cloud security alliance®

valence

Survey Report

The State of SaaS Security

Trends and Insights for 2025-2026

Acknowledgments

Lead Author

Hillary Baron

Contributors

Marina Bregkou
Josh Buker
Ryan Gifford
Alex Kaluza
John Yeoh

Graphic Design

Claire Lehnert
Stephen Lumpe

About the Sponsor

Valence finds and fixes SaaS risks. The Valence platform discovers, protects, and defends SaaS applications by monitoring shadow IT, misconfigurations, and identity activities through unparalleled SaaS discovery, SSPM, and ITDR capabilities. Recent high-profile breaches highlight how decentralized SaaS adoption creates significant security challenges. With Valence, security teams can control SaaS sprawl, protect their data, and detect suspicious activities from human and non-human identities. Valence goes beyond visibility by enabling security teams to remediate risks through one-click remediation, automated workflows, and business user collaboration. Trusted by leading organizations, Valence ensures secure SaaS adoption while mitigating today's most critical SaaS security risks.

https://www.valencesecurity.com

Table of Contents

Executive Summary

Software-as-a-Service (SaaS) applications have become foundational to business operations, and organizations are responding with greater investment and attention. Yet, the 2025 CSA SaaS Security Survey reveals that while prioritization is increasing, core challenges in visibility, identity, and governance persist—highlighting the need for a more unified, purpose-built approach to SaaS security.

Key findings from the survey include:

1. SaaS Security Is a Growing Priority

SaaS security is now a high priority for 86% of organizations, with 76% increasing budgets and 79% expressing confidence in their programs. Organizations are focusing on key areas like threat detection (50%) and posture management (47%).

2. Sensitive Data Remains at Risk

Data oversharing and poor access control continue to expose organizations to risk. 63% report external oversharing, and 56% say sensitive data is uploaded to unauthorized apps, often without sufficient visibility or enforcement.

3. Decentralized SaaS Adoption and Management Creates Security Gaps

With 55% of employees adopting SaaS without security's involvement and 57% reporting fragmented administration, many organizations struggle to maintain consistent oversight and policy enforcement across teams and tools.

4. Human Identity Management Lacks Automation and Consistency

IAM remains a challenge, with 58% struggling to enforce privileges and 54% lacking automation for lifecycle management. These gaps directly contribute to breaches and leave organizations vulnerable.

5. SaaS Integrations and Non-Human Identities Are Blind Spots

SaaS-to-SaaS integrations and GenAI tools are expanding the attack surface. Nearly half of organizations (46%) struggle to monitor non-human identities (NHIs), and 56% report concerns about over-privileged API access.

6. Current Tooling and Strategies Fall Short of Holistic Security

Despite confidence, many organizations rely on vendor-native tools (69%), general-purpose solutions like Cloud Access Security Brokers (CASBs) (43%), and even manual audits (46%). These fragmented strategies leave critical gaps across the SaaS environment.

Most current SaaS security strategies are still reactive and fragmented leaving organizations' sensitive data at risk. To truly reduce risk, organizations must align investment with integrated capabilities spanning discovery, posture management, threat detection, identity security, and remediation.

Key Findings

SaaS has become a core part of modern business operations—but securing it remains a moving target. As organizations embrace more cloud-based applications than ever, they're also facing a rising tide of security challenges, from visibility gaps and shadow IT to over-privileged access and unchecked third-party integrations. As threats evolve and SaaS environments become more interconnected, security strategies must shift from passive monitoring to proactive risk reduction. The question isn't whether SaaS security is a priority—it's whether organizations are actually keeping up.

Key Finding 1:

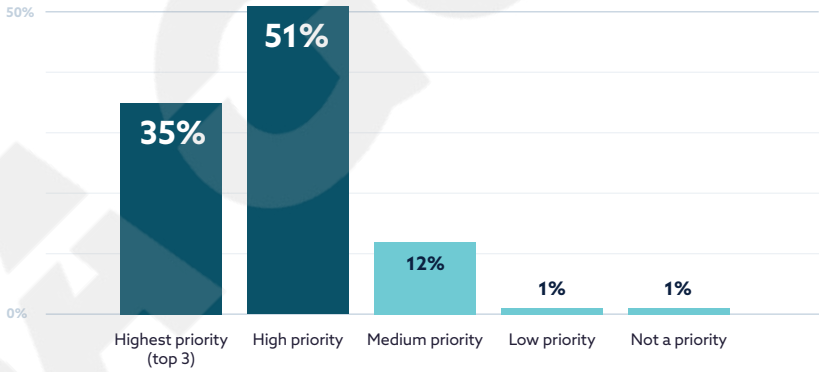
SaaS Security Is a Growing Priority as Organizations Ramp Up Investment

SaaS security is more of a priority than ever, with **86% of organizations ranking it as a high or highest priority**. This marks an increase from the 80% in CSA's 2024 survey that reported it was a moderate to high priority, reflecting growing recognition of the need for stronger protections.

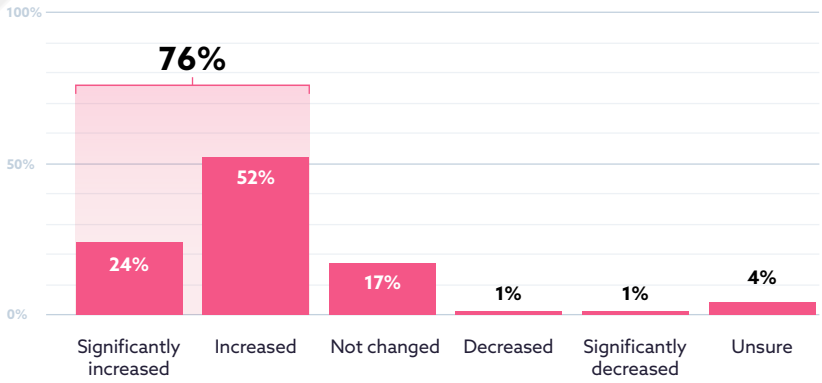
Investment has followed this prioritization, with **76% of organizations increasing their SaaS security budgets this year**, nearly doubling the 39% who reported budget increases in 2024.

As SaaS environments continue to expand, organizations are not just allocating more budget to security, but also sharpening their focus on key risk areas.

In your organization, how important is SaaS security?



How has the budget for SaaS security changed over the past 2 years?



Which aspects of SaaS security does your organization currently prioritize?

50% SaaS threat detection

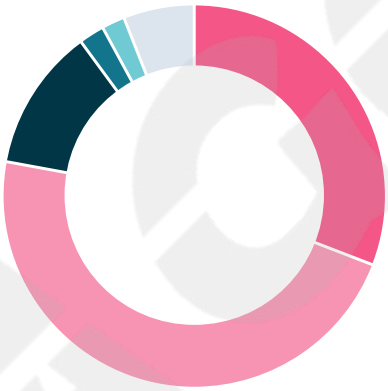
47% SaaS Security Posture Management (SSPM) solutions

31% SaaS application discovery

Half of organizations (50%) are prioritizing SaaS threat detection, another **47% are prioritizing SaaS Security Posture Management (SSPM) solutions**, and **31% are prioritizing SaaS application discovery** —suggesting that security teams are actively seeking ways to strengthen visibility and control over their SaaS applications. Discovery, posture, and threat detection and response are all core aspects of a holistic SaaS security strategy. As SaaS environments become more complex, strategies that can connect these functions will be better positioned to comprehensively manage security and risk.

At the same time, confidence in security programs remains strong, with **79% expressing confidence in their SaaS security processes**, indicating that many organizations feel they are making progress in managing SaaS-related risks. However, this confidence may not fully reflect the realities of the intended strategy and day-to-day operations. This suggests that many organizations may be overestimating their ability to effectively manage SaaS security at scale.

How confident are you in your organization's process for security SaaS



79%

31% Very confident
48% Somewhat confident
12% Somewhat unconfident
2% Very unconfident
2% Unsure
6% N/A - no process

Does your organization have specific personnel focused on SaaS security?

61% Yes **39%** No

Despite these advancements, securing SaaS remains a **complex challenge**, particularly as organizations **scale their security strategies to keep pace with SaaS adoption. Thirty-nine percent of organizations still lack dedicated SaaS security personnel**, signaling that many teams are working to manage these environments without dedicated or specialized resources. As SaaS security investment grows, organizations will need to ensure that their investing in a holistic strategy which includes both technology and expertise, reinforcing their ability to detect threats, enforce policies, and reduce risk across their SaaS ecosystem.

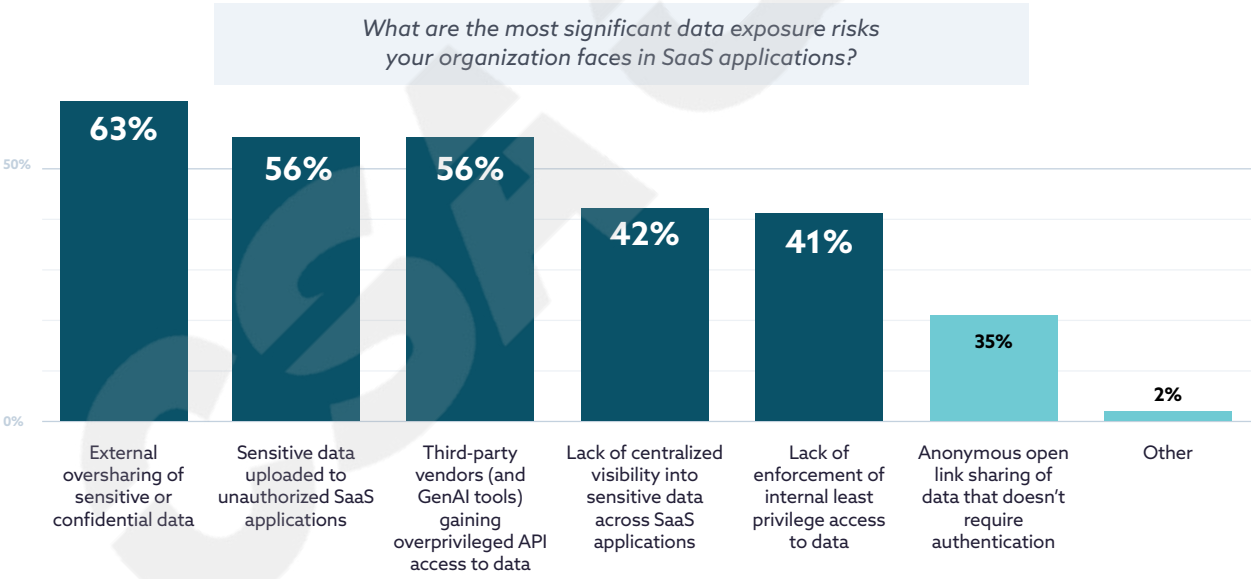
This year's findings demonstrate a clear shift toward greater SaaS security prioritization and investment, with organizations not only recognizing its importance but actively working to prioritize threat detection and security posture management. As SaaS adoption accelerates, maintaining this momentum will be critical to ensuring security strategies evolve in tandem with the increasingly complex SaaS landscape.

Key Finding 2:

Sensitive Data in SaaS Is at Risk Due to Poor Visibility and Weak Access Controls

The urgency behind these SaaS security investments becomes clear when looking at the data exposure risks organizations are facing. **Sixty-three percent of organizations cite external oversharing of sensitive or confidential data as a top risk**, while **56% report employees uploading sensitive data to unauthorized SaaS applications**. These findings suggest that while organizations are committing more resources to SaaS security, many are still struggling to establish the fundamental protections needed to secure sensitive data across their environments.

A major contributing factor to these risks is ineffective privilege and access management practices. **Forty-one percent of organizations report that least privilege access policies are not effectively enforced**, meaning users and systems often retain excessive permissions, increasing the risk of data leaks, privilege abuse, and insider threats. This challenge is not limited to human identities. Generative Artificial Intelligence (GenAI) integrations are introducing new layers of complexity, often requiring broad access to sensitive data across multiple applications to perform their tasks. **Fifty-six percent of organizations are concerned about third-party vendors and AI-powered SaaS tools gaining overprivileged API access to data**.



Unlike traditional tools, GenAI and third-party integrations frequently operate autonomously, often moving and analyzing data, connecting across applications, and generating output at scale. These functions can significantly expand the blast radius of misconfigured permissions or overlooked integrations. Without proper oversight, these tools can put data at risk. As AI tools and systems become more embedded in SaaS workflows, they introduce not just new types of users, but entirely new patterns of behavior that security teams must understand and manage. Yet the same oversight and lifecycle controls are not applied, even as the potential attack surface grows.

The emergence of open-source GenAI tools like DeepSeek further amplifies these concerns. While these tools offer powerful capabilities, they are often adopted without IT or security oversight and lack adequate privacy and security controls. DeepSeek, in particular, has raised alarms due to minimal investment in safeguards and the legal requirement for Chinese companies to share information with government authorities. Despite these risks, tools like DeepSeek are freely accessible through any browser, enabling unsanctioned use by employees. This increases the likelihood of sensitive data being exposed without proper monitoring or enforcement, making it even harder for organizations to maintain control over their SaaS environment.

A lack of centralized visibility into SaaS data flows and unmonitored SaaS-to-SaaS integrations compounds these issues, with **42% of organizations struggling to track and monitor sensitive data across their SaaS applications**. Without clear oversight, security teams face challenges in enforcing compliance policies, detecting unauthorized data movement, and responding to risks in real time. These visibility gaps—combined with weak access controls and the rapid expansion of third-party integrations—suggest that many organizations lack a fundamental understanding of their own SaaS landscape.

While SaaS security is a growing priority, and many organizations are increasing their budgets to strengthen their security posture, addressing these risks requires more than just additional investment—it demands a more cohesive and structured approach particularly in the age of GenAIVisibility into SaaS environments, enforcement of least privilege access, and consistent monitoring of data movement across applications are essential first steps, but security strategies remain fragmented, often applied on an application-by-application basis rather than holistically across the SaaS ecosystem. Without a strong foundation in SaaS security and a more unified strategy, organizations will continue to struggle with protecting sensitive data, managing third-party risks, and translating security investments into meaningful, lasting improvements rather than isolated fixes.

Key Finding 3:

The Rise (and Risks) of Decentralized SaaS Adoption and Management

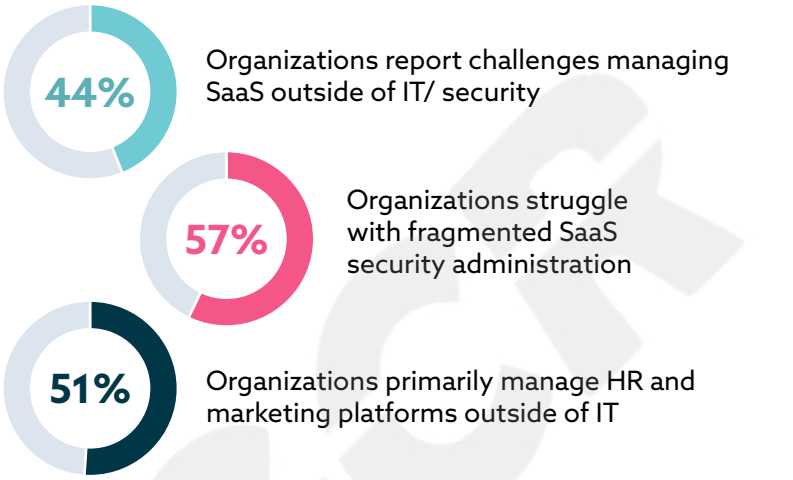
As SaaS adoption accelerates, employees are increasingly bringing in applications without security or IT involvement, making it difficult to track, secure, and govern these tools effectively. **Fifty-five percent of organizations report that employees sign up for SaaS applications without security's involvement**, introducing new risks as sensitive data flows into unmonitored environments. While this decentralized adoption provides flexibility for business teams, it also creates security blind spots, leaving organizations unaware of what applications are in use, how they are configured, and where sensitive data is stored.

Fifty-five percent of organizations report that employees sign up for SaaS applications without security's involvement

Beyond adoption, SaaS management itself is also often shifting outside of IT and security teams, leading to inconsistencies in security oversight. **Forty-four percent of organizations report challenges managing SaaS outside of IT/security**, while **57% struggle with fragmented SaaS security administration**.

This challenge is particularly concerning for **HR and marketing platforms—applications that often contain highly sensitive data—which are primarily managed outside of IT in 51% of organizations**. Without a centralized approach to governance, security policies are often applied inconsistently, increasing the risk of misconfigurations and delays in responding to security incidents.

SaaS management shifting causes inconsistencies in security oversight



Further complicating the issue, collaboration barriers between security, IT, and business teams make it even harder to address SaaS risks. **Forty-one percent of organizations cite collaboration challenges as the largest barrier to remediating SaaS risks**, and **35% report specific difficulties working with business units on SaaS security**. With responsibility for security spread across multiple teams but no clear ownership, accountability becomes diluted. This leads to gaps in policy enforcement, inconsistent security controls, and uncertainty over who is responsible for mitigating risk.

Difficulties addressing SaaS risks

Organizations need a more structured, proactive approach to SaaS security—one that emphasizes clear governance and centralized oversight. While SaaS adoption will always involve multiple teams, security responsibilities must be clearly defined from the start, ensuring that ownership extends beyond initial adoption and into ongoing management. Without a consistent and unified strategy for SaaS security, fragmented administration will continue to create visibility gaps, policy inconsistencies, and security blind spots. Just as critical is the need to foster stronger collaboration with business units and security teams. Establishing trusted partnerships with these stakeholders ensures that secure onboarding, monitoring, and access control processes are followed across the organization. Without this shift, the decentralized model will continue to introduce unmanaged risks, making SaaS security a patchwork of inconsistent policies rather than a cohesive, collaborative strategy.

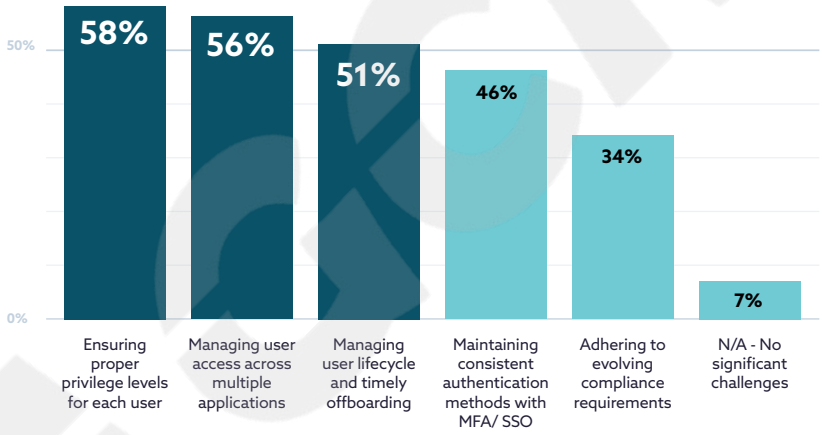
Key Finding 4:

Human Identity Management in SaaS Remains a Persistent and Expanding Security Challenge

Strong Identity and Access Management (IAM) is essential to securing SaaS environments, ensuring users have the appropriate level of access while preventing unauthorized activity. However, inconsistencies in how IAM is implemented, and a lack of automation across SaaS applications, have made it a persistent challenge.

One of the biggest contributors to this challenge is privilege management, with **58% of organizations struggling to enforce proper privilege levels across SaaS applications**. Without consistent privilege enforcement, users may retain excessive permissions beyond what they need, increasing the risk of data leaks and insider threats. Compounding this issue, **56% of organizations struggle to manage user access across multiple SaaS applications**, highlighting how difficult it is to maintain visibility and control over identities when every SaaS application has its own access model and role-based controls. These inconsistencies lead to identity sprawl, making it harder for security teams to enforce uniform policies and quickly respond to potential threats.

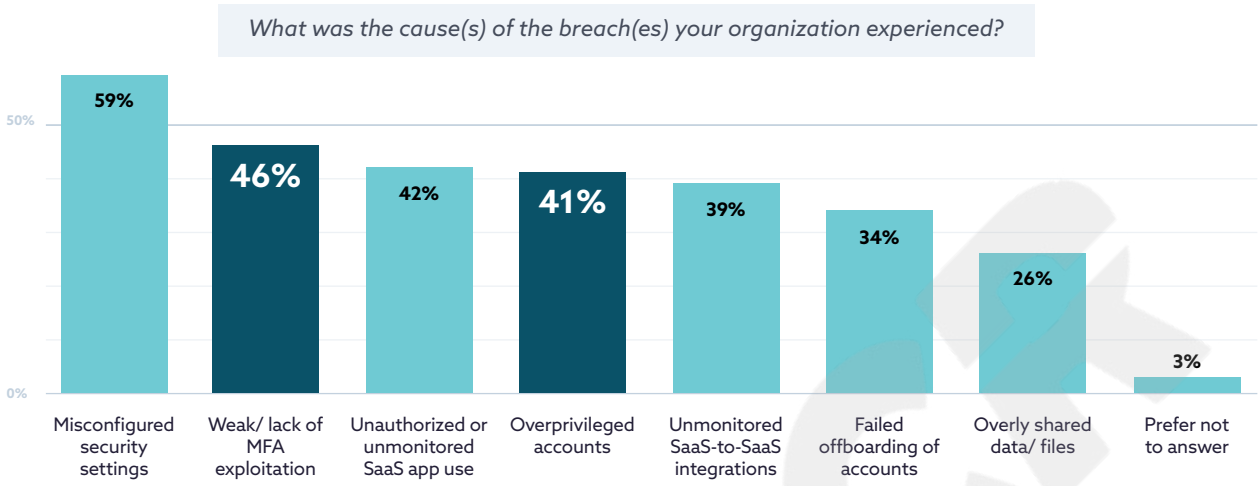
What challenges does your organization face with Identity and Access Management (IAM) for SaaS?



More than half of organizations (54%) report that they lack automation for provisioning and deprovisioning user accounts

Access management is further complicated by a lack of automation in identity lifecycle processes. **More than half of organizations (54%) report that they lack automation for provisioning and deprovisioning user accounts**, which increases the risk of orphaned accounts, privilege accumulation, and unauthorized access. This is likely a contributing factor for the **51% of organizations struggling with managing identity lifecycle processes, including timely offboarding**. Without automated lifecycle management, security teams

are forced to rely on manual processes that are inefficient, error-prone, and difficult to scale across a growing SaaS ecosystem.



These IAM failures are not just hypothetical risks. **Forty-six percent of SaaS breaches were linked to weak or exploited MFA protections**, while **41% were caused by over-privileged accounts**. When organizations struggle to enforce multifactor authentication (MFA), apply least privilege or enforce identity governance, attackers can take advantage of unsecured access, misconfigurations, excessive permissions, or unsecured accounts to move laterally across SaaS applications. This not only increases the likelihood of data breaches but also complicates incident response, as fragmented identity controls make it difficult to detect and contain unauthorized access before significant damage is done. It's important to remember that while MFA remains an important defense, it cannot address the full range of identity-related risks, especially when basic processes like access provisioning and privilege management are still inconsistent or incomplete.

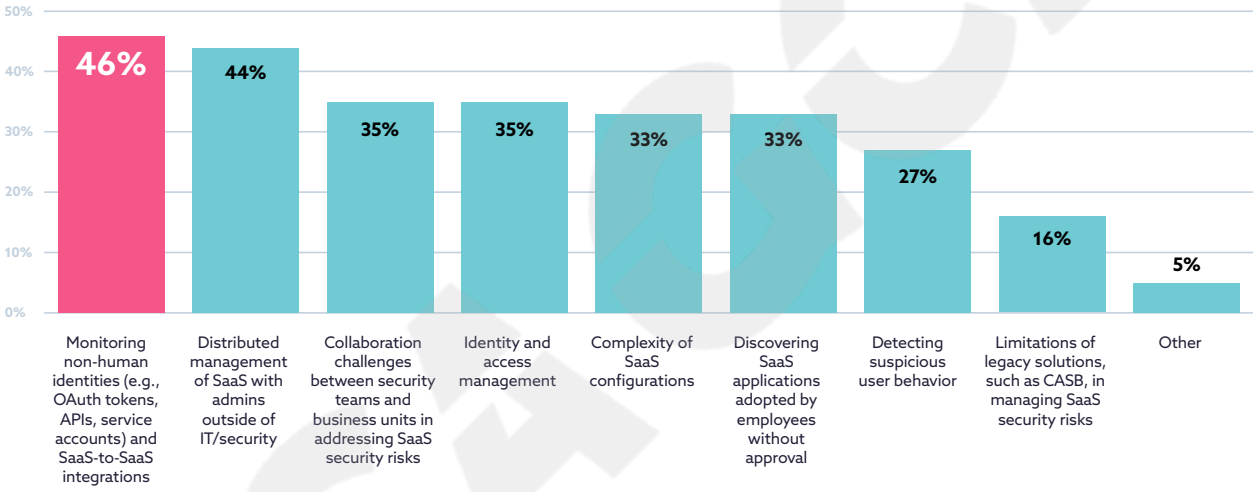
The growing complexity of IAM in SaaS environments is a key driver of broader SaaS security fragmentation. Unlike traditional IAM models, SaaS identity security must account for hundreds of applications, each with unique authentication and role structures. Without a centralized approach, organizations will continue to struggle with enforcing access controls at scale, leaving security gaps that undermine broader SaaS security efforts. To reduce risk, organizations must adopt SaaS security solutions that enforce least privilege, streamline user lifecycle management, and provide consistent oversight across all SaaS applications. Organizations that can integrate these capabilities into their broader SaaS strategy will be better equipped to manage identity-related risks and avoid the compound effect of fragmented security strategies.

Key Finding 5:

Non-Human Identities & SaaS-to-SaaS Integrations Are an Expanding Security Blind Spot

Human identities aren't the only challenge when it comes to IAM; non-human identities (NHIs) are also becoming increasingly difficult to monitor and secure. **Forty-six percent of organizations cite monitoring NHIs as a top challenge**. Organizations are struggling with privilege enforcement, identity sprawl, and lifecycle management for users; these same challenges apply to API-based connections, OAuth tokens, and service accounts often in even more complex ways.

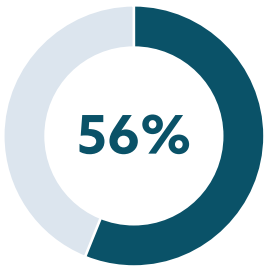
What are the top 3 SaaS security chalenges facing your organization?



A major factor contributing to the rapid growth of SaaS-to-SaaS integrations is the rise of GenAI and copilotized applications. These tools often operate autonomously, executing actions, retrieving data, and triggering workflows without human intervention. **Fifty-six percent of organizations report that third-party vendors and GenAI tools have overprivileged API access to sensitive data**, highlighting how the combination of excessive permission and lack of visibility and oversight can introduce risk. These integrations are frequently set up once and forgotten, leading to an accumulation of unmonitored connections that can be exploited for unauthorized access or data exfiltration.

GenAI and Agentic AI tools further complicate the security landscape. By design, these systems are built to ingest and interact with large volumes of data across applications—necessitating broad access by default. When these tools are deployed without proper governance, they can unintentionally

What are the most significant data exposure risks your organization faces in SaaS applications?



Third-party vendors (and GenAI tools) gaining overprivileged API access to data

access or modify sensitive information beyond their intended scope. Unlike traditional service accounts, GenAI-driven tools often blur the line between human and machine activity, making them difficult to track using conventional IAM approaches for SaaS.

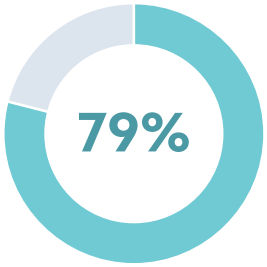
Despite their growing prevalence, NHIs are rarely subject to the same governance rigor as human accounts. NHI security and governance must be integrated into organizations' broader SaaS security strategy. Without dedicated visibility, lifecycle controls, and policy enforcement for NHIs, security teams remain in the dark which allows critical access points to operate unchecked. As NHIs become more central to how SaaS applications interact, overlooking their management further fragments the security landscape, creating inconsistent protections that make it harder to enforce a cohesive SaaS security posture.

Key Finding 6:

Overconfidence in Current SaaS Security Strategy Masks Gaps

While SaaS security is clearly a growing priority, many organizations still lack the integrated strategies and purpose-built tools needed to manage it effectively. Confidence remains high—**79% of organizations report being confident in their SaaS security programs**—but that confidence may be masking critical capability gaps. Security efforts are often stitched together with inconsistent tools, siloed processes, and limited visibility, which collectively undermine the ability to secure the SaaS environment holistically.

Confidence in SaaS security programs



Discovery remains one of the foundational gaps in many organizations' SaaS security strategies. Despite SaaS sprawl, **42% of organizations say they lack comprehensive SaaS discovery capabilities**, limiting their visibility into which applications are in use, where sensitive data resides, and how users are interacting with those apps. Discovery is not just an essential first step to securing SaaS, but an ongoing capability that supports posture management, threat detection, and risk remediation. Without it, organizations are flying blind, unable to identify misconfigurations, enforce consistent policies, or detect unsanctioned tools before they become security liabilities. It's no surprise then, that **55% of organizations report employees are still signing up for unsanctioned or free SaaS tools**, introducing unmanaged risks and expanding the attack surface beyond what security teams can effectively monitor or control.

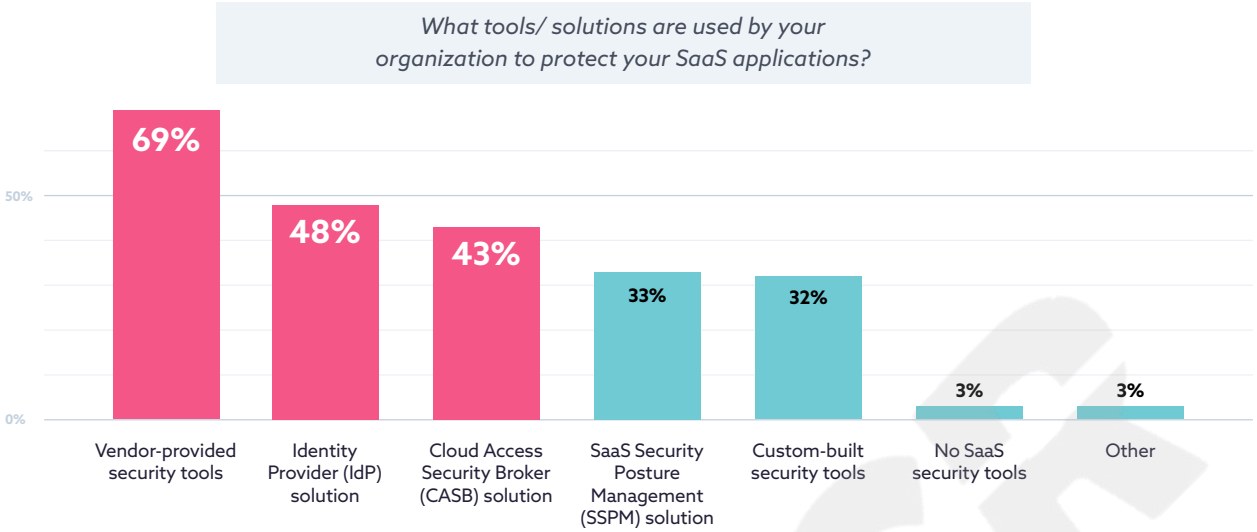
What are the biggest challenges your organization faces in identifying all SaaS applications in use?

Employees signing up for free versions of SaaS applications

55%

Lack of tools for comprehensive SaaS discovery

42%

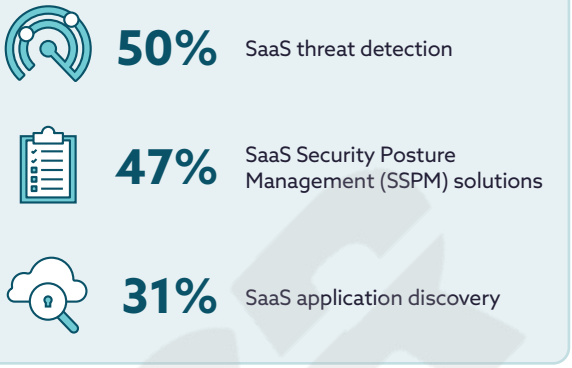


Despite the pace and complexity of SaaS adoption, **46% of organizations still rely on manual audits to manage SaaS risks**—a reactive and resource-intensive approach ill-suited to dynamic, app-driven environments. **In addition, 69% of organizations rely on vendor-provided, native security features** within individual SaaS applications. This approach often results in isolated controls and inconsistent protections across the broader SaaS environment. The recent Snowflake customer breach serves as a reminder of why relying solely on vendor-native controls can be risky. When organizations assume providers will handle all aspects of security, they may overlook critical responsibilities, such as identity governance, API monitoring, or threat detection. As seen in that case, even trusted providers cannot fully shield organizations from breaches if internal misconfigurations or inadequate oversight are present. This reinforces the importance of a shared responsibility model and the need for organizations to maintain independent visibility and control.

Many also turn to more general cloud security solutions, such as **Identity Providers (IdPs) (48%) and Cloud-Access Security Brokers (CASBs) (43%)**, in an effort to extend coverage. While these tools serve an important role in broader security architectures, they may not be well suited to address the SaaS-specific issues organizations are currently facing. The continued reliance on a piecemeal approach, highlighted in both this report and in the 2024 CSA SaaS Security Survey, suggests that without a shift in approach, these gaps may persist and even widen as SaaS environments grow more complex.

Encouragingly, organizations are starting to prioritize the types of solutions that align with their most pressing challenges—**50% now prioritize SaaS threat detection**, **47% are prioritizing Saas Security Posture Management (SSPM)**, and **31% are prioritizing application discovery**. These trends indicate a shift away from legacy approaches and toward a more proactive mindset—one that recognizes that visibility, control, and response capabilities must all work together to secure the entire SaaS ecosystem. Taken together, the data reflects SaaS security strategies that remain fragmented, reactive, and incomplete.

Which aspects of SaaS security does your organization currently prioritize?



To close the gap between growing investment and actual capability, organizations must move beyond ad hoc, app-by-app controls toward a more unified approach—one that addresses core challenges, such as discovery, posture management, threat detection, and risk remediation. The growing prioritization of SaaS threat detection and posture management along with the overall elevation of SaaS security as a top priority, signals that many organizations are ready to address their current challenges and create a more holistic and coordinated strategy.

Conclusion: SaaS Security Is a Work in Progress

SaaS security has become a top organizational priority, with increased budget allocations and growing attention to core areas like threat detection and posture management. Organizations recognize the importance of SaaS in their operational infrastructure and are taking steps to secure it. But while confidence in SaaS security programs is high, the findings suggest that many organizations are still early in their journey toward building mature, scalable SaaS security strategies.

The risks driving this urgency are real. Sensitive data is flowing through SaaS environments yet many organizations struggle with enforcing least privilege access and tracking where data resides or how it's shared. Oversharing, unauthorized uploads, and excessive third-party access point to a lack of visibility and control across the data lifecycle. Without stronger governance and centralized oversight, these gaps leave sensitive data vulnerable to both internal missteps and external threats.

At the same time, the decentralized nature of SaaS adoption and management continues to complicate security efforts. Employees adopt applications without security involvement, and critical platforms like HR and marketing are often managed outside IT entirely. This creates inconsistency in how SaaS applications are onboarded, configured, and monitored—and when no single team owns the process end to end, security responsibilities fall through the cracks. Collaboration and accountability remain among the biggest barriers to risk remediation, keeping many organizations in a reactive rather than proactive security posture.

These challenges are further compounded by identity-related issues, which span both human and non-human identities. Human IAM remains a persistent problem due to inconsistent privilege management and a lack of automation in identity lifecycle processes. Non-human identities—including OAuth tokens, API connections, and increasingly autonomous GenAI tools—add yet another layer of complexity. These integrations often operate outside the scope of traditional IAM, creating unmonitored and over-privileged pathways that expand the attack surface and evade detection.

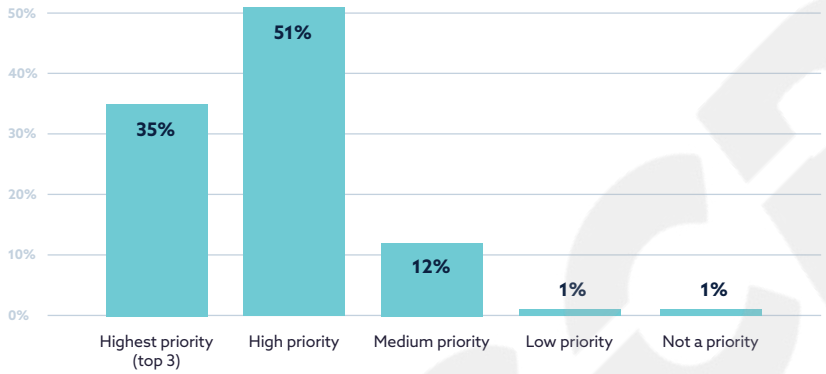
Taken together, the findings reveal that SaaS security continues to be an afterthought. Despite clear progress in prioritization and investment, most organizations are still relying on tools and strategies not built for the realities of SaaS—including manual audits, general-purpose cloud security solutions, and native app-level controls. Most organizations are working with incomplete coverage and inconsistent enforcement, leaving their environments exposed and their confidence potentially misplaced.

To keep pace with the speed of SaaS and AI innovation, organizations must act now. That starts with expanding awareness—understanding what tools, strategies, and practices are best suited to support SaaS security as an ecosystem, not a set of disconnected applications. Whether through better discovery, automated posture management, or proactive risk detection, a more integrated and forward-looking approach is needed. With SaaS adoption only accelerating, the window to address these foundational challenges is closing fast.

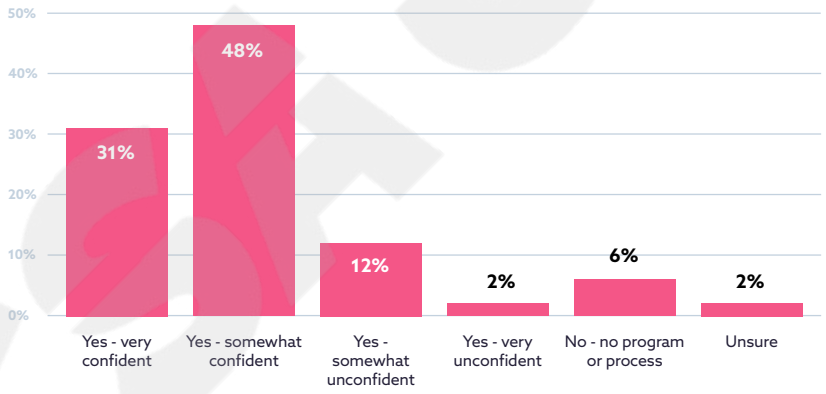
Full Survey Results

Overview

In your organization, how important is SaaS security?

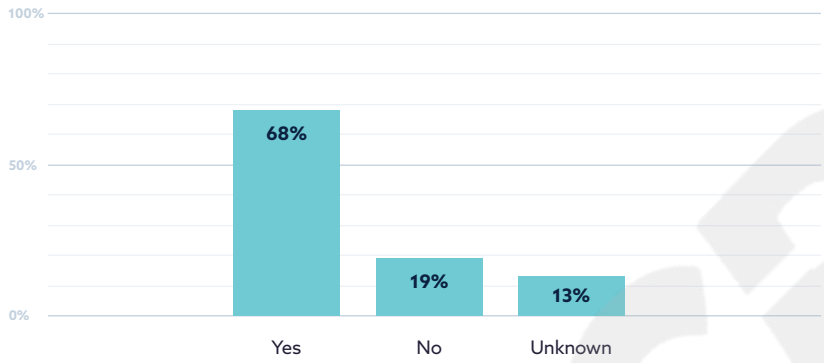


Does your organization have a program or process for securing SaaS applications? If yes, how confident are you in its effectiveness?

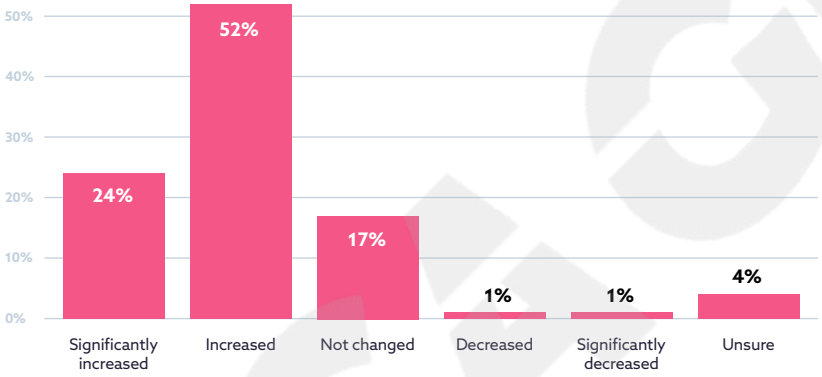


SaaS Security Program

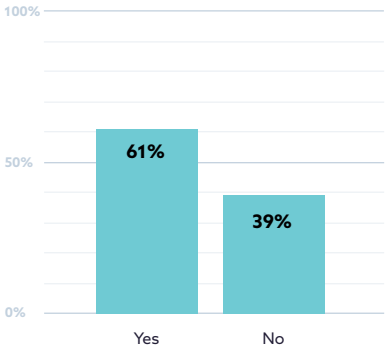
Is SaaS Security budgeted for in your organization?



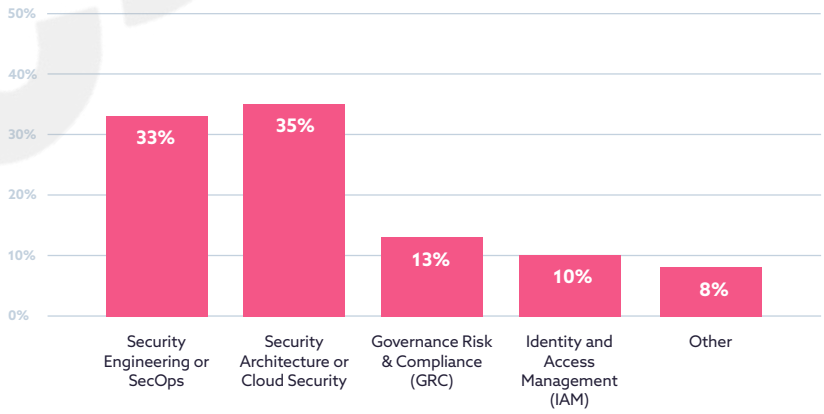
How has the budget for SaaS security changed over the past 2 years?



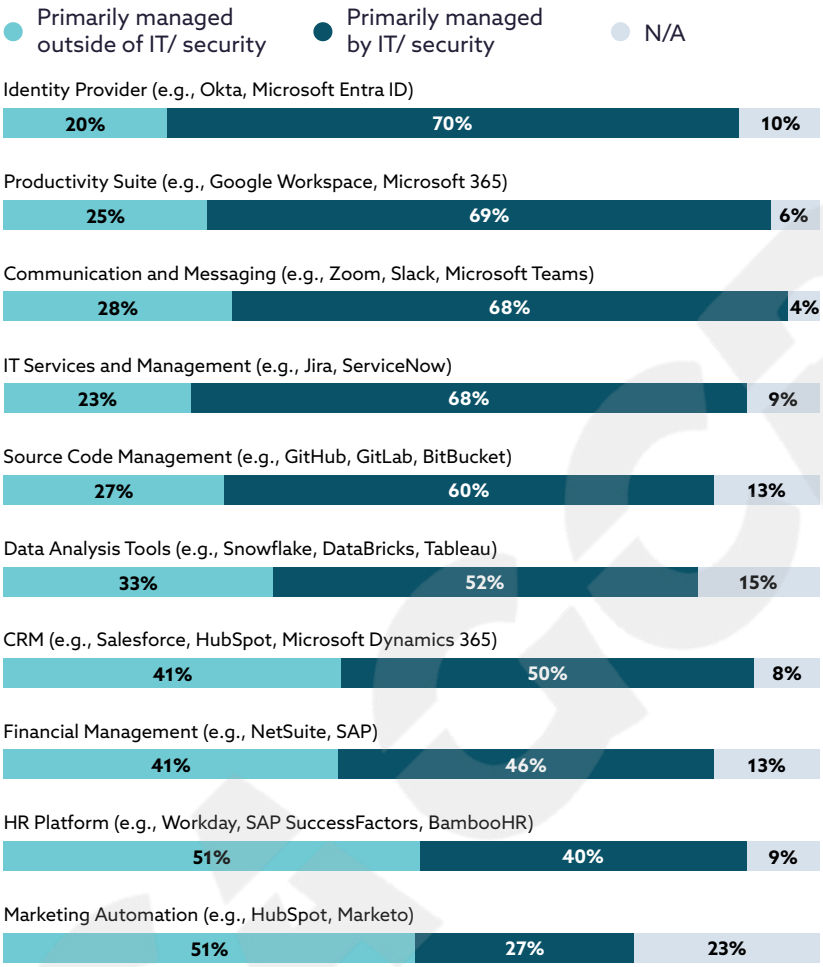
Does your organization have specific personnel focused on SaaS security?



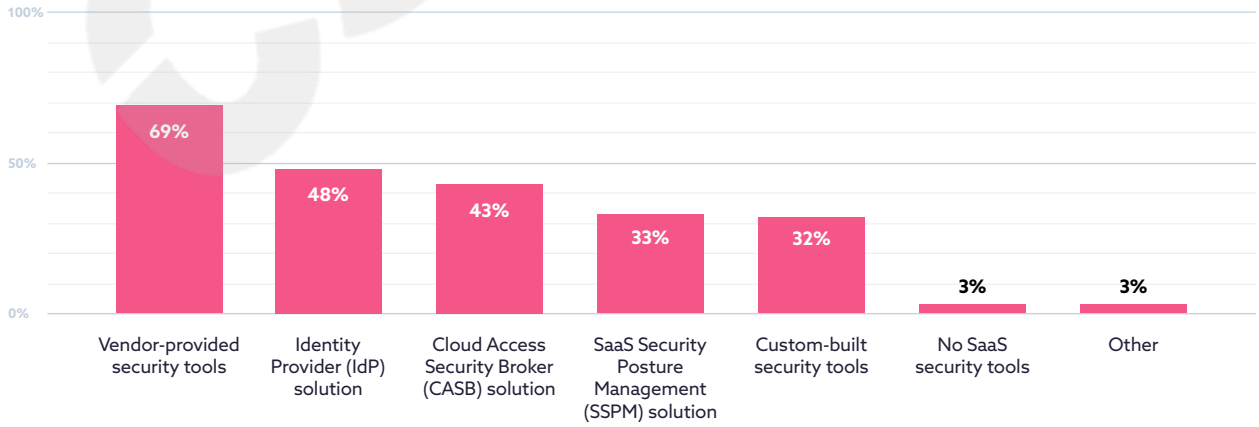
Which team is primarily responsible for SaaS security in your organization?



Which SaaS applications in your organization are primarily managed outside of IT/ security?

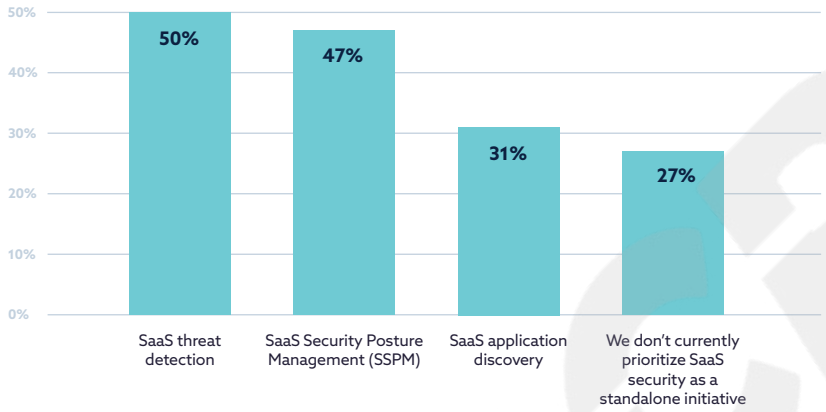


What tools/ solutions are used by your organization to protect your SaaS applications?

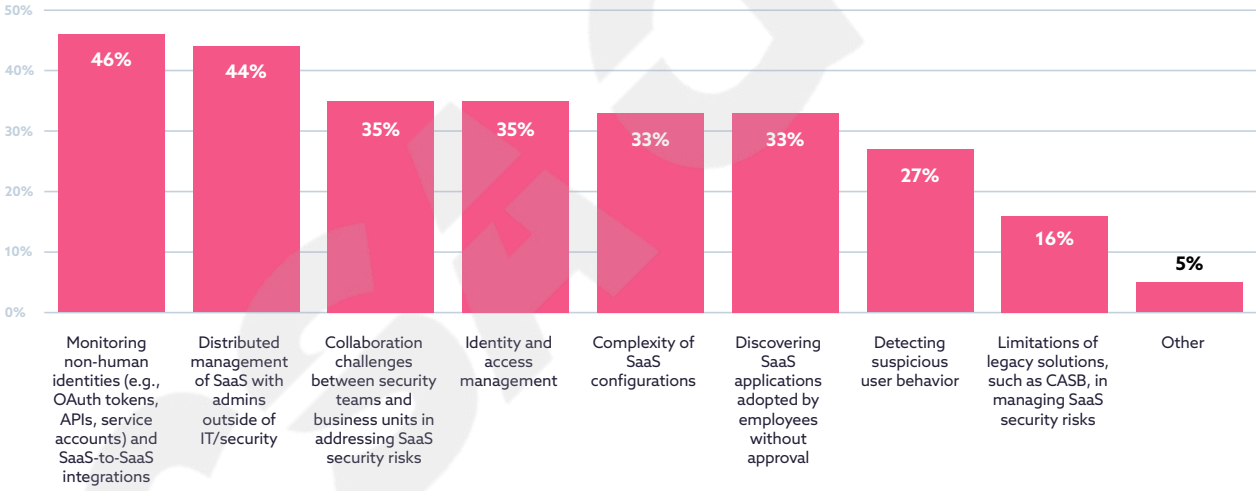


Priorities and Challenges

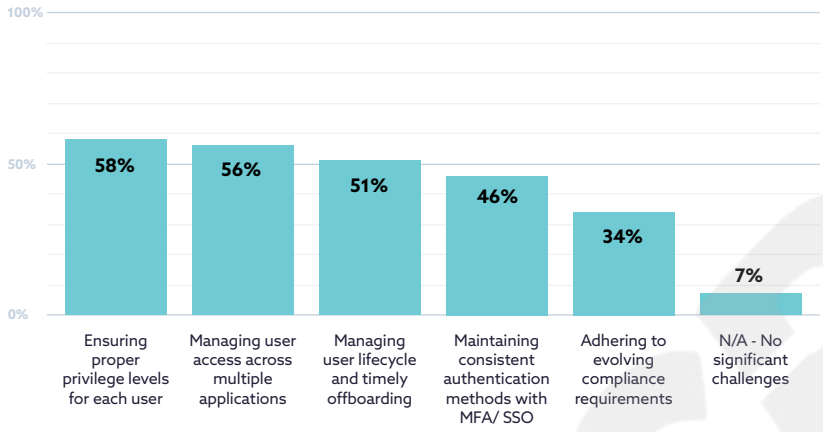
Which aspects of SaaS security does your organization currently prioritize?



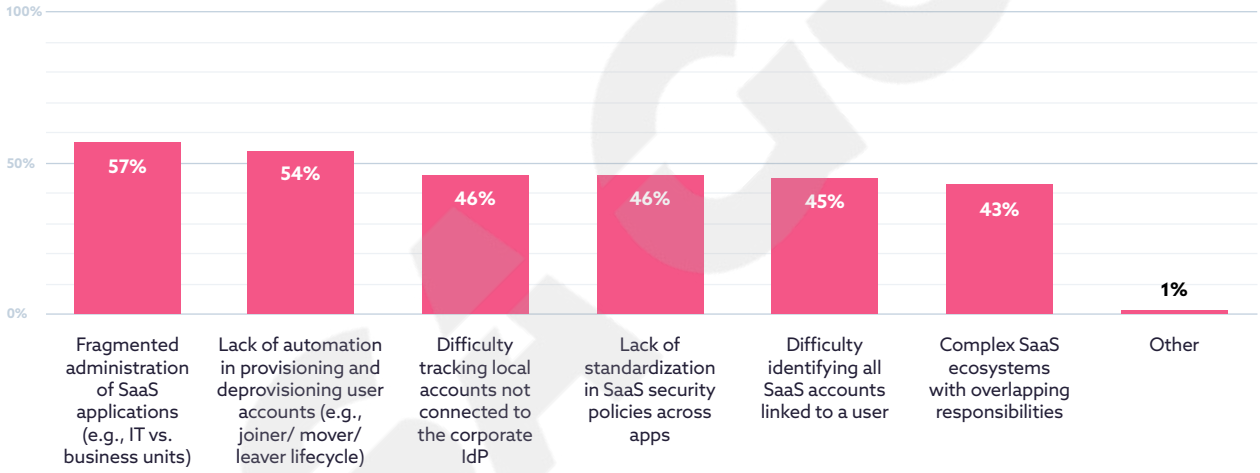
What are the top 3 SaaS security chalenges facing your organization?



What challenges does your organization face with Identity and Access Management (IAM) for SaaS?

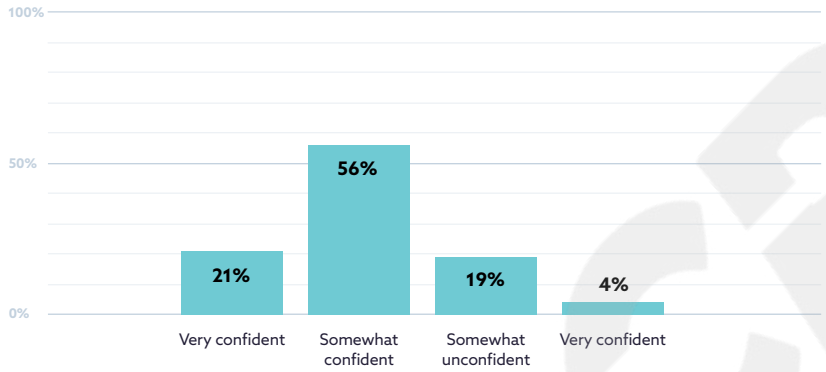


What are the primary factors contributing to these IAM challenges?

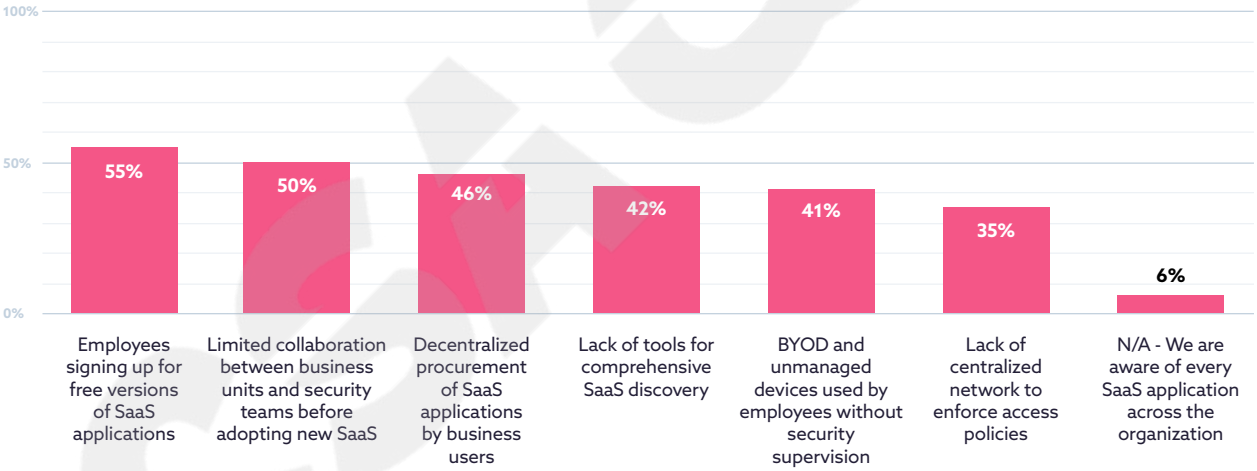


SaaS Discovery

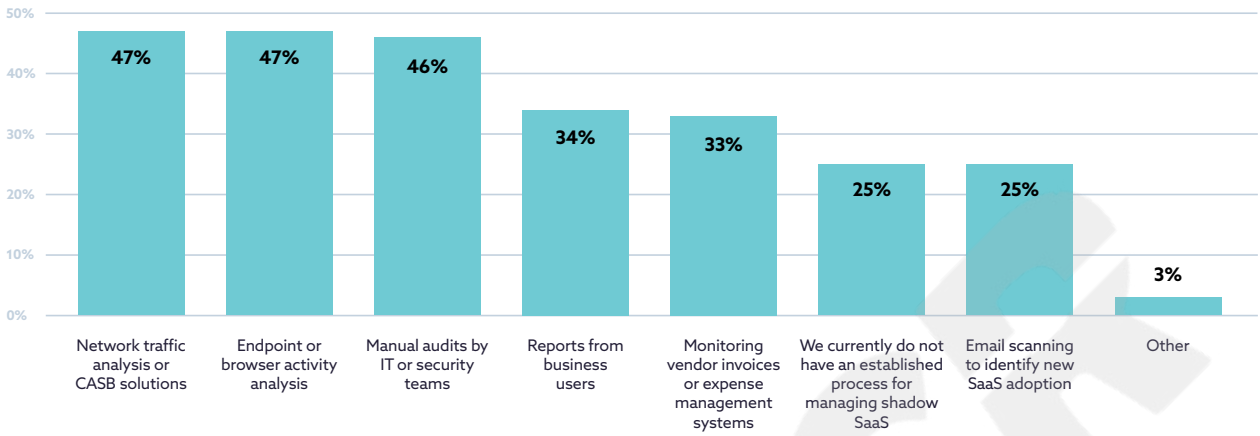
How confident is your organization in its ability to detect all SaaS (sanctioned and unsanctioned) applications currently in use across the organization?



What are the biggest challenges your organization faces in identifying all SaaS applications in use?

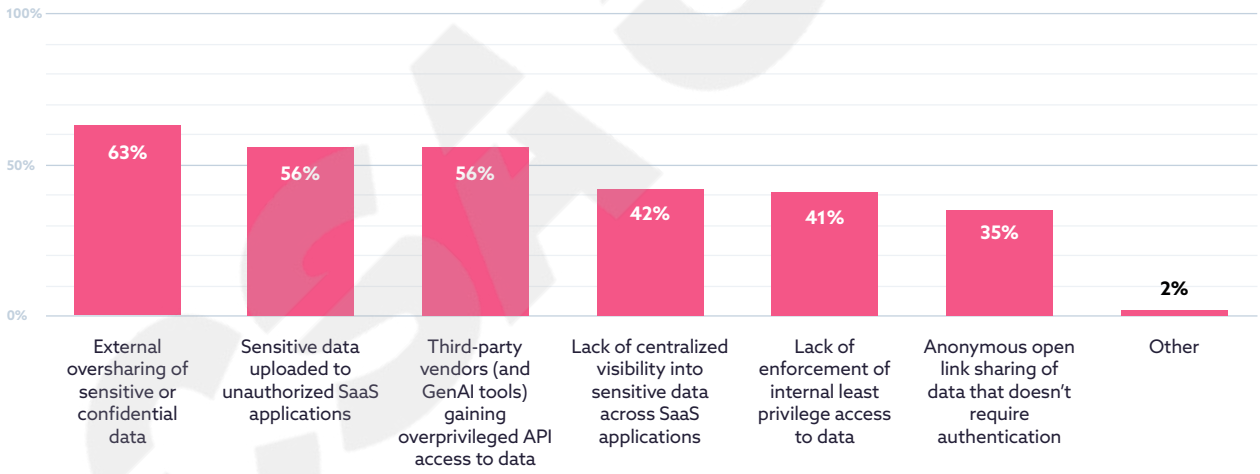


What processes or tools does your organization use to discover and manage shadow SaaS applications?

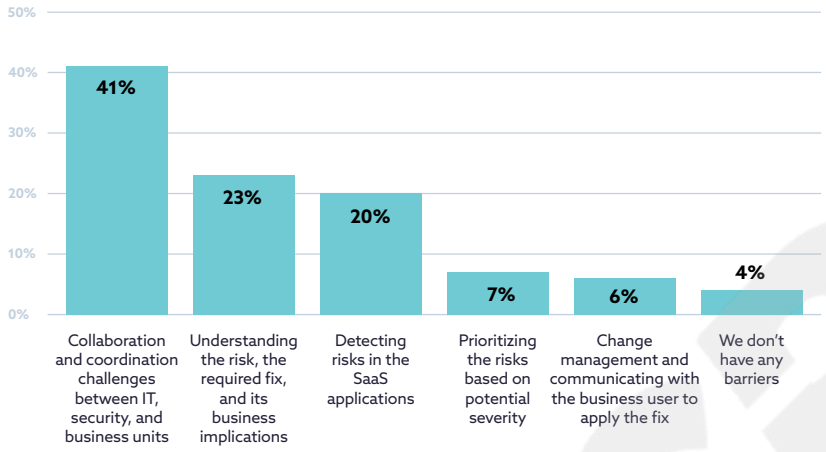


SaaS Security Incidents

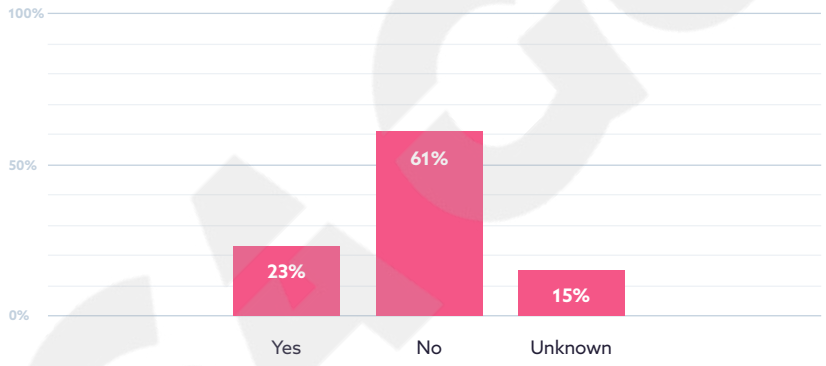
What are the most significant data exposure risks your organization faces in SaaS applications?



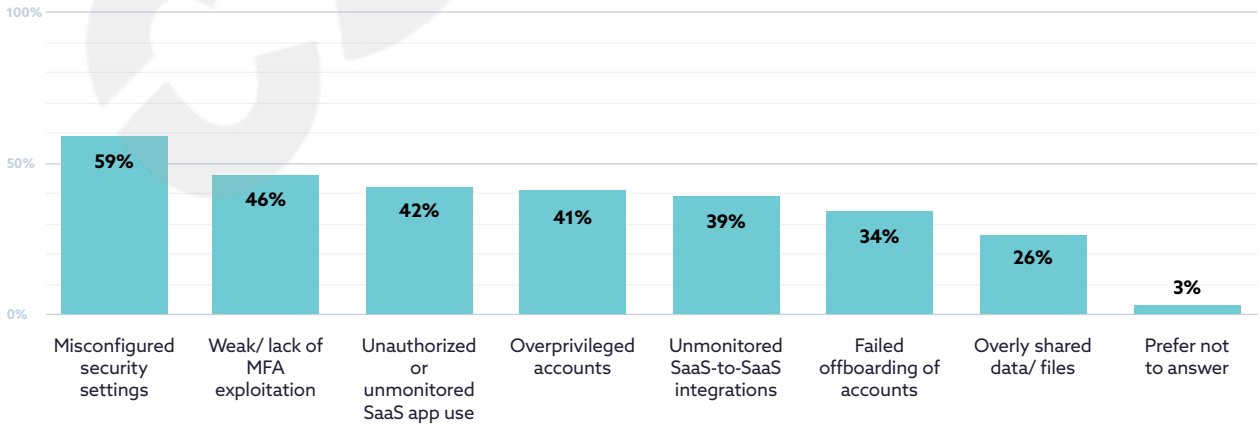
What is the largest barrier to remediating SaaS risks in your organization?



Has your organization been impacted by a SaaS breach the past 12-18 months?

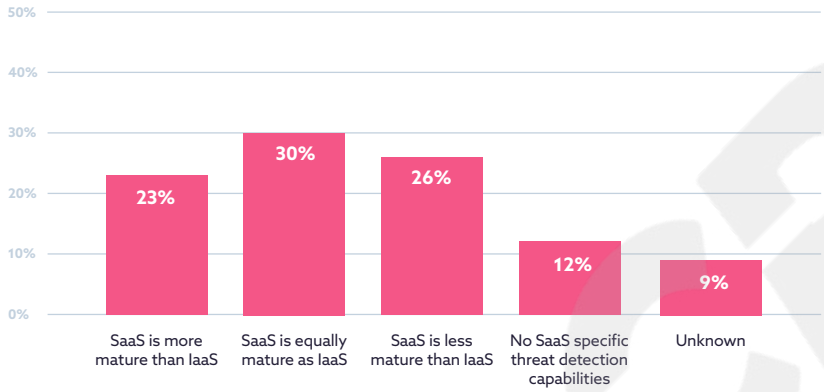


What was the cause(s) of the breach(es) your organization experienced?

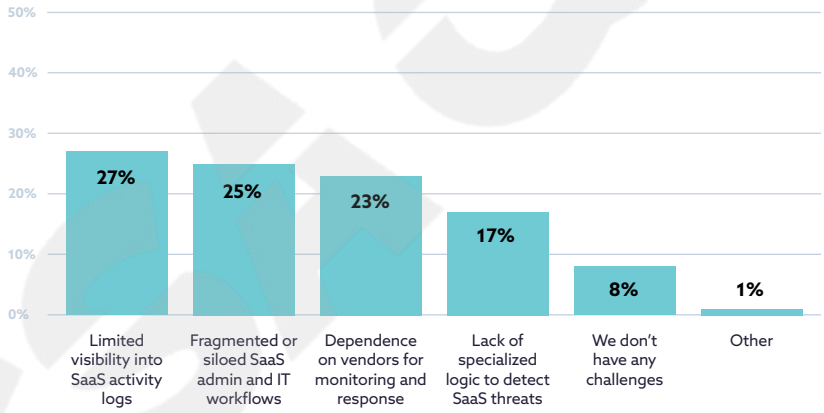


SaaS Detection and Response

How does your organization's SaaS threat detection and response capabilities compare to those for IaaS?



What is the biggest challenge your organization faces in detecting and responding to SaaS-specific threats?

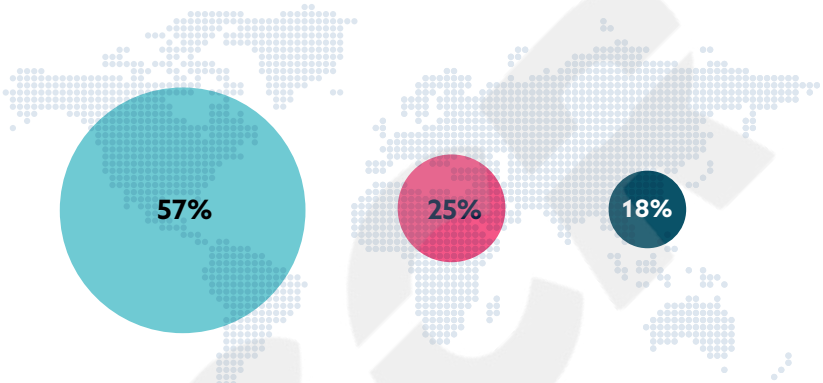


Demographics

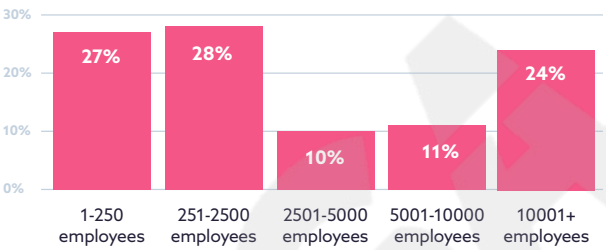
This survey gathered insights from 420 IT and security professionals across a diverse range of organizations, spanning different industries, sizes, and geographic regions. The demographic breakdown provides important context for understanding the findings, highlighting the varied experiences and challenges faced by organizations in different sectors and operational scales.

What region of the world are you located in?

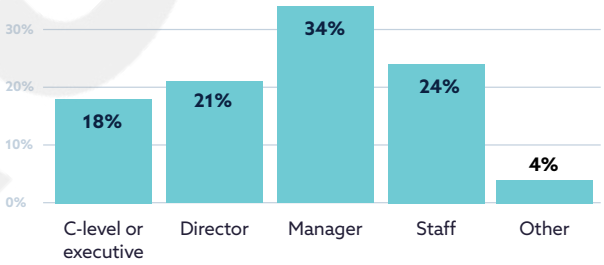
- Americas
- Europe, Middle East, Africa (EMEA)
- Asia Pacific (APAC)



Organization size



Which best describes your job level?



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

33%	Telecommunications, Technology, Internet & Electronics	3%	Education	1%	Airlines & Aerospace (including Defense)
16%	Finance & Financial Services	2%	Advertising & Marketing	1%	Entertainment & Leisure
6%	Retail & Consumer Durables	2%	Automative	1%	Food & Beverages
6%	Prefer not to answer	2%	Business Support & Logistics	1%	Health & Fitness
5%	Healthcare & Pharmaceuticals	2%	Nonprofit	1%	Real Estate
5%	Government	2%	Transportation & Delivery		
4%	Manufacturing	2%	Utilities, Energy, and Extraction		
3%	Construction, Machinery, and Homes	1%	Agriculture		

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.

Valence Security commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding SaaS security. Valence Security financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in January 2025 and received 420 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 study aims to assess the **current state of SaaS security**, uncover key challenges, and explore how organizations are securing and managing their SaaS environments. Through industry insights, we seek to:

- **Understand SaaS security management:**
  Who is responsible, what tools are used, and how security is enforced.
- **Identify top risks and challenges:**
  Including misconfigurations, identity security gaps, shadow IT, and third-party access risks.
- **Evaluate security strategies and investments:**
  How organizations prioritize SaaS security, allocate budgets, and adopt security solutions.
- **Examine emerging threats:**
  The impact of AI-driven integrations, SaaS-to-SaaS connections, and non-human identities (NHIs).