



The Essential Guide to Identity-First SaaS Security

Introduction

SaaS has revolutionized business operations, enhanced efficiency, and driven rapid growth, but it also introduces significant security challenges in visibility, identity, and risk management. As SaaS environments expand, tracking and managing solutions becomes tougher, requiring organizations to enhance visibility and control to mitigate risks.

This eBook explores the market trends of increased SaaS app adoption and the challenges of Shadow IT, SaaS sprawl, and identity blind spots. It examines how organizations often lack visibility into all their apps, leading to security risks. You'll learn about the limitations of traditional security tools and how innovative solutions like Savvy offer comprehensive visibility and support organizations by augmenting their existing IAM solutions.

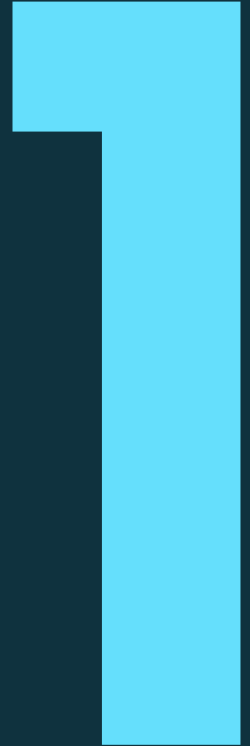




Chapter 1

The SaaS Explosion

Riding the Wave of Modern Apps



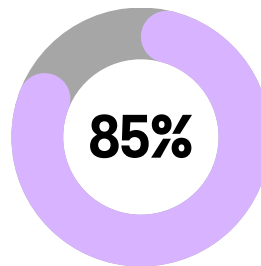
SaaS app adoption has seen unprecedented growth in recent years. According to the [Annual SaaS Security Survey Report of 2024](#) from the Cloud Security Alliance, over 85% of organizations now use SaaS apps for various business functions. This trend is driven by the need for flexibility, scalability, and cost-efficiency that SaaS solutions offer, helping businesses innovate and grow without significant infrastructure investments. However, this widespread adoption and growth is challenging to oversee, leaving organizations with gaps when managing and securing these apps.



The average organization uses over

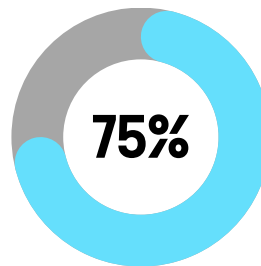
1,000 SaaS apps

Statistics and Trends in SaaS Usage You Should Know



of organizations use SaaS apps.

CSA Annual SaaS Security Survey Report (2024)



of organizations have experienced shadow IT incidents.

Cloud Security Alliance Survey (2023)

Shadow IT and SaaS sprawl

A major challenge to visibility in SaaS apps is the addition of IT systems without the IT department's approval. Teams often purchase their own SaaS solutions to meet business needs, bypassing IT approval. This creates unmanaged shadow IT infrastructure, significantly affecting organizations. Unauthorized SaaS apps can lead to security risks like data breaches and compliance violations.

This proliferation of SaaS apps creates a challenging-to-manage sprawl. Gartner reports that organizations use over 1,000 different SaaS apps on average, many unknown to IT. This complicates app management and security, making consistent security policy enforcement difficult.





Chapter 2

Visibility and Identity Challenges

2

The Impact of Insufficient Visibility

Lack of visibility into all SaaS apps used within an organization poses significant risks. Without a comprehensive inventory, IT and security teams are blind to potential risk and compliance issues. This lack of visibility can lead to unmonitored data flows, unsecured endpoints, and increased cyberattack opportunities.

Consequences for IT and Security Teams

For IT and security teams, the lack of visibility means an inability to enforce security policies uniformly. This results in inconsistent security practices across the organization, with some apps having proper security measures in place while others are left vulnerable. Additionally, the inability to monitor all apps hampers incident response efforts as security teams may be unaware of all potential entry points for attackers.



“Organizations with poor visibility into their SaaS environments are 30% more likely to experience a data breach, driving a critical need for effective tools and strategies to gain complete visibility.”

CSA Annual SaaS Security Survey Report (2024)

Security Incidents Due to Lack of Visibility



Panera Bread Hack

In 2018, Panera Bread's website had a vulnerability that exposed the personal information of millions of customers. A security researcher initially reported the issue, but Panera Bread failed to address it promptly. The problem was partly due to shadow IT practices, where employees used unauthorized tools and processes to manage the website, leading to poor security practices and exposure of sensitive data.

[Unpacking the Panera Bread Attack - Medium](#)




Anthem Security Breach

The health insurance giant Anthem experienced a massive data breach in 2015 affecting 78.8 million people. The breach was partly attributed to shadow IT practices, where employees were using unsanctioned devices and applications that were not properly secured, making it easier for attackers to infiltrate the network.

[Anthem Hacking Points - The New York Times](#)

Identity Blind Spots in Your IAM Framework

Single Sign-On (SSO) is a powerful tool for managing user identities and ensuring secure app access. It allows SaaS apps to leverage centralized authentication, simplifying management efforts and reducing the risks when users leave the organization. However, many SaaS apps are not formally onboarded through SSO, creating significant identity blind spots where organizations cannot see who has access to an app. These non-onboarded apps also come with additional risks where they may allow users to bypass SSO using a native SaaS account. This leads to fragmented identity management and increased security risks.

A large, stylized purple graphic of the number '68%' is centered in the upper half of a light yellow rounded rectangle. The font is bold and modern.

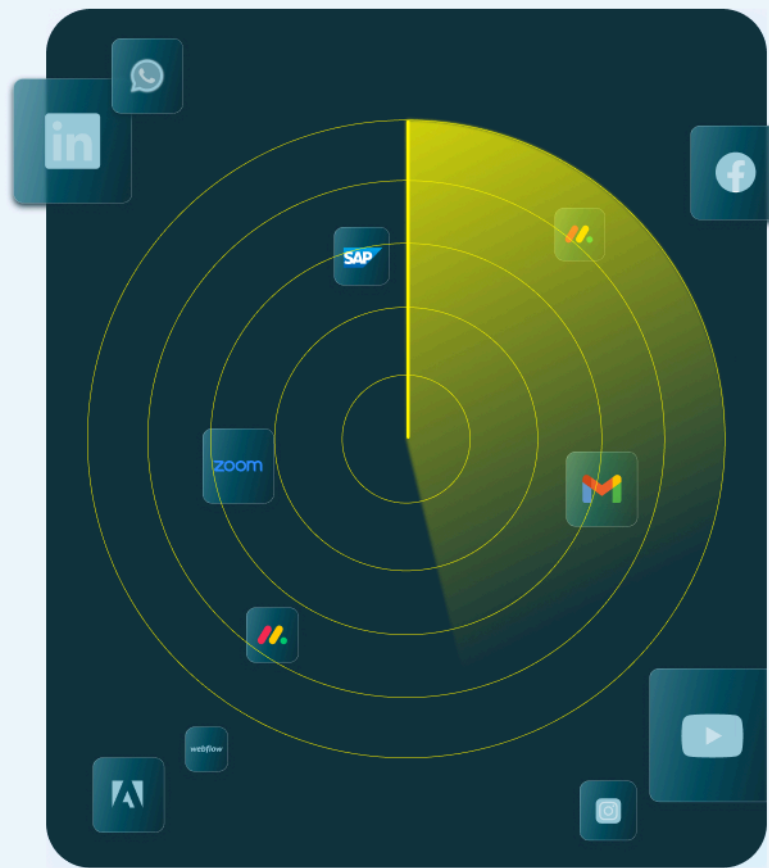
of organizations report that a significant portion of their SaaS apps are accessed directly without going through the corporate SSO.

Cloud Security Alliance Survey (2023)

Bypasses such as this undermine the benefits of SSO's security controls and policies, making enforcing consistent identity management practices difficult.

Another identity blind spot that's often overlooked comes from SSO Bypass. These are logins that use a direct login form with the app, despite the availability of an SSO login method. Since there are some valid uses of direct logins (e.g., break glass accounts), business context is key to determining if the activity is valid. And since SaaS apps are implemented in a multitude of ways, it's difficult to be sure if direct login access is disabled when SSO has been enabled.

Additionally, the detection of shared accounts poses a significant challenge. When multiple users share the same login credentials, it complicates tracking user activity and enforcing accountability. Shared accounts are a common workaround for role-based access limitations or licensing restrictions, but they significantly undermine security and compliance efforts.



Risks from Weak and Leaked Credentials

When SaaS apps are not onboarded through SSO, users often resort to using weak passwords or reusing credentials across multiple platforms. This practice significantly increases the risk of credential theft.

Weak and leaked credentials are a major security concern as they provide an easy entry point for attackers. IT teams are often unaware of these vulnerabilities without a tool that provides proper visibility into these apps until a breach occurs.

55%

of organizations have experienced incidents where employees used passwords that were previously leaked on the dark web.”

CSA Annual SaaS Security Survey Report (2024)

Prevalence of Personal Credentials

A troubling trend is the use of personal credentials to access professional SaaS apps. This practice blurs the line between personal and corporate data, making it difficult to secure sensitive information.

This lack of separation exposes corporate data to risks associated with personal account breaches. It complicates the management of user access and offboarding processes. Ensuring that all apps are onboarded through corporate SSO and that employees adhere to strong password policies is critical for mitigating these risks. But how can organizations enforce these policies without clear visibility into the risks?

42%

of employees admitted to using personal email addresses and passwords for work-related apps.

Statista Technology Report (2020)



Chapter 3

Improving Identity Hygiene

3

Security Incidents Due to Poor Hygiene



Change Healthcare Breach

In 2023, threat actors compromised credentials for a SaaS app with no MFA enabled on the account. The absence of multi-factor authentication allegedly exposed other remote access apps, making them vulnerable to credential stuffing attacks. Cybercriminals loitered on the US health provider's systems for nine days before stealing data and launching a ransomware attack that impacted operations and had far-reaching effects across the industry.
[Healthcaredrive.com](https://healthcaredrive.com) - [Change Healthcare Breach](#)



Okta Hack

The Okta hack in 2023 occurred when an employee stored their login credentials in their private Google profile on the Chrome browser and later logged in on a company endpoint, exposing the credentials. This security breach resulted in the theft of data from multiple Okta customers.
[Thehackernews.com](https://thehackernews.com) - [Okta Driven Credential Stuffing Attacks](#)



Microsoft-Russian Hack

In 2023, Microsoft discovered a nation-state attack attributed to the same Russian hackers behind the SolarWinds attack (Midnight Blizzard). The threat actors accessed the email accounts of senior leadership, possibly for weeks. The breach began with a password spraying attack on a non-production test account lacking two-factor authentication.
[Nbcnews.com](https://nbcnews.com) - [Russian hackers spied on executive emails](#)

Gaining hygiene visibility

Addressing authentication challenges requires more than stronger passwords. Modern attacks often leverage stolen passwords from phishing, info-stealing malware, and previous breaches. Multi-factor authentication (MFA) adds a crucial layer of security, making it harder for attackers to use stolen credentials. However, many SaaS apps don't enforce MFA, leaving them vulnerable to trivial attacks.

Proper identity hygiene also goes beyond MFA. It involves best practices for password management, regular credential updates, and monitoring for suspicious activity. Without these measures, organizations risk identity-related breaches.

IT teams need tools for visibility into SaaS app usage to enforce identity hygiene effectively. They must quickly to identify apps lacking MFA, misconfigurations, and password reuse across platforms. Without this visibility, blind spots emerge that attackers can easily exploit.

Only 57%

of organizations have implemented MFA for all their SaaS apps.

CSA Annual SaaS Security Survey Report (2024)

Enforcing hygiene standards

Addressing authentication challenges requires more than stronger passwords. Modern attacks often leverage stolen passwords from phishing, info-stealing malware, and previous breaches. Multi-factor authentication (MFA) adds a crucial layer of security, making it harder for attackers to use stolen credentials. However, many SaaS apps don't enforce MFA, leaving them vulnerable to trivial attacks.

Proper identity hygiene also goes beyond MFA. It involves best practices for password management, regular credential updates, and monitoring for suspicious activity. Without these measures, organizations risk identity-related breaches.

IT teams need tools for visibility into SaaS app usage to enforce identity hygiene effectively. They must quickly identify apps lacking MFA, misconfigurations, and users reusing passwords across platforms. Without this visibility, blind spots emerge that attackers can exploit.

Misconfigured MFA

appeared in two of the biggest attack campaigns so far in 2024: a ransomware attack against Change Healthcare and dozens of attacks against Snowflake customers.

Cybersecurity Dive (2024)



Chapter 4

Limitations of SSPM and CASB

4

Limitations of SSPM and CASB

SaaS Security Posture Management (SSPM) and Cloud Access Security Broker (CASB) tools are commonly used to manage and secure SaaS apps. However, these tools often come with high costs and complexities, making them difficult to implement and maintain. **According to Gartner, organizations spend 20% of their IT security budget on SSPM and CASB tools. Yet, many still struggle with visibility and control of their identities, and organizations continue to deal with security breaches.**

The complexity of these tools can also be a barrier. IT teams need specialized skills to configure and manage SSPM and CASB solutions effectively. This complexity can lead to gaps in coverage and missed opportunities to identify and mitigate risks.

Organizations spend 20% of their IT security budget on SSPM and CASB tools. Yet, many still struggle with visibility and control of their identities, and organizations continue to deal with security breaches.

CSA Annual SaaS Security Survey Report (2024)

Gaps in Visibility and Effectiveness

Despite their capabilities, SSPM and CASB tools often fail to provide complete visibility into all SaaS apps used within an organization. **The Annual SaaS Security Survey Report of 2024 found that 54% of organizations using SSPM and CASB tools reported gaps in their visibility.** These gaps can leave critical apps unmanaged and unmonitored, exposing the organization to potential security risks.

Additionally, these tools may not effectively address the dynamic nature of SaaS environments. New apps and services are continually being adopted, and traditional tools can struggle to keep up with this pace of change. This can result in outdated security policies and configurations that do not reflect the current state of the SaaS environment.

54%

of organizations using SSPM and CASB tools reported gaps in their visibility.

CSA Annual SaaS Security Survey Report (2024)



Chapter 5

Augmenting Existing IAM Tools

5

Augmenting Existing IAM Tools

Savvy augments existing IAM tools to eliminate identity blind spots by providing comprehensive identity-first SaaS security. The solution uses advanced discovery techniques to identify all SaaS apps within an organization, including those not formally onboarded. This comprehensive discovery process provides IT teams a complete inventory of all apps, reducing the risk of shadow IT and SaaS sprawl.

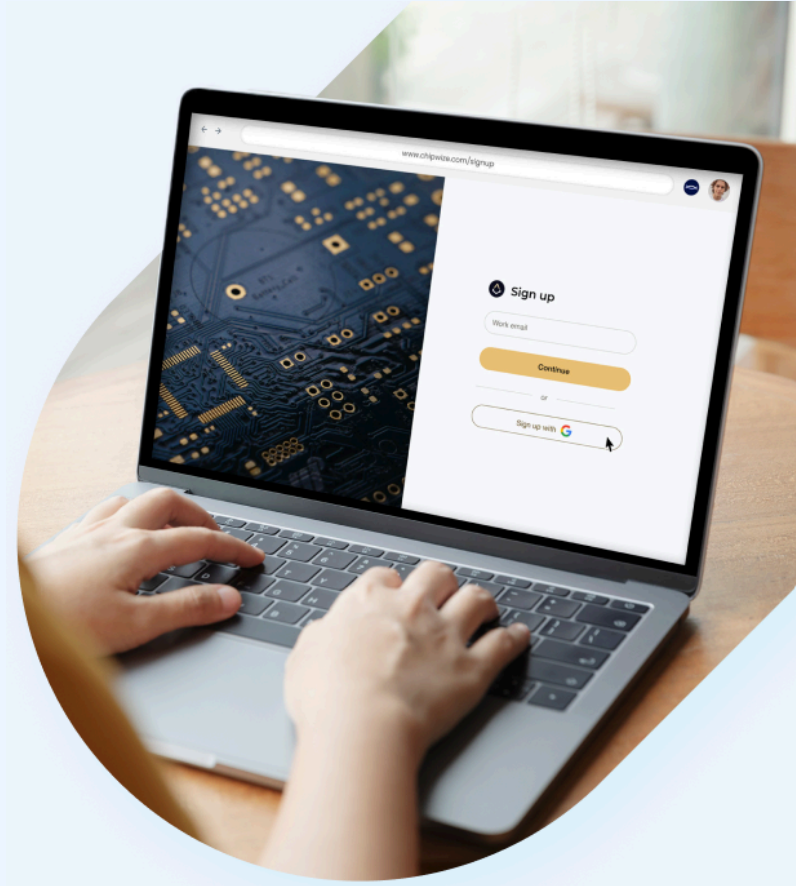
Real-Time Inventory

Creating a real-time inventory of SaaS apps is critical for maintaining security and compliance. Savvy provides this capability by continuously monitoring the SaaS environment and updating the inventory in real time. This real-time visibility allows IT teams to quickly identify and address security risks, such as apps lacking MFA or using weak credentials.



Uncovering Identity Hygiene Risks

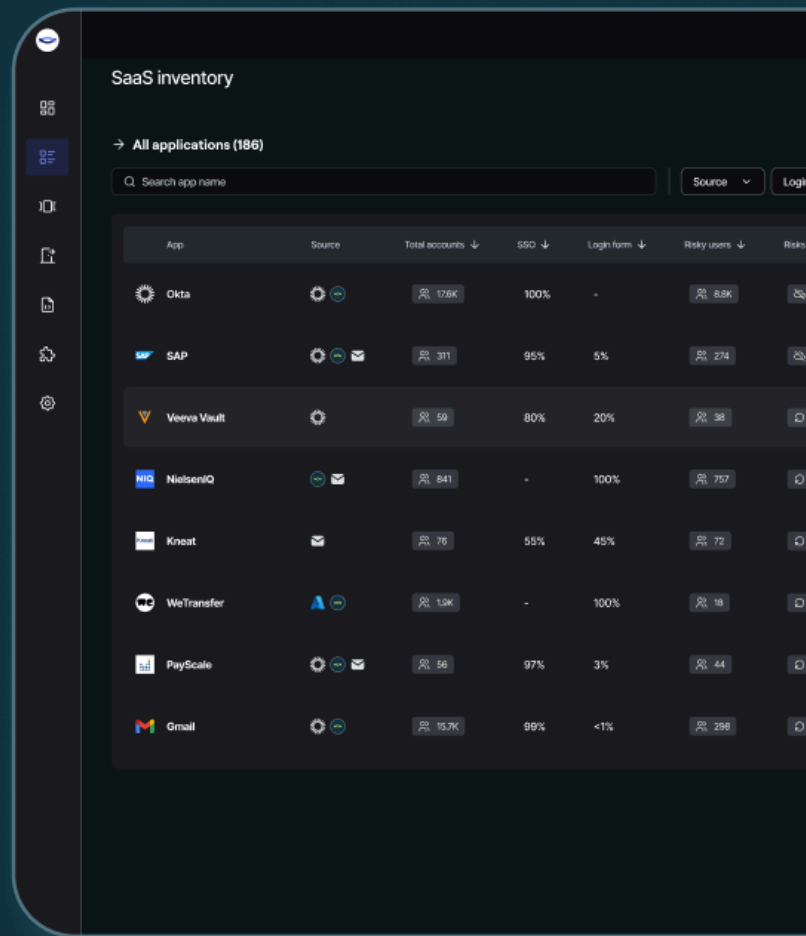
Savvy's advanced analytics can identify apps and users that do not adhere to best practices for identity hygiene. For example, Savvy can detect which apps lack MFA, use weak passwords, or have credentials leaked on the dark web. This information enables IT teams to take proactive measures to mitigate these risks.



Reducing SSO Bypass

One of the key benefits of using Savvy is its ability to reduce SSO bypass and direct logins. Savvy continuously monitors and detects when a user logs in directly to a SaaS app instead of logging in through your organization's SSO. By monitoring direct logins, Savvy ensures that all user activity is authenticated and authorized through your organization's secure SSO system. This reduces the risk of unauthorized access and potential data breaches, as SSO typically enforces more robust authentication mechanisms such as multi-factor authentication (MFA).

Additionally, it helps maintain compliance with security policies. It provides a centralized log for all access events, which is crucial for auditing and incident response.



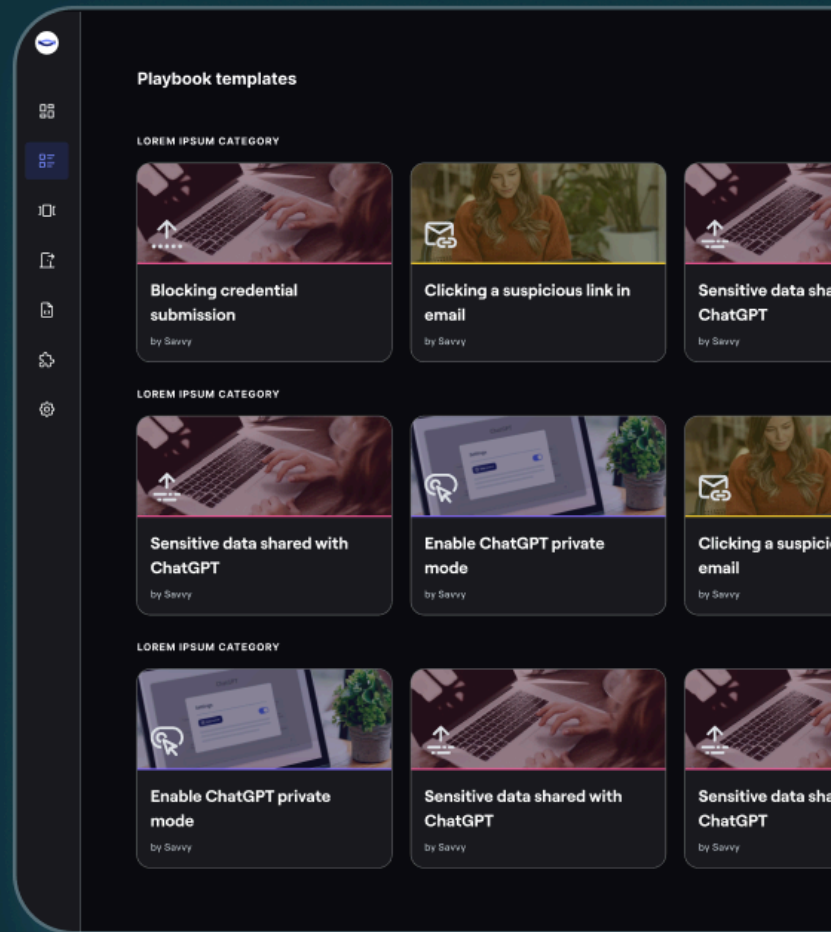
The screenshot displays the 'SaaS inventory' section of the Savvy application. It features a sidebar with navigation icons and a main content area with a search bar and a table of applications. The table columns include App, Source, Total accounts, SSO, Login form, Risky users, and Risk score. The data is as follows:

App	Source	Total accounts ↓	SSO ↓	Login form ↓	Risky users ↓	Risk score
Okta		176K	100%	-	8.8K	
SAP		311	95%	5%	274	
Veeva Vault		59	80%	20%	38	
NielsenIQ		841	-	100%	757	
Kneat		76	55%	45%	72	
WeTransfer		1.9K	-	100%	18	
PayScale		56	97%	3%	44	
Gmail		15.7K	99%	<1%	258	

Automation Playbooks

Savvy enables IT teams to prioritize security by highlighting the most significant risks. The platform provides detailed insights into each app's security posture, allowing IT teams to focus on high-risk areas first. Additionally, Savvy supports the creation of security automation playbooks, which can automatically gather context from end users and respond to identified risks.

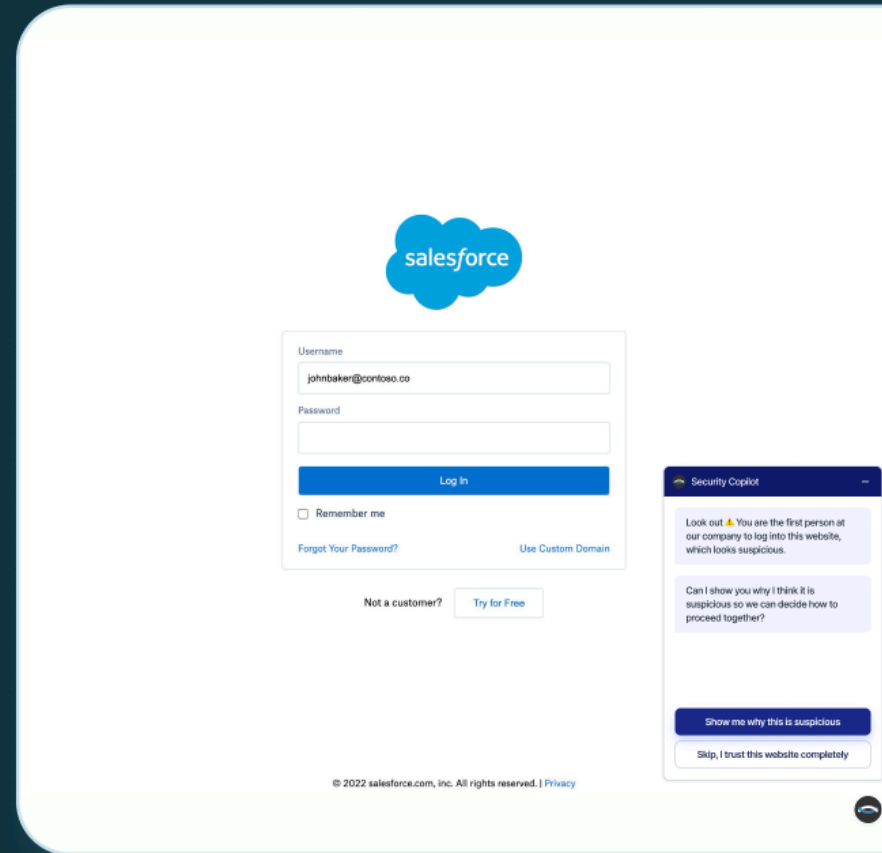
For example, suppose Savvy detects an app without MFA. In that case, it can trigger an automation playbook that alerts the responsible user and provides guidance on enabling MFA. This proactive strategy contributes to upholding a strong security standard throughout the organization while streamlining security processes to reduce IT's workload.



Just-In-Time Security Guardrails

Just-in-time security alerts are crucial for guiding users towards proper security hygiene. These alerts provide real-time feedback and recommendations, helping users make informed decisions about their security practices. Savvy's just-in-time security alerts cover a wide range of scenarios, from enabling MFA to recognizing phishing attempts.

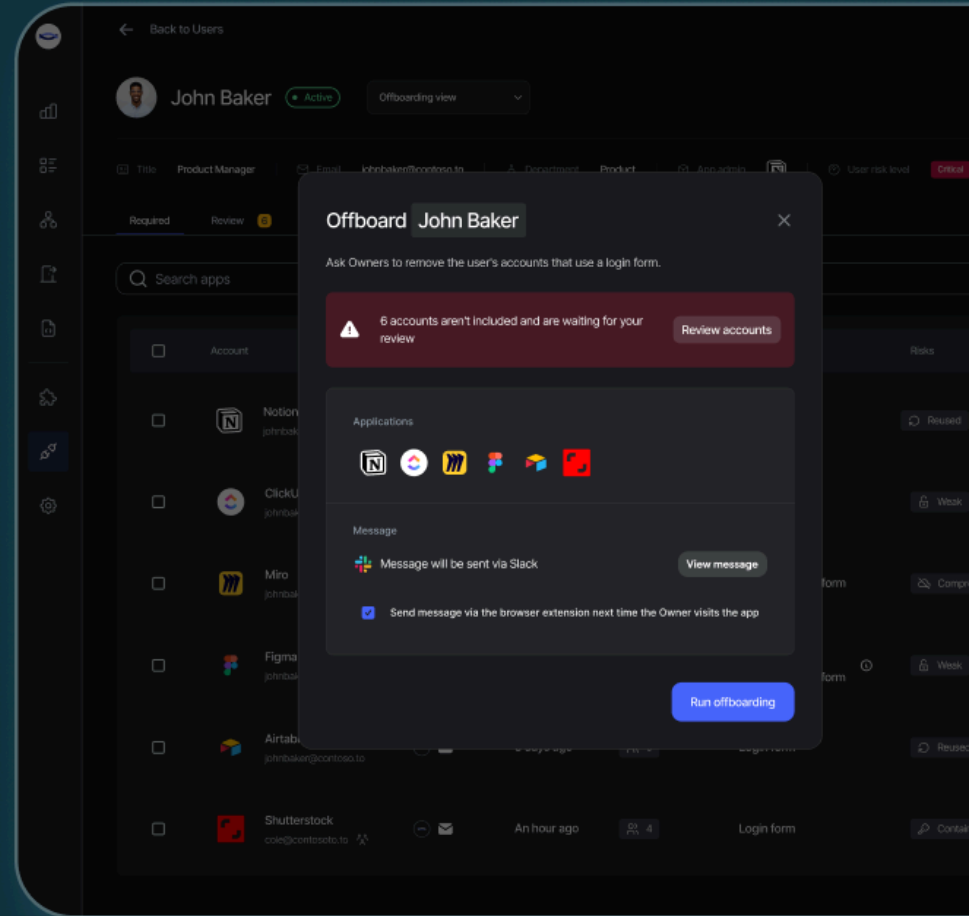
For example, if a user attempts to access an app without MFA, Savvy will alert them and provide step-by-step instructions on enabling MFA. This approach empowers users to take responsibility for their security practices and reduces the burden on IT teams.



Offboarding Capabilities

Savvy's just-in-time security alerts also include guidance on offboarding capabilities. When employees or contractors leave the organization, Savvy ensures that all their access to SaaS apps is properly revoked. This automated offboarding process helps secure sensitive data and reduces the risk of unauthorized access.

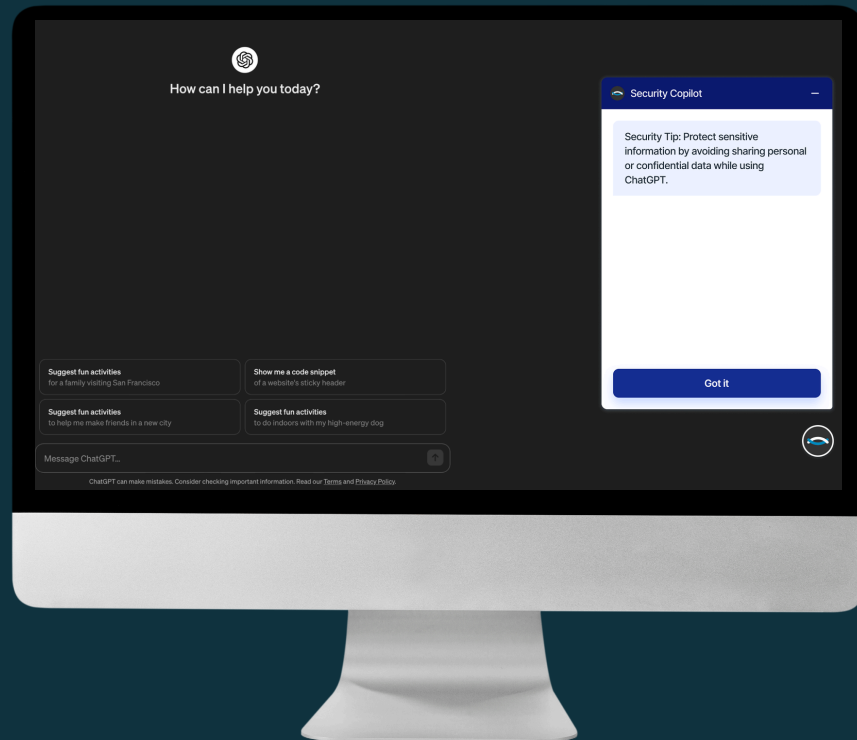
Leveraging automation to handle the offboarding process can reduce the risk of human error and ensure that access rights are promptly removed.



Responsible AI Usage

Savvy enables a proactive and empowering approach to address the challenges of Shadow AI. Instead of hindering your team's innovative spirit, we provide just-in-time guardrails and alerts that guide them in making responsible security decisions regarding AI usage.

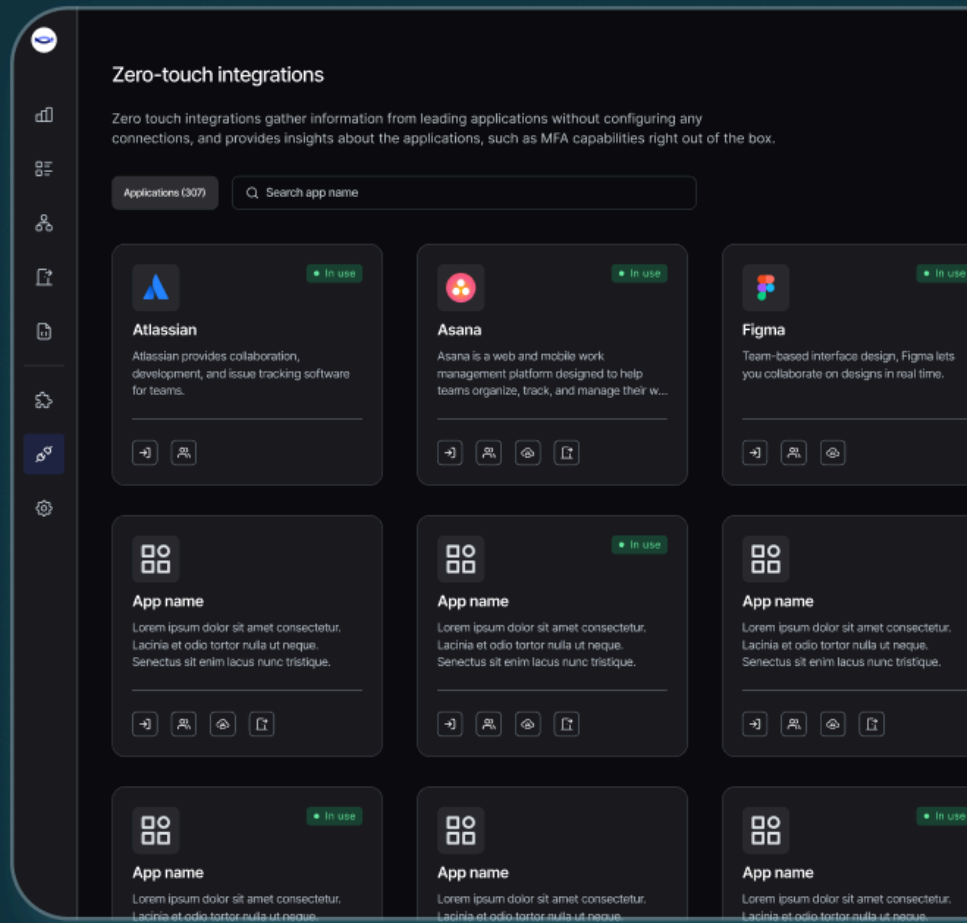
Our guidelines ensure that generative AI tools are used responsibly within the organization, preventing inadvertent exposure of sensitive data. By embracing Savvy's proactive security approach, you strengthen your organization's data protection framework while enabling your employees to maximize AI's transformative potential.



Effortless App and Identity Visibility

Imagine instantly detecting a new app's adoption, identifying the admin, inventorying all accounts associated with the app, and validating the accounts' security posture without lifting a finger. That's the magic of Savvy Zero-Touch Integrations (ZTIs).

Behind the scenes, ZTIs are a capability of the Savvy browser extension. They leverage already established sessions on the client side to interrogate the app, revealing its security posture. This information is then relayed via the browser extension back to the Savvy platform, where it is used to enrich and update Savvy's continuous and real-time inventory of SaaS apps, identities, and risks.



Savvy Identity-First Security for SaaS

Experience the benefits of Savvy's innovative solutions firsthand with interactive demos on our website. Then, schedule a live demo today to see how Savvy can help fortify your SaaS environment, ensuring robust protection and peace of mind in an increasingly complex cyber landscape.

<https://savvy.security/>

