPM platforms at less than five percent, and in over 150 engagements with senior security leaders, over half admitted that they had no prior knowledge that SaaS security controls monitoring capabilities exist.

Reasons for SaaS Cybersecurity Confidence?



With over one-third of respondents expressing that they "trust in the SaaS provider," this level of trust shows a lack of understanding of the Shared Responsibility Model and the role that misconfigurations can play in exposing data in SaaS environments. Leading industry analysts also project that 99% of SaaS data breaches will be caused by application misconfigurations.

Breaking apart the survey data further shows that 34% of respondents believe they have the ability to assess end-user access and entitlements. This ability is largely grounded in enterprise identity provider and governance solutions, however, these solutions do not account for any of the following scenarios:

- Super-user "break glass" accounts
- Data access modeling and mapping to SaaS objects
- API access to the underlying SaaS data schema
- Side-loaded accounts in the SaaS environment
- High-level permission scopes and permissions changes to in-application roles

In AppOmni's real world SaaS risk assessments, over 95% of evaluated companies had over-permissioned and inactive end-users.

If there are personnel changes within the organization or off-boarding employees, this also requires adjustments to end-user privileges and many organizations still fail to deprovision accounts appropriately. Managing and ensuring correct access privileges across your organization is a continuous challenge that is often not effectively addressed, especially if SaaS app configuration management and monitoring is done on a manual and piecemeal basis.

While it may be true that certain applications can be monitored and assessed individually, the ability to monitor, assess end-user access and entitlements, and ensure secure configurations on a continuous basis becomes increasingly challenging due to the complexity and volume of SaaS applications deployed within an organization. Each SaaS application comes with its own specific and unique controls and settings, adding to the complexity of the landscape.

The reality is that due to the constantly evolving and dynamic nature of SaaS, it becomes very difficult to maintain secure SaaS configuration for just one application, let alone dozens or hundreds of apps across an organization. Continuous integration and delivery processes can introduce frequent functionality and operability changes, which may affect security settings. Moreover, these DevOps changes occur on both the vendor and customer sides, further complicating the matter.

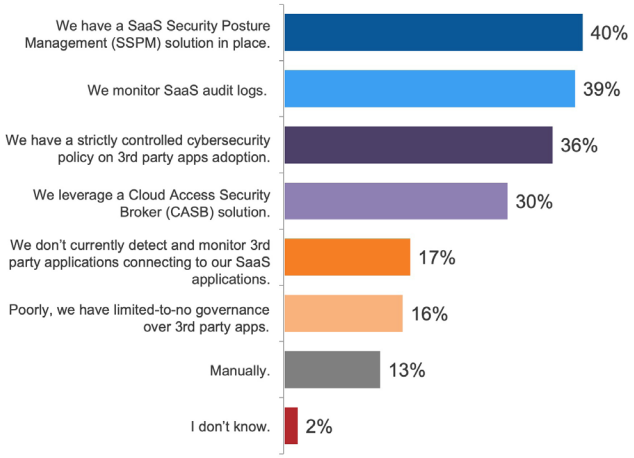
Effectively monitoring activity at the organizational level requires a comprehensive understanding of the event profiles for each SaaS app and the capacity to handle the huge volumes of data in the form of event logs. As a result, achieving full and holistic visibility across the entire SaaS estate becomes a difficult task, particularly due to the complexity of configurations and the SaaS landscape.

Misunderstanding the SaaS Threat Model

One of the critical SaaS security gaps that organizations are just beginning to understand, especially with the rising adoption of AI and large language models (LLMs), are SaaS-to-SaaS connections, or third-and fourth-party integrations. These types of integrations can enhance SaaS apps' functionalities and capabilities, making them a very attractive option to end-users. But they also increase the attack surface risk by improperly exposing insecure applications or data to threat actors.

With over 66% of respondents claiming that they detect and monitor these third-party apps via a CASB or via policy, it's evident that there is still a clear misunderstanding of the threat model and how these connections tie into SaaS. (Fig 9)

Detecting and monitoring SaaS to SaaS connections (3rd party apps)



The reason that these applications present a high risk and invisible entry point into SaaS platforms is due to the nature of the installation. First, these installations are often end-user driven. This means that the end-user accepts an End User License Agreement (EULA) with no procurement, legal or security reviews. It also means the end-user approves the permission scope for the application to connect into the SaaS platform, and the connection established is a permanent OAuth connection, often with excessive write-level permissions.

The reality is that a CASB has no visibility into this type of connection because it is made on the SaaS platform or between SaaS platforms and the policy on 3rd party apps, while a good best practice, does not prevent users from actually performing the install process on the SaaS platform itself.

AppOmni's data shows that on average, there are 256 distinct SaaS-to-SaaS applications and 3rd party plug-ins connecting into a single SaaS instance within an enterprise.

In large-scale organizations, hundreds of instances of a single SaaS application may be deployed. Half of those apps are connected directly by end-users, and not by IT or security administrators.

Multiple issues can arise with third-party apps, including uncertainty around knowing which apps are approved, what permissions an app has, and who can install an app. In April of 2022, GitHub incurred a well-publicized data breach where source code was stolen from dozens of organizations via stolen OAuth tokens and these SaaS-to-SaaS connections.

With no overarching security monitoring platform, organizations are unable to monitor this important and growing attack surface, including what data these third-party apps have access to. More concerningly, within six months over half of these SaaS-to-SaaS apps become dormant, yet still retain read and write privileges, making them highly attractive targets to threat actors seeking to access an organization's information system.

Recent **SaaS breaches**, including the MOVEit managed file transfer software compromise, reveal that without continuous monitoring capability for SaaS, organizations have no way of knowing whether any of their SaaS systems or data have been compromised in a SaaS supply chain attack.

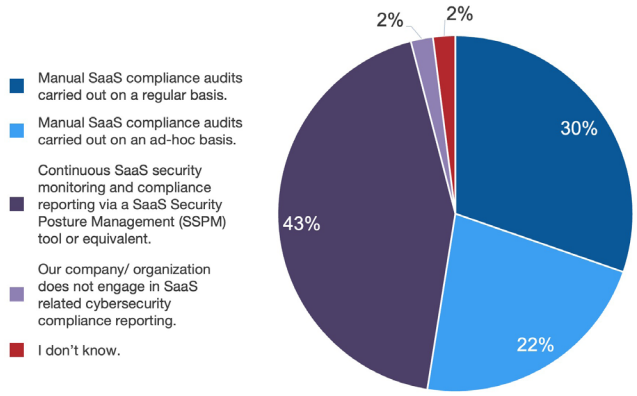
Controls, Compliance and Risk Management

So how do companies today ensure SaaS cybersecurity?

When asked what the most important SaaS cybersecurity capabilities are, threat detection and forensics topped the list (24%), followed by SaaS-to-SaaS connectivity visibility (20.3%), and user privileges and activity monitoring (18%). Governance and compliance (17.9%) and configuration and posture management (17.4%) rounded out the fourth and fifth most valued capabilities. One way of understanding the importance given to threat detection and forensics can be due to the high degree of SaaS cybersecurity incidents reported among the interviewees.

When it comes to compliance, 43% of respondents state that their organizations use some form of SaaS Security Posture Management (SSPM) tool or equivalent to ensure compliance with industry-specific or regional regulations (e.g., GDPR, HIPAA, CCPA / APPI / Privacy Act, etc.) But the most common way to ensure compliance is by performing manual performing manual SaaS compliance audits on a regular or ad-hoc basis (52%).

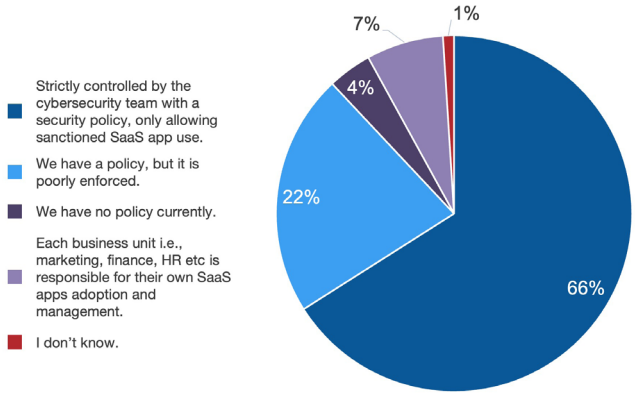
How SaaS Cybersecurity Compliance is Ensured?



In addition, there is no current universally standardized definition for SSPM. Different providers will offer varied capabilities and features under this label, but it's up to organizations to evaluate and carefully choose a solution that aligns with their specific cybersecurity requirements and the SaaS applications they use.

According to the survey, 66% of individuals report that their organizations have the necessary controls and policies in place for managing the secure adoption of SaaS applications (including SaaS-to-SaaS connections).

SaaS Cybersecurity Policies and Policy Enforcement



The main reason that certain applications may not be sanctioned for use was uncertainty over data security (31%).

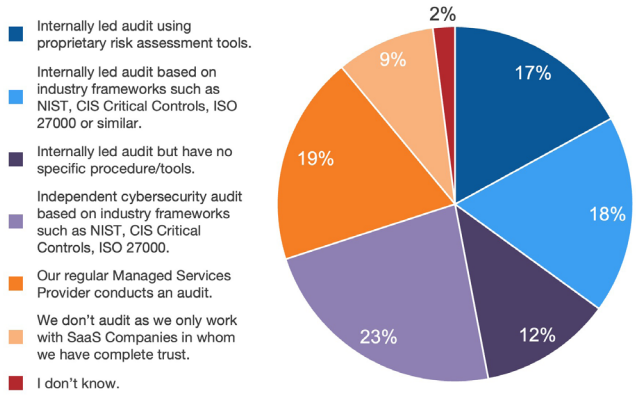
26% of respondents indicated that the decision for using unsanctioned SaaS is that it is decentralized and is not controlled by IT.

Crucially, only 13% of respondents state that it is impossible to use unsanctioned SaaS applications in their organization, reaffirming a well-known reality that unsanctioned SaaS application use is pervasive for the majority of organizations.

Effectively managing the risks of adopting a new SaaS application or outsourcing functions to a new SaaS provider is crucial. In fact, 89% of companies often conduct some form of audit as part of their overall procurement process, as mentioned earlier. The majority (47%) declare that their organization carries out internally-led audits, with 19% relying on their usual managed service provider (MSP) to do so. And while the use of independent cybersecurity audits is less frequent (23%), fewer than one in ten respondents state that their organizations don't perform audits,

rather they rely on trusting vendors to guarantee their security.

SaaS Adoption Risk Management Proceess'

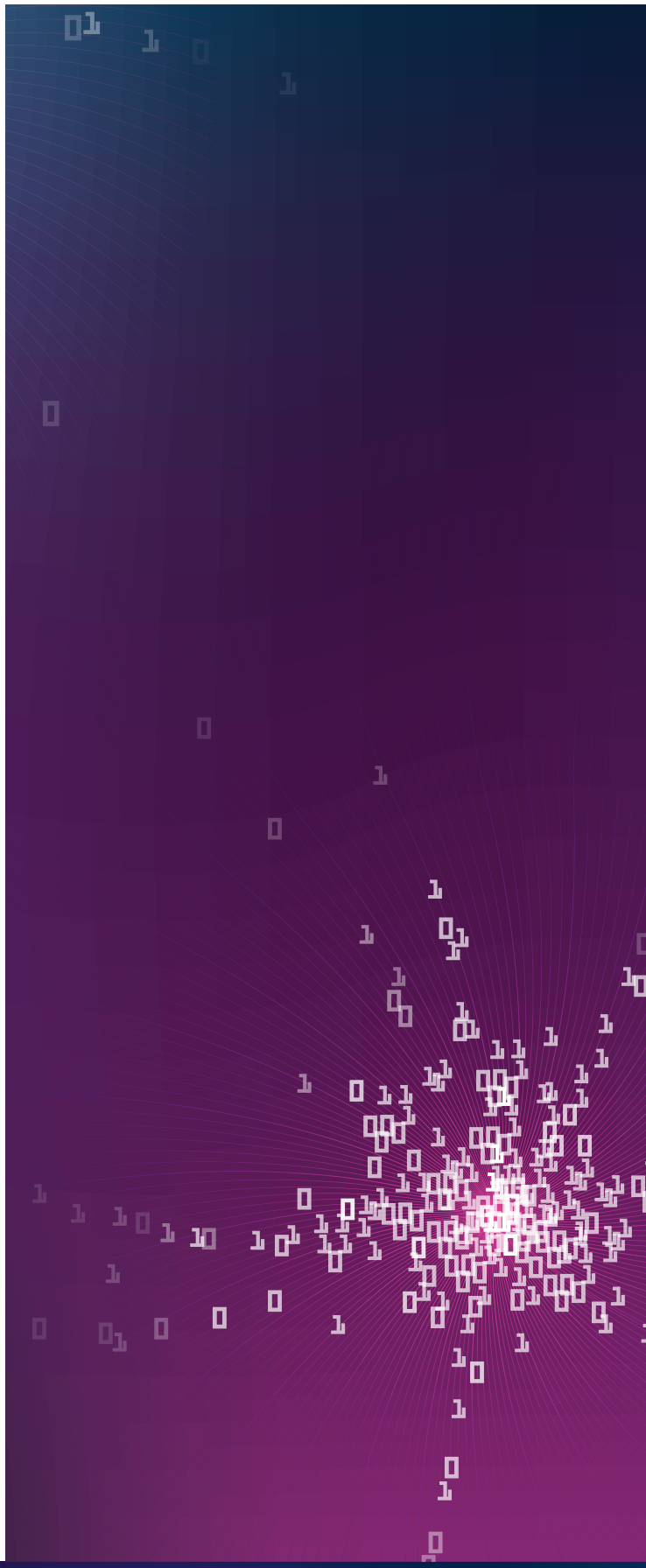


As noted earlier in the report, 60% of respondents have extremely limited or no ability to monitor and detect SaaS-to-SaaS connections via corporate SaaS applications. Instead they rely on CASBs, policies, or manual checks.

The surge in SaaS app usage may lead to an increase in the use of SaaS-to-SaaS connections, with AppOmni finding an average of 256 SaaS-to-SaaS connections in a typical enterprise SaaS instance. This presents an impossible challenge when attempting to control the cybersecurity posture for these applications with a CASB, policies or manual procedures.

Once again, we identify an emerging pattern: Although very few organizations completely ignore the cyber risks associated with the use of SaaS, many still heavily rely on incorrect tooling or various forms of manual controls and monitoring to secure their SaaS applications.

Cybersecurity compliance audits are initially conducted at the procurement stage to ensure vendor trustworthiness. However, after that, the organization may lack the necessary structures, processes, and tools for continuous monitoring and corrective action to ensure ongoing security within the corporate SaaS environment.



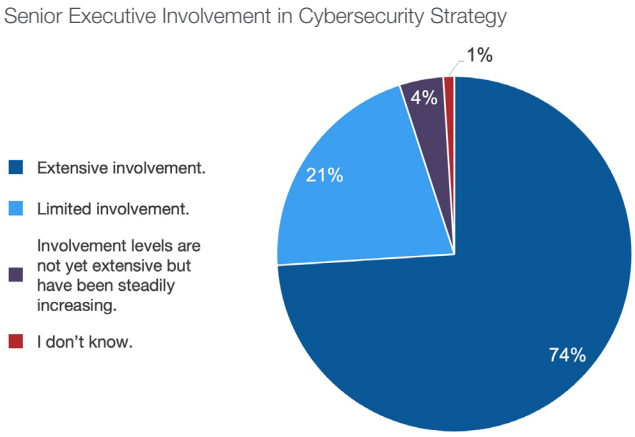
SaaS Cybersecurity Awareness Among Decision Makers

Cybersecurity awareness is increasing as threats grow in scope and sophistication.

As enterprise digitization continues to reach new heights, the threat landscape continues to grow in scope and sophistication. Enterprise cybersecurity has never been so important. Executive involvement is crucial as leaders recognize that cybersecurity is no longer solely an IT issue, but a strategic business concern.

Our survey results highlight this evolution, showing a high-level of reported involvement of senior executives and board members in shaping and overseeing cybersecurity strategy. In fact, 78% of respondents declared that in their organizations, board/executive level involvement in cybersecurity strategy is extensive or growing.

For companies with more than 2500 employees, cybersecurity strategy involvement by senior executives rises to 83%, indicating that the larger enterprises are even more aware of the increasing risks.



The survey reveals that 97% of senior executives are prioritizing SaaS cybersecurity, with 70% stating that it is likely to become a top three cybersecurity initiative within the next 1 to 3 years.

This evolution towards higher involvement and awareness is evident in the allocation of the cybersecurity budget towards SaaS cybersecurity. Notably, 80% of respondents now allocate 20% or more of their cybersecurity budget towards SaaS cybersecurity. These findings appear to validate that there definitely is a higher-level of awareness at the executive level and much more of a mandate up to the board level, in terms of the impact that cybersecurity has on the overall risk profile of a company.

Shared Responsibility in SaaS Cybersecurity

Organizations are often unaware of where the responsibility for their SaaS cybersecurity starts and ends.

In SaaS cybersecurity, the NCSC's Shared Responsibility Model emphasizes the critical role of shared responsibility in data protection and risk mitigation. As technology has evolved, the distribution of responsibilities between enterprises and vendors have also shifted.

The technology stack model has changed: from on-premises (where enterprises secured everything), to IaaS (where vendors secured the underlying infrastructure), to PaaS (where vendors secured infrastructure, runtime, and development frameworks).

As in the early days of public cloud adoption, many enterprises and SaaS users still appear to assume that the responsibility for their SaaS cloud security rests solely with the SaaS vendor.

Although it is true that in the SaaS model, the vendor is responsible for a significant portion of the cybersecurity responsibilities (including securing the infrastructure, applications, and data), it is important to understand that the enterprise still has key responsibilities of their own. Several layers of cybersecurity responsibility at an application-level fall within the enterprise's remit. For example, managing end-user identities and access, configuring security settings, and educating employees about safe usage practices are all the enterprise's duties.

The shared responsibility model emphasizes the need for collaboration and cooperation between enterprises and vendors. By recognizing and embracing this shared responsibility approach, parties can work together to strengthen cybersecurity measures and ensure a resilient and secure SaaS environment.

Conclusion

> *"It ain't so much the things that people don't know that makes trouble in this world, as it is the things that people know that ain't so."*
>
> **Mark Twain**

Without dedicated SaaS cybersecurity tooling, SaaS adoption is expected to outpace the ability of cybersecurity teams to secure their organization's critical SaaS apps and data. he confidence-related data shows that security practitioners have only a general awareness level of the key risk and cybersecurity activity areas for SaaS platforms. This general awareness may lead to potential misunderstandings in effectively securing SaaS. This is not surprising considering the general lack of attack surface visibility and the lack of disclosure of actual SaaS breaches. Similar incongruences between awareness and actual expertise have been observed throughout the evolution of other cybersecurity categories and use cases.

Organizations report that the primary challenge of implementing effective SSPM solutions and programs is a lack of awareness/understanding of risks. Yet, there appears to be a general over-optimism pertaining to managing those cyber risks. This is evidenced by 50% of respondents stating they have full visibility into SaaS-related cyber risks, while at the same time, reporting that 79% have suffered from a SaaS cybersecurity incident over the past 12 months.

There is still much to be done to ensure companies and end-users fully understand the scope and challenge of securing the continuously expanding SaaS attack surface. This will not be achieved as a one-off effort but rather through continuous education, specifically concerning the intricacies and complexities of securing SaaS proactively and at scale across the enterprise.

High levels of SaaS cybersecurity will only be achieved by thoroughly understanding the cyber risk landscape, the delineation of responsibilities between SaaS vendors and SaaS end-users, and the implementation of a truly proactive approach. And as we have seen, a few common misconceptions can lead to the key weaknesses in SaaS cybersecurity.

Ultimately, data protection is always the responsibility of the organization that owns the data. To bridge the security gap effectively, security teams should implement a SaaS Security Posture Management (SSPM) solution that brings unmatched cyber risk observability into the SaaS estate.

But, as revealed in this survey, many organizations still rely on manual and piecemeal approaches to secure their SaaS applications. Such an approach is infeasible, retroactive, immediately irrelevant once completed, and leaves organizations exposed to mounting SaaS cyber risk.

In contrast, a dedicated SSPM solution powered by security automation can discover SaaS cybersecurity threats, protect SaaS environments from unnecessary cyber risks, continuously monitor applications for drift from established security baselines, and ensure organizations adhere to compliance and regulatory standards.

An SSPM solution allows organizations to move quickly and confidently, providing security guardrails to protect sensitive and business-critical SaaS apps and data, without interrupting business.

What are you doing to secure your SaaS?

To learn more, email us at **info@appomni.com** or visit **appomni.com**.

Research Methodology

How was our research carried out?

Sample and survey details

- Sample size: 644
- 50% of the respondents from companies with 500– 2499 employees, and 50% in companies with 2500+ employees.
- Regions covered: North America (US), Europe (UK, France, Germany), and APAC (Japan, Australia).
- Method: Online from May 30th to June 8th, 2023.

Who were the respondents?

The sample consisted of 76% IT/Cybersecurity roles and 24% Leadership/Management or functional roles, all self-declaring as having decision making or decision process involvement in vendor selection for cybersecurity solutions.