2025 SaaS Security Risks Report

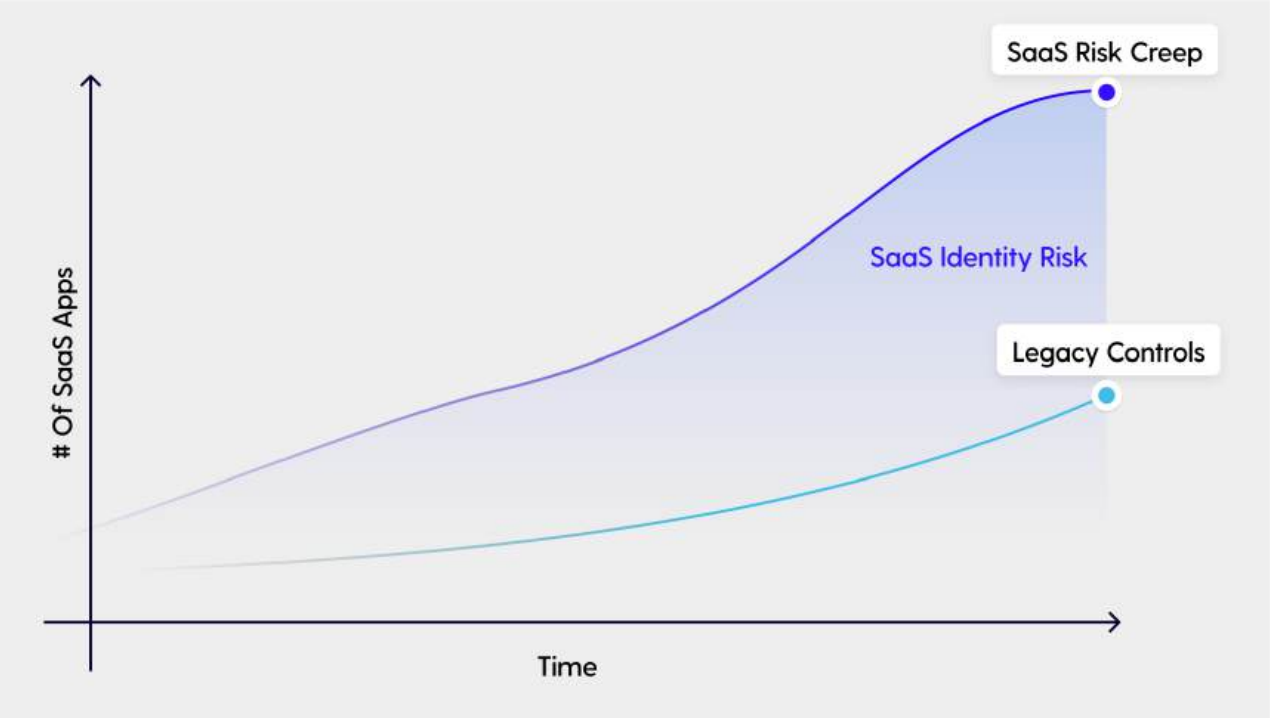
grip

Table of Contents

Executive Summary

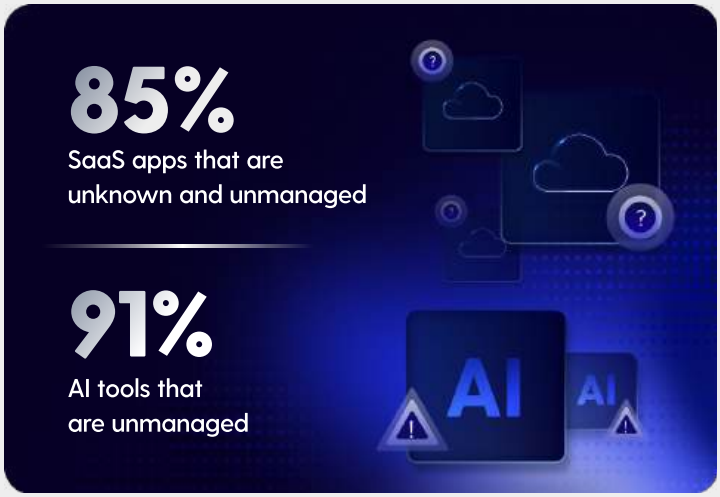
The explosive growth of SaaS, the surge in Shadow IT, and the rapid adoption of AI have created a tsunami of risks that many organizations are unprepared to handle. Businesses are now heavily reliant on SaaS, and as these apps become more accessible, employees are increasingly bypassing IT departments, resulting in a flood of unmonitored and unsecured software.

This report takes a comprehensive look at how shadow SaaS and shadow AI are reshaping the security landscape. Using anonymized data from the SaaS Security Control Plane (SSCP) deployments, Grip analyzed over 29 million SaaS user accounts, 1.7 million identities, and 23,987 distinct SaaS applications to understand the scale and nature of these risks. The findings highlight a growing challenge: traditional security measures are no longer enough to protect organizations from "SaaS risk creep," the slow but steady accumulation of vulnerabilities that arise from unmanaged apps and the user accounts tied to them.



As organizations increasingly manage more SaaS apps and user accounts than ever before, a new strategic approach is essential. Gartner projects that by 2027, 75% of employees will use technology outside of IT's purview. This shift demands more than just monitoring—it requires a complete rethinking of SaaS security to address the nuances of shadow SaaS and shadow AI. Without adapting to these changes, enterprises face an expanding gap between perceived security and the reality of unmonitored risk. A flexible, identity-centric approach that empowers employees while controlling risk is the only way forward in this evolving landscape.

Key Findings

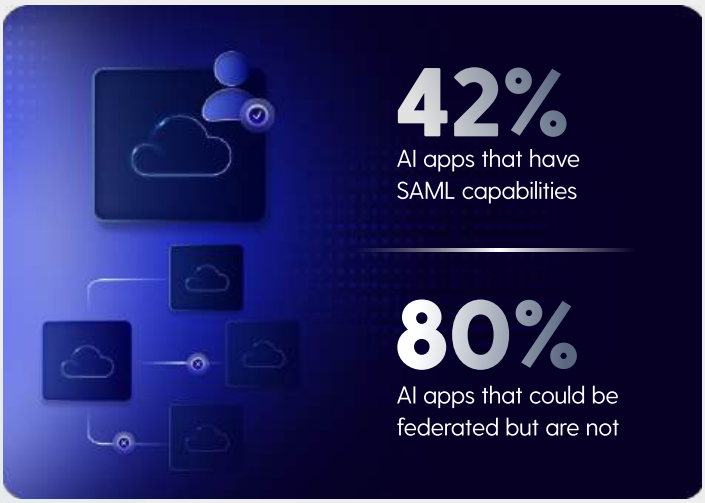


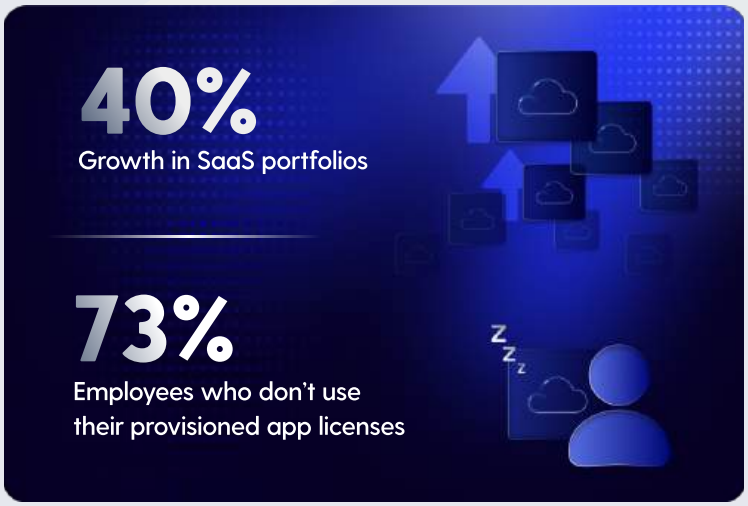
SaaS ignorance is not bliss—it's a growing problem.

Shadow SaaS and shadow AI are grossly underestimated and pose more significant risks than most organizations realize. As the number of unsanctioned apps and AI grows, so does the organization's exposure to potential security breaches.

AI adoption is outpacing security governance by a 4:1 margin.

Without proper governance, AI apps create blind spots in identity security, leaving potential entry points for cyberattacks. Balancing the benefits of AI with the risks it poses is critical, as unmanaged adoption can leave businesses vulnerable to significant security threats.





Efficient growth hinges on tech optimization, not consolidation.

While tech consolidation has been a popular strategy, employee behavior tells a different story. As employees independently adopt new SaaS tools, many of the SaaS licenses provisioned for them go unused. This creates a dual problem of risk exposure and financial waste, underscoring the need to optimize tech usage rather than just reduce tools.

SaaS Adoption Continues to Grow

As the SaaS market grew, so did adoption in the workforce.

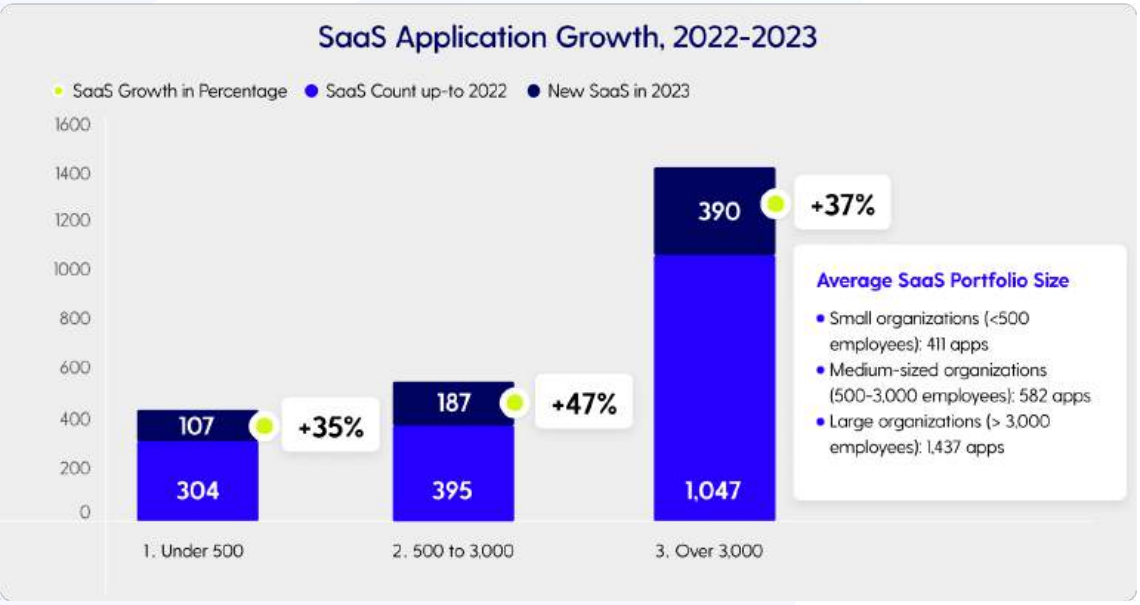
A trend that started during the pandemic has led to a surge in employees acquiring their own SaaS tools, driving a spike in SaaS usage organization-wide. Remote workers found it easy and convenient to start cloud subscriptions independently without consulting IT. According to industry data, SaaS adoption skyrocketed 62% in the first year of COVID lockdowns (2019-2020) and grew another 28% the following year. Despite previous efforts to consolidate technologies, decentralized SaaS gained momentum, a trend that continues today. Consequently, organizations now have more SaaS apps and identities than ever before, most of which were procured by employees or functional teams outside of IT's visibility.

SaaS App Stats

In 2023, small companies used 411 apps, medium companies 582 apps, and large companies 1,437 apps. These figures represent a substantial increase from 2022, an average increase of 40%.

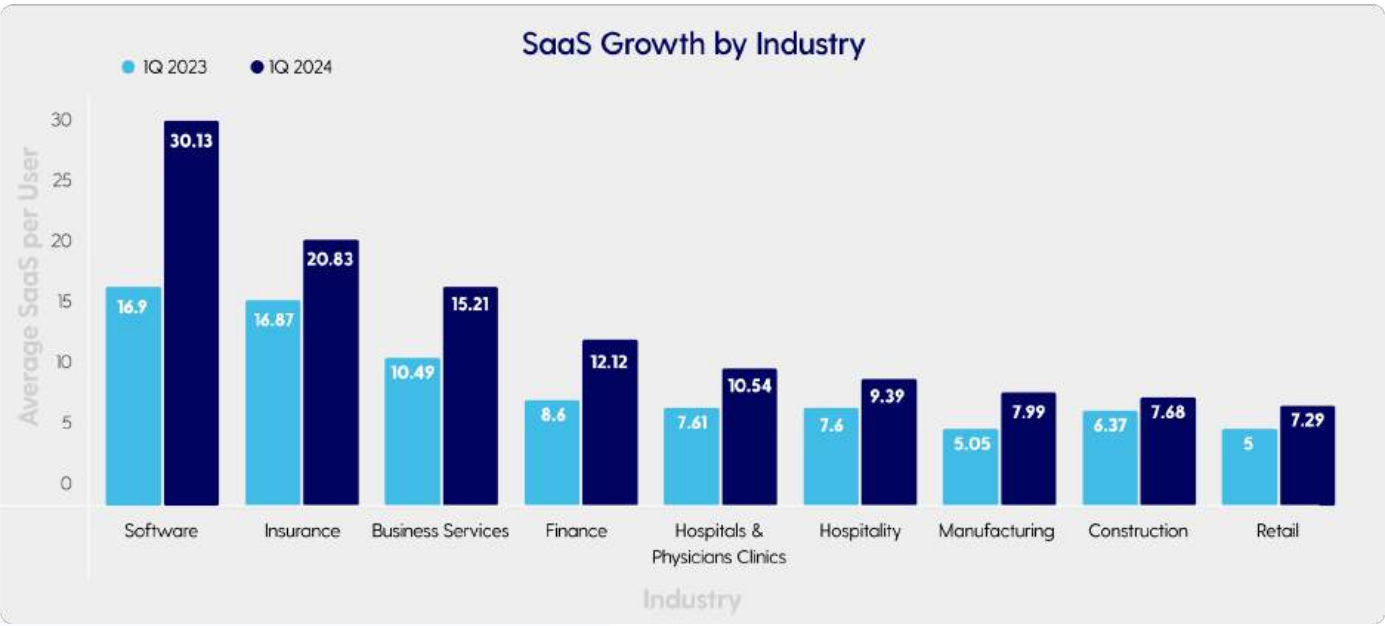
SaaS portfolios grew by **40%** in 2023

Analyzing the data by company size reveals that medium-sized companies adopted SaaS at the highest rate, a 47% increase, compared to 35% for small companies and 37% for large companies. This variance may be attributed to the unique position of medium-sized companies, as they often lack the robust governance, risk, and compliance (GRC) functions that large companies possess, making them more agile and open to adopting new tools. Conversely, they are not small enough to rely on a single team's consensus for tool usage, necessitating a broader range of applications to meet diverse needs.



SaaS Adoption by Industry

SaaS adoption surged across all industries, reflecting a broader trend as companies strive to stay competitive, adapt to changing market demands, and increasingly rely on cloud-based solutions. Between Q1 2023 and Q1 2024, sectors like software, insurance, and business services substantially increased SaaS usage, driven by the need for scalable solutions to enhance efficiency and foster innovation.

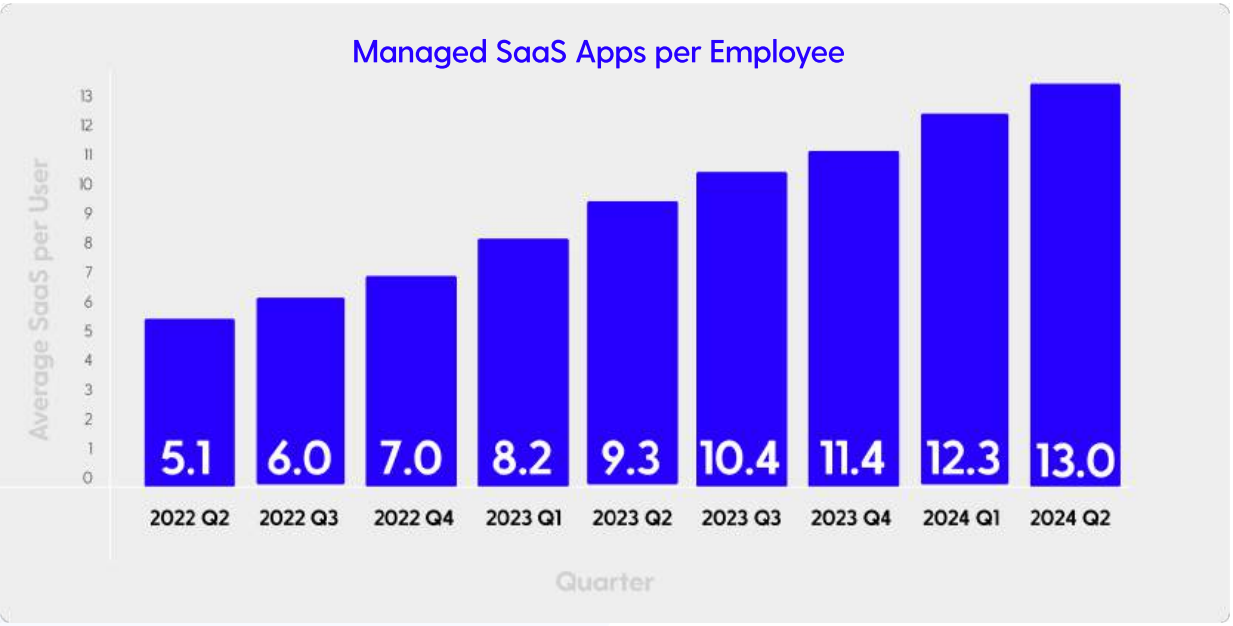


The software industry, already at the forefront of technological advancements, relies on SaaS to enhance collaboration and streamline development processes. Insurance companies leverage SaaS tools to improve customer service, claims processing, and regulatory compliance. Meanwhile, business service organizations are adopting SaaS to optimize operational workflows and offer more dynamic service offerings. As these sectors expand their SaaS portfolios, implementing strong security and governance measures becomes critical to managing the associated risks.

> **"What surprised us was just how much our SaaS and identity landscape changed day-to-day and week-to-week.**
>
> Director of IT and Security

SaaS per Employee - Provisioned vs. Used

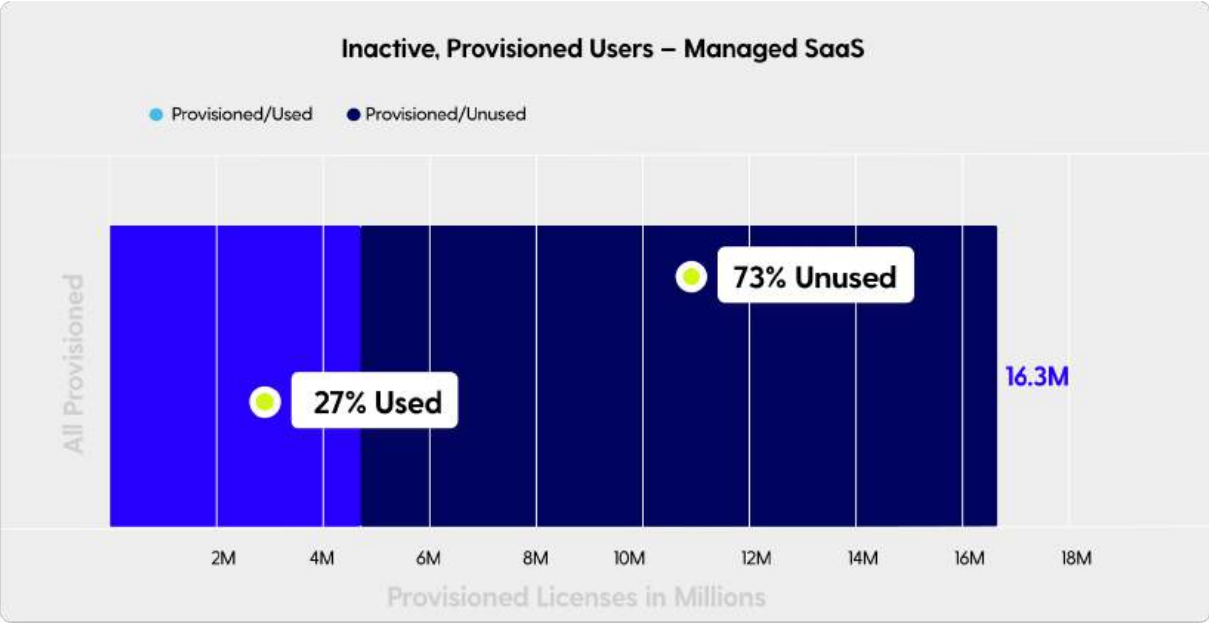
The number of SaaS applications per employee has steadily risen, marking an 85% increase in managed SaaS tools usage when broken down by individual users. In 2022, employees used an average of 7 tools, which rose to 11 in 2023 and increased to 13 by early 2024. This trend highlights the growing reliance on SaaS applications as an integral component of an employee's daily workflow.



However, the data also reveals discrepancies between provisioned SaaS licenses and actual usage. While IT teams provision 30 SaaS tools on average for employees, they use only 13 on average. This gap between the number of tools employees are given and the number they actually use results in overspending on licenses for software that isn't fully utilized. This discrepancy becomes even more critical at a time when tech spending is under intense scrutiny.

To illustrate, a large enterprise leveraged Grip to audit the usage of Adobe licenses. Based on their findings, they were able to reclaim unused SaaS licenses and re-negotiate their software contract, saving them almost a million dollars annually.

The above example is not uncommon. When isolating usage data for managed applications, Grip research shows that, on average, 73% of provisioned users never utilized their application license. This indicates that even managed SaaS tools are not adequately monitored and maintained, leading to significant security and compliance risks, wasted budget dollars, and operational inefficiencies.



Organizations must prioritize gaining visibility into all identities across the enterprise to reduce security risks and optimize tech expenditures. It is also essential to implement ongoing monitoring to regularly prune unused accounts and identify account usage and activity changes to ensure that all managed applications and identities remain secure. Through comprehensive SaaS management practices, organizations can protect against potential breaches and control technology spending even as the SaaS landscape changes and identities grow.

Sprawling SaaS Accounts & Identities

While the number of SaaS applications in use has experienced explosive growth, an equally important trend is the significant increase in the number of SaaS accounts. Unlike the sheer count of different apps, SaaS accounts refer to the number of individuals accessing a single application. This figure is typically higher than the number of SaaS applications within an organization, as a single tool can have multiple users. For instance, consider Microsoft Office—while it's counted as one SaaS application, it can support many users within the same organization, reflecting a much larger user base than the number of applications alone.

While the average SaaS portfolio or number of applications used within an enterprise illustrates the growing reliance on cloud-based solutions to manage diverse business functions, the exponential growth in accounts demonstrates the increased risks to an organization's attack surface. Each account signifies a user with specific roles, responsibilities, and access levels, contributing to the overall complexity of SaaS identity risk management. As organizations onboard more users onto these applications, the challenges of securing, managing, and optimizing SaaS accounts become more pronounced.

Managing this surge in SaaS accounts means organizations must prioritize effective account governance to safeguard their digital assets and maintain operational integrity. The growing number of accounts also necessitates regular audits and reviews to identify inactive or redundant accounts, which can pose additional security vulnerabilities and inflate technology costs.

SaaS Realizations

The heightened adoption of SaaS emphasizes three key realizations:

1. Organizations need streamlined, comprehensive, and systematic security measures to manage the expanding SaaS landscape, particularly the apps acquired outside IT's visibility and bypass traditional security reviews.

2. CISOs, responsible for mitigating risks and safeguarding their organization, now face increased exposure and liability from SaaS employees adopt independently, outside their knowledge.

3. As SaaS procurement behaviors shift, CISOs must transition from gatekeepers to secure innovation enablers. By embracing a programmatic approach towards decentralized SaaS adoption, CISOs can mitigate the risks while empowering business units to meet their technology needs. This means fostering collaboration, improving visibility into departmental technology acquisitions, and implementing robust governance frameworks that allow for secure and compliant use of unsanctioned tools.

> **"It's a difficult balance to enable a highly distributed workforce with such diversity of tools and SaaS apps in use.**
>
> Head of Information Security

Organizations Struggle to Manage SaaS Growth

"Unmanaged SaaS" refers to any application not centrally monitored, maintained, or controlled by the organization's IT department, posing significant security risks and operational inefficiencies. The data clearly shows that SaaS management is a universal problem.

Regardless of an organization's size, securing SaaS environments is a struggle, especially as the use of SaaS tools skyrockets and employees start new subscriptions. Isolating baseline averages before adopting Grip, the data reveals that unmanaged SaaS far exceeded managed applications: managed SaaS hovered around 10-15%, and 85-90% of SaaS tools were unmanaged.

While the importance of SaaS security is well-recognized, organizations face difficulties addressing it effectively. Technical debt, or the backlog of software and systems that have not been adequately managed, documented, or integrated over time, has long been thought to be the primary driver behind the high proportion of unmanaged SaaS. However, it is only one of the contributing factors. Looking at the initial baseline average and isolating SaaS onboarded in 2023 shows that 82-90% of new applications were unmanaged, a consistent trend across different company sizes. Underlying causes include a lack of awareness of the SaaS tools used across an enterprise, understaffed IT teams, and, once SaaS is discovered, technical limitations such as applications not supporting SAML or imposing high premiums for it.

Digging deeper and further analyzing both managed and unmanaged applications, we found that 27% of unmanaged apps were verified to support SAML, though it wasn't enabled. Of the managed applications, 63% have semi-managed user access, meaning a social login is being used, and 53% are accessed using local app credentials or a user-defined login and password.

The data paints a clear picture: there's a massive gap in SaaS governance. Users independently acquire applications that are not federated and create their own credentials, which often fail to comply with strict organizational policies. This practice opens up significant security vulnerabilities, exacerbated by common issues such as password reuse, weak password choices, and access from unmanaged or personal devices. Industry data cites that only 12% of users consistently use different passwords, and over half of users (52%) use easily guessable information, such as pet names or "123456", making it easy for cybercriminals to crack their passwords.

85%- 90%

of SaaS in use is unmanaged.

27%

of SAML-supported apps do not have it enabled.

Governance gaps expand when unmanaged or personal devices are used to access corporate applications. Compromised credentials were responsible for 19% of data breaches in 2023, showcasing the significant impact weak password practices can have on overall security. Improving password hygiene and implementing robust identity security governance are essential steps to mitigate these risks and protect organizational data.

As the "business-led IT" trend grows, organizations must approach SaaS identity management using systematic, data-driven processes to mitigate SaaS risk creep and address operational inefficiencies. The primary challenge stems from a lack of visibility into the applications used across an organization. Shadow SaaS—tools that employees adopt independently without IT oversight—means that IT departments are often unaware of the full scope of SaaS applications in use, making it difficult to implement comprehensive security measures and governance protocols.

Additionally, security teams frequently rely on SaaS Security Posture Management (SSPM) tools, which, while useful for managing known SaaS applications, fail to detect shadow SaaS. Similarly, Cloud Access Security Brokers (CASBs) are designed to provide visibility and control over cloud services but often generate excessive data noise and false positives, which are overwhelming and time-consuming for security teams to sift through. This makes it challenging to extract actionable insights and address SaaS security risks effectively, often resulting in a reactive response vs. a proactive one. Only by addressing these core issues can organizations manage their expanding SaaS environments, contain risk creep, and mitigate the associated risks.

Defining Unmanaged, Managed, and Tolerated SaaS

The terms used to describe the status of SaaS within an organization are defined as:

Unmanaged SaaS includes shadow IT and SaaS applications that the organization does not centrally monitor or govern access. These apps are often called "unfederated" SaaS.

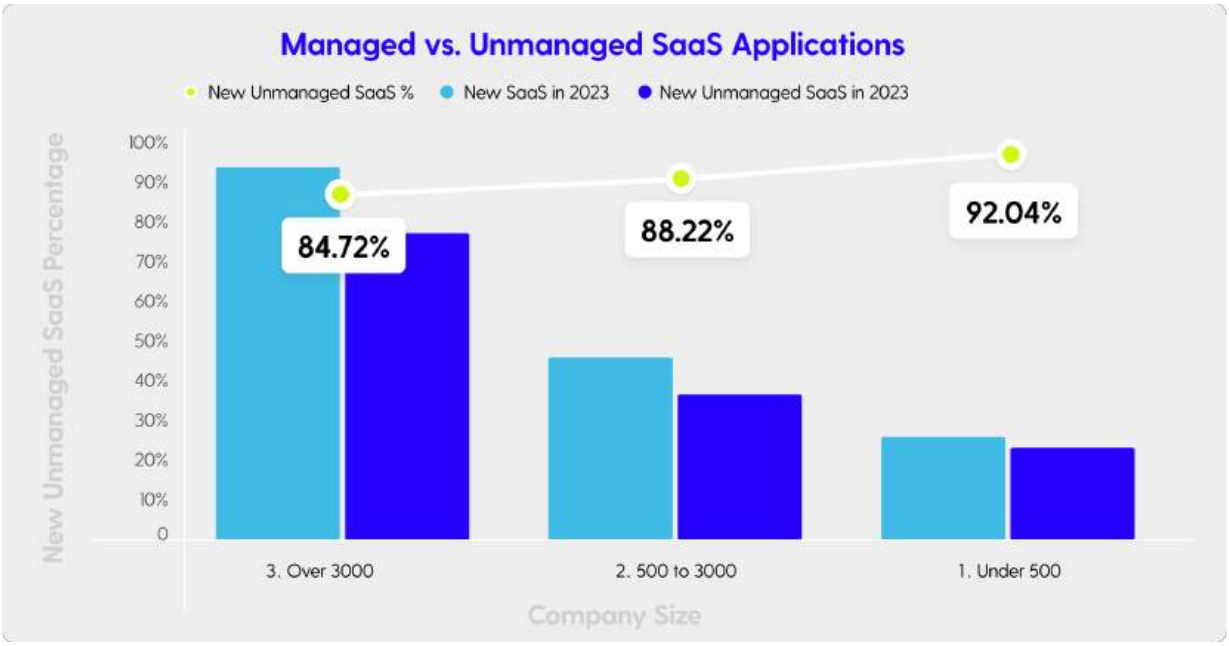
- Shadow SaaS and unapproved applications.
- Not monitored or governed by IT.
- Poses significant security and compliance risks.

Managed SaaS refers to applications known and governed by the organization. These applications use Single Sign-On (SSO) or Identity Providers (IdP) and are often termed "federated" SaaS.

- Known and governed by IT.
- Uses SSO or IdP for secure access.
- Actively monitored and managed for security and compliance.

Tolerated SaaS includes applications that are known and approved (sanctioned) but are deemed to represent low risk, so they are not actively managed.

- Known and approved by the organization, though the organization has opted not to take action.
- Considered low risk, hence not actively monitored.
- Sanctioned, but not centrally governed like managed SaaS.
- Can still pose risks as SaaS usage changes.

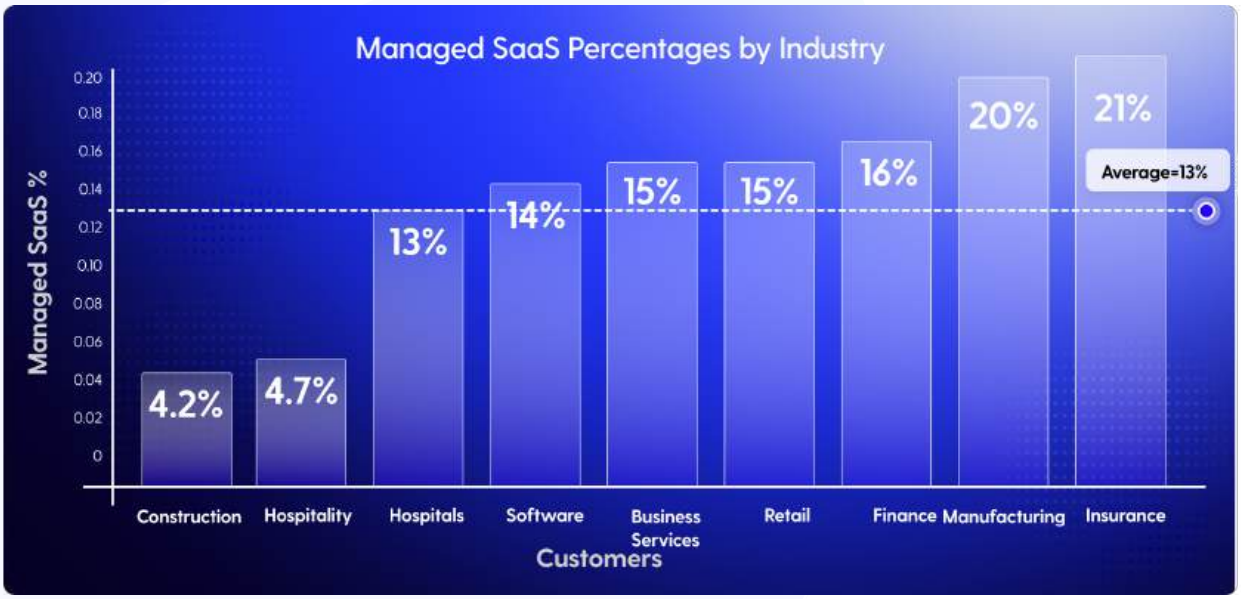


SaaS Risk Management Varies by Industry

Managed applications vary significantly across industries, reflecting their distinct operational needs, priorities, and SaaS adoption rates.

As an example, only 4.2% of SaaS applications in the construction industry are managed, suggesting a substantial gap in oversight and control. However, SaaS adoption is also lower than in other verticals, indicating that this industry may be less dependent on SaaS and, therefore, less concerned about managing it.

Conversely, a major SaaS adopter, such as the insurance industry, demonstrates a much higher level of SaaS management, with 21% of applications actively managed. This contrast highlights the varying maturity levels in SaaS governance across industries. Sectors subject to regulatory compliance standards prioritize SaaS security more rigorously than others.



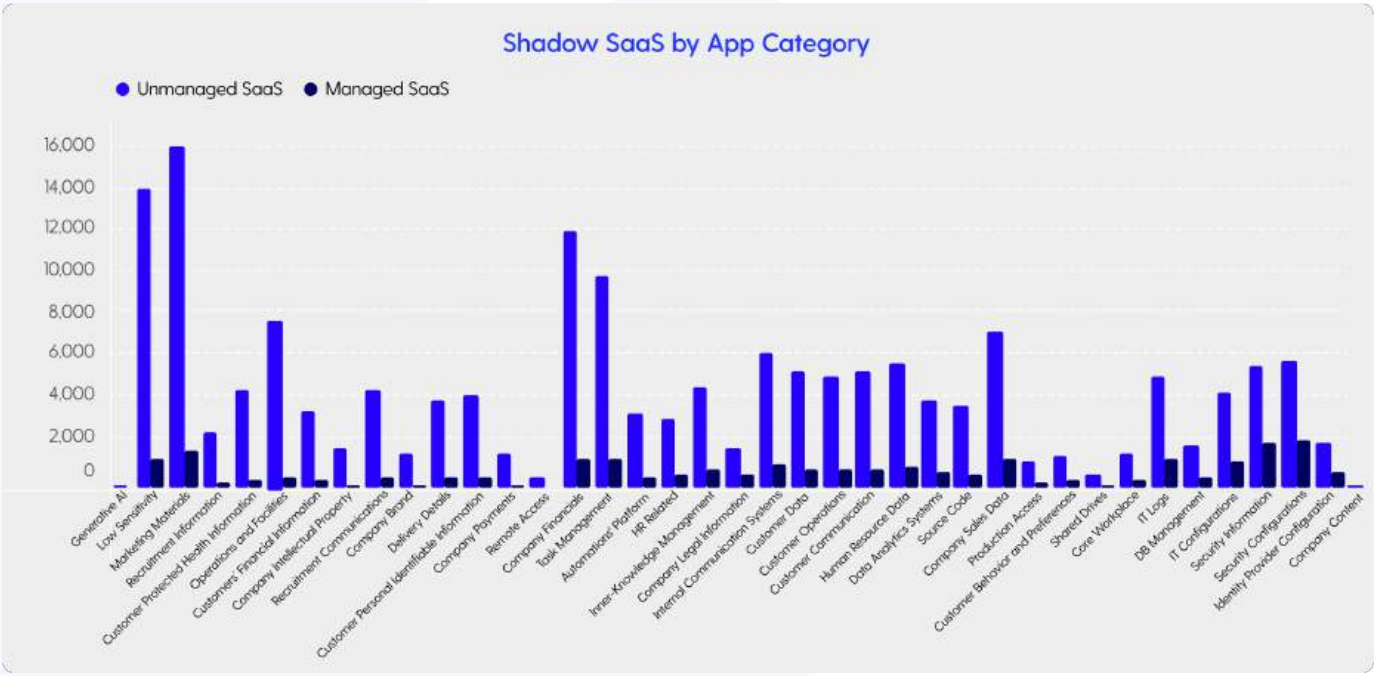
Some Apps are Better Managed Than Others

Analyzing SaaS applications by type vs. their management status reveals a distinct pattern. The data shows a slightly higher concentration of managed IT, production, and security apps, with management rates between 16% and 22%. In contrast, marketing apps, many of which are niche apps with few users, are among the lowest concentration of managed apps (5.8%) and a high volume of shadow SaaS (94.2%). Other sensitive applications, such as those containing financial data, are also managed significantly less often (7%), highlighting a critical oversight in SaaS risk management.

The data suggests that IT and security teams, which are usually part of the procurement process, are more apt to follow SaaS review protocols. However, they lack awareness of SaaS usage in other areas, likely from functional teams sidestepping the established procurement and security reviews. As a result, IT and security teams may not fully grasp the extent of shadow SaaS and the risks within their organization.

The 2024 MarTech Composability Survey found that 83% of marketers chose an alternative app even though the primary, sanctioned tool had the same functionality. The survey also found that SaaS app selection varied by individual preference, explaining the high amount of shadow SaaS in our findings.

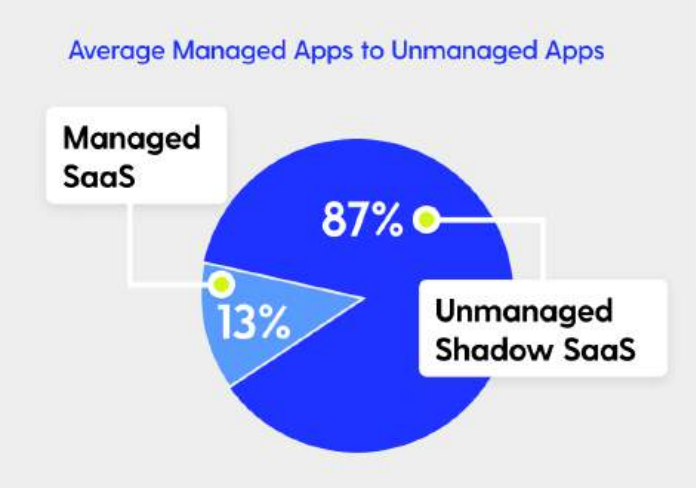
> **At our company, we want to secure the workforce, not block them. However, our SaaS risk landscape is often hidden as our business philosophy enables our users to have choices. The only way to manage SaaS security at scale is to focus on identity as the only available constant in every SaaS account.**
>
> **VP of Information Security**



The Prevalence of Shadow SaaS

Organizations often misjudge the volume of shadow SaaS that exists in their SaaS environment, leading to significant oversight in managing risks and maintaining security. These unapproved applications fly under the radar, bypassing traditional security protocols, undetected by identity management tools, and leaving critical data vulnerable. The lack of visibility into these tools means that organizations may not fully understand the scale of shadow SaaS within their environment, which can include hundreds or thousands of unmonitored apps.

As evidence, Okta's Businesses at Work 2024 report cites that, on average, organizations use 93 SaaS applications, all of which are managed. However, Grip's research uncovered an average of 835 SaaS applications, almost ten times more. The delta, 742 applications, represents unmanaged shadow SaaS, illustrating the vast gap in SaaS visibility.



> **Without clear visibility into what's being used, I can't fulfill my primary duty—securing the company.**
>
> **Director of IT and Security**

Shadow SaaS is Grossly Underestimated

Shadow SaaS is a more significant issue than most organizations realize. Shadow SaaS proliferates as employees and functional teams acquire tools outside of IT's visibility, now exceeding the known SaaS applications in an organization's SaaS ecosystem.

As an example, Grip uncovered nearly seven times more SaaS applications than a mid-size company's security team was aware of, along with active accounts belonging to former employees.
In addition to shadow SaaS, employees are also adopting other resources, such as IaaS tenants and AWS tenants independently; in an engagement with a Fortune 300 organization, the security team believed they had 35 AWS accounts. Grip uncovered ten times that amount, or 350 active tenants.

These examples illustrate how widespread shadow SaaS has become and the limited visibility security teams have.

The Shadow AI Boom: Rapid Growth and Unseen Risks

Generative Artificial Intelligence (GenAI) has taken the world by storm, starting with the ChatGPT craze and followed by a flurry of AI-powered features in other apps. GenAI is now mainstream, and users are indulging. Bloomberg predicts the AI market will skyrocket from $40 billion in 2022 to $1.3 trillion by 2032. However, as GenAI adoption soared, company policies lagged. The Conference Board reports that 57% of organizations lack an AI policy to guide their employees, highlighting a critical gap in GenAI app governance.

> **55% of employees use generative AI tools, and 84% admit to publicly exposing their company's data.**
>
> Oliver Wyman Forum

Accelerated Adoption: Tools and Users

The accelerated adoption of AI tools across industries is reshaping how businesses operate and compete. Grip's research highlights a steady and consistent rise in personal usage of AI apps over the last two years, with a slight upward trend in new users. This steady increase suggests that AI adoption is not just a spike of interest but a sustained and linear growth in active usage.

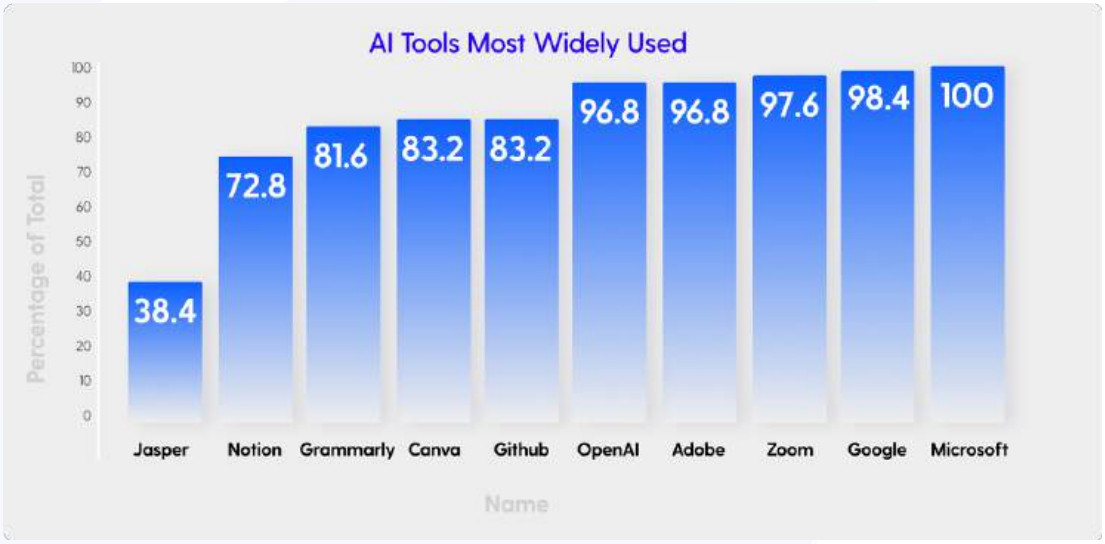
What's particularly noteworthy is that this trend pertains to actual usage, not just provisioned or granted access. This means that the focus is on active users who are engaging with and sharing data through AI tools, highlighting the practical integration of AI into daily workflows. As AI becomes more embedded into business operations, organizations need to be aware of the potential risks associated with widespread adoption. While AI offers numerous benefits, the rapid growth in its use and the challenges of managing AI-driven data present new security and governance concerns that cannot be overlooked.

This chart highlights the user growth of AI tools, excluding AI features within large SaaS applications like Microsoft, Adobe, Atlassian, and Google. In the 3rd quarter of 2022, coinciding with the launch of ChatGPT, there were only 1,876 users of AI tools. By the following quarter, that number had risen to 4,641; by the 1st quarter of 2024, the user count had surged to 44,440. This surge represents another significant challenge: many of the smaller, niche AI apps remain undetected and unmanaged by legacy security tools, further expanding an organization's attack surface.

The Most Widely Used AI Tools

Looking at all AI tools, the most widely used AI tools are embedded within corporate-sanctioned platforms, although they aren't explicitly recognized as "AI tools." Major players like Microsoft, Google, Zoom, and Adobe lead the pack, with the data showing that 97-100% of organizations analyzed have provisioned usage of these tools.

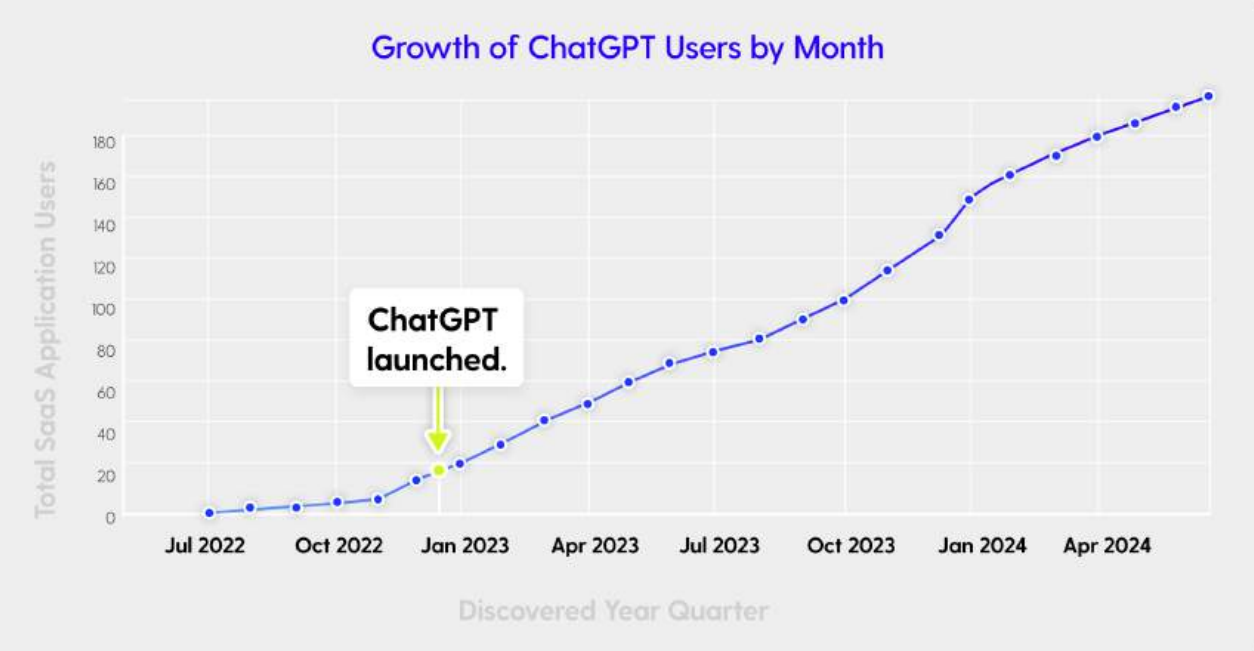
Other commonly provisioned AI tools include GitHub and Canva (83% each), Grammarly (82%), Notion (73%), and Jasper (39%).



ChatGPT

ChatGPT has been criticized for security concerns, including data privacy issues and potential data leaks, leading to a ban in several prominent public organizations and government agencies. However, it was still present in 96% of the organizations analyzed.

Here, we can see ChatGPT's user adoption trend since its launch in December 2022; ChatGPT usage has increased 24x in less than two years. Yet, despite its capability to be more tightly controlled, it is managed at a slightly lower rate (9%) than the average SaaS application (13%).



AI Apps are Hot but Remain in the Shadows

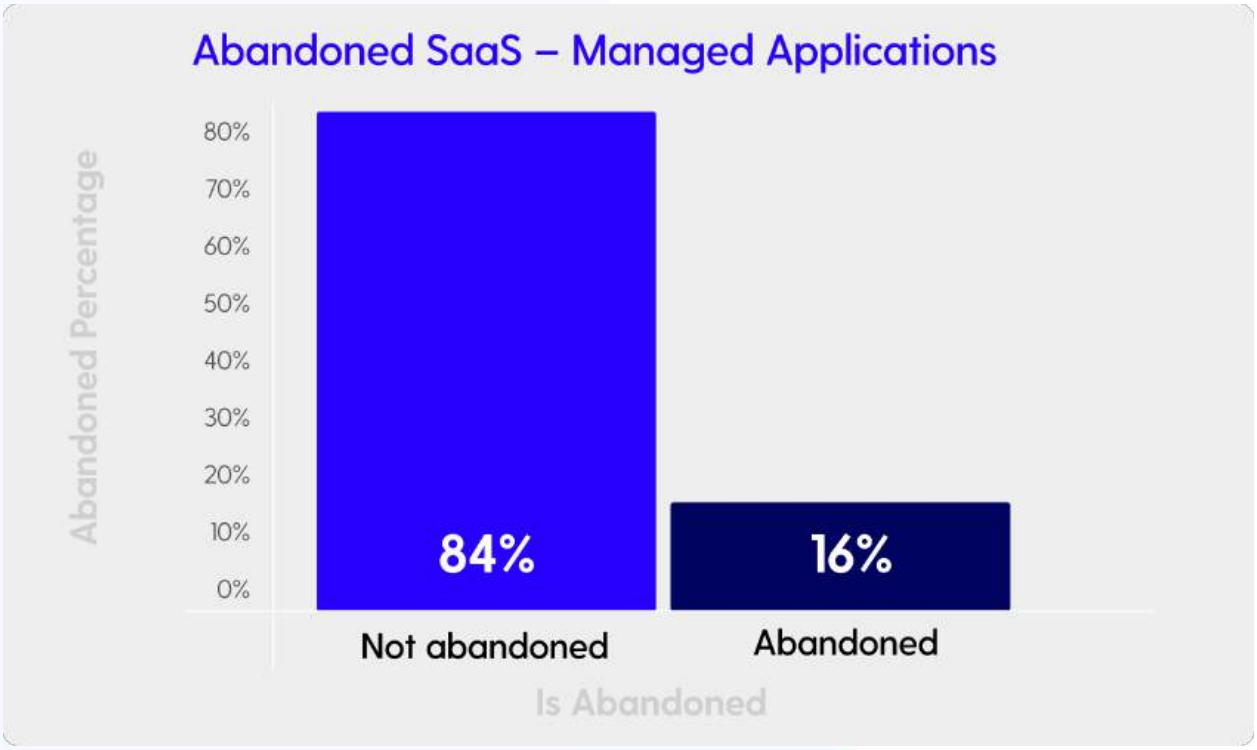
Grip's research also found that "major" or corporate SaaS applications with AI features, those with large user bases and subject to traditional procurement and security reviews (examples: Salesforce, Zoom, and Microsoft), are managed at a higher rate compared to the smaller, niche apps with fewer users, such as Canva and Grammarly.

Additionally, Grip data reveals that 42% of popular AI apps have SAML capabilities; however, 80% of AI apps that could be centrally managed and federated with the SAML protocol are not. The low management rate may stem from the security team's lack of visibility into which apps have AI capabilities or the app is low risk, so it is tolerated but not centrally managed.

The high percentage of AI applications that lack SAML support (58%) introduces significant security challenges, as identity management systems cannot govern or secure these apps. Many of the newer AI tools, particularly those not primarily focused on enterprise customers, haven't yet integrated this essential security feature. As a result, organizations allowing employees to use these AI apps for productivity gains risk expanding their attack surface and introducing blind spots into their identity security programs. Without proper governance, these tools become potential entry points for threat actors, making it critical for companies to weigh the benefits of AI apps against the security risks they pose.

Managed Apps Still Present Risks

High-profile breaches such as Microsoft Midnight Blizzard and Snowflake illustrate the dangers of forgotten and abandoned software accounts and dangling user access. Grip data revealed that 16% of managed applications were abandoned in 2023 yet remained connected to core systems.



Abandoned user accounts are likely resulting from two key trends. With workforce reductions surging in 2023, labor-intensive manual offboarding processes often couldn't keep up. The problem was further worsened by a lack of visibility into shadow IT, preventing security teams from revoking access to unknown accounts.

The other contributing factor to the high abandon rate is the easy access to apps, enabling employees to trial multiple apps and choose the one they prefer. Then, when a new option is introduced, they may again try the alternative and shift from one tool to another.

By failing to manage abandoned accounts and revoking dangling access, companies expose themselves to heightened security risks and undermine their financial health. Abandoned accounts, often left active after employees leave or roles change, can be exploited by cybercriminals to gain unauthorized access to sensitive data. The Microsoft breach, in which a forgotten test account was inadvertently left active, is a harsh reminder that no organization is immune to the risks posed by unmonitored accounts.

16% of managed apps were unused in 2023 yet remained connected to core systems.

Conclusion

As the SaaS landscape evolves, so must the security measures organizations use to protect their environments. Despite billions spent on addressing SaaS-related risks, the data shows that the problems haven't been solved.

The high volume of shadow SaaS underscores the primary issue: a lack of visibility into SaaS usage. Additionally, the prevalence of SAML-supporting apps without enabled security features highlights the challenge of prioritizing which applications pose the most significant risks and determining the right actions to mitigate them.

Traditional tools like CASBs have been relied upon but have proven ineffective because SaaS applications disrupt conventional network and endpoint monitoring models. Furthermore, the excessive data noise and false positives generated by these tools prevent teams from identifying and addressing the issues that genuinely demand their attention.

Organizations today are SaaS-reliant, and employees want the freedom and flexibility to choose their tools. According to analysts, business-led IT is one of the top drivers impacting information security, emphasizing the urgent need for organizations to adopt a more pragmatic approach to managing the risks of the new SaaS era.

Responsibility can no longer rest solely on IT and security teams; a collaborative effort involving the appropriate stakeholders, including business app owners and end users, is essential to effectively manage SaaS risks at scale.

Without a change in strategy, organizations will remain vulnerable to significant security breaches. High-profile incidents like those at Snowflake and Microsoft are stark reminders of the potential consequences of unmanaged SaaS environments, shadow SaaS, and dangling access. Enterprises that proactively adapt to changing SaaS trends will be better positioned to protect their sensitive data, ensure compliance with evolving regulations, optimize their financial resources, and enable innovation while mitigating the associated risks of a SaaS-driven business world.

Methodology

The SaaS Adoption and Security Risks Report provides an in-depth view of SaaS usage trends, security practices, and risk management across a wide range of industries and organization sizes. This report is based on anonymized customer data from Grip SaaS Security Control Plane (SSCP) deployments, encompassing over 29 million SaaS user accounts, 1.7 million identities, and 23,987 SaaS applications posing potential risks. Another 55,000 SaaS applications were identified but excluded from this report, as they were smaller apps with single users or internal websites, representing more noise than significance to our analysis. By leveraging this extensive and diverse dataset, Grip analysts uncovered key patterns from Q3 2022 – Q3 2024, revealing the current state and future direction of SaaS management and security, and providing insights previously unavailable to the industry.

About Grip Security

Grip Security is the industry leader in SaaS identity risk management, providing cutting-edge solutions to help enterprises navigate the security challenges of widespread SaaS and AI adoption.

Our platform enables companies to discover, prioritize, secure, and orchestrate SaaS risk mitigation. By leveraging identity as the central control point, we provide a comprehensive approach to securing all SaaS applications—including shadow SaaS and shadow AI—empowering organizations to adopt SaaS confidently and securely. Contact us to arrange a personal demo of the award-winning SaaS Security Control Plane.

Contact Us

info@grip.security

@GripSecurity

grip.security

SOC 2 Type II Certified

ISO 27001 Certified