

Savvy:

A Comprehensive Solution
for Shadow IT Governance
and Identity Security



Carlos E. Rivera

Principal Advisory Director
Info-Tech Research Group

Savvy is an identity-first SaaS security vendor that has rapidly gained traction in the market. While the company is relatively young, its founders and core team bring decades of experience from leading identity and access management (IAM) providers such as Ping Identity, Okta, and SailPoint. This deep understanding of the IAM landscape is evident in Savvy's approach to addressing the pervasive challenges of shadow IT governance and identity security. With a growing member network of over 50,000 individuals and organizations, Savvy has established itself as a trusted advisor and provider of innovative solutions in the SaaS-identity security space.

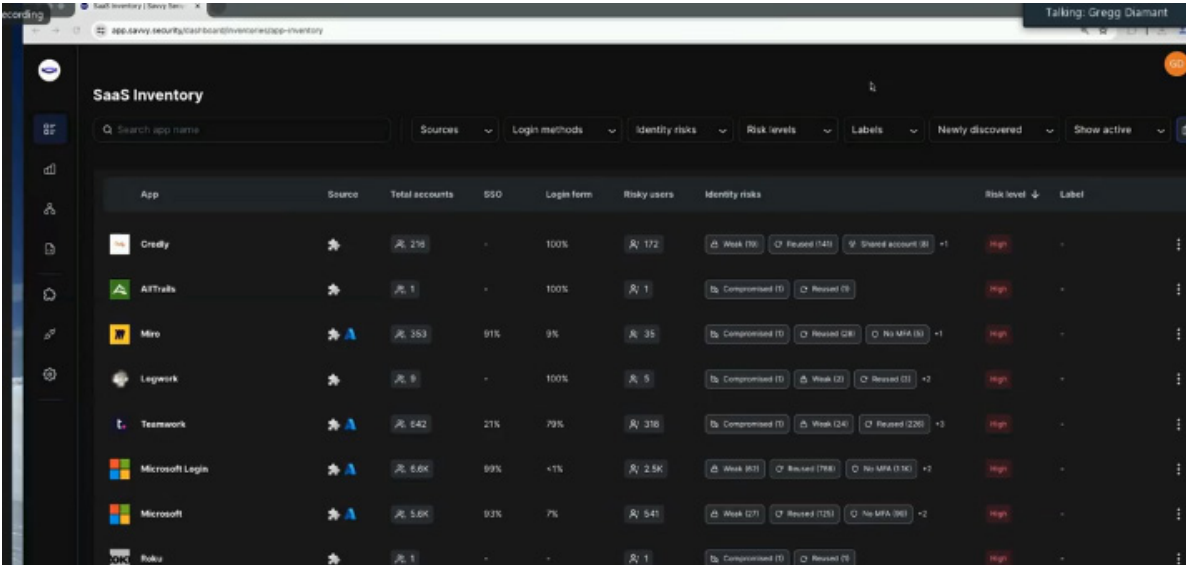


Source: Savvy, Analyst Briefing Deck (07/2024)

Standard Features: Visibility and Risk Assessment

Savvy's platform offers a comprehensive suite of features designed to provide organizations with deep visibility into their SaaS landscape and the associated identity risks. The platform leverages multiple data telemetry sources, including identity provider (IdP) APIs, email APIs (including cloud workspaces), SaaS APIs, and a browser extension, to capture and analyze user behavior across both managed and unmanaged applications. This approach enables Savvy to identify shadow IT applications, track user login events, and detect risky identity hygiene practices such

as weak or compromised passwords, shared accounts, and password reuse. The browser extension plays a crucial role in collecting granular ground truth on user interactions within applications, while the IdP, SaaS, and email APIs provide additional context and validation. The combination of telemetry sources allows the Savvy platform to detect SSO bypass, misconfigured MFA, and rogue admin accounts.



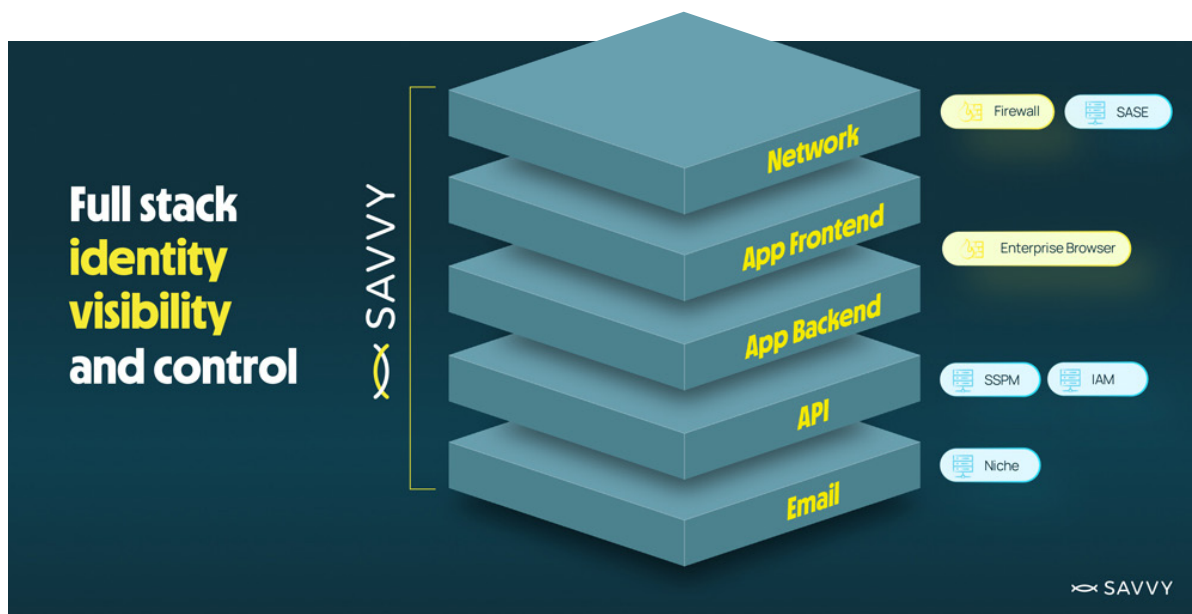
The screenshot shows the 'SaaS Inventory' dashboard with a table listing various applications and their associated security risks. The table includes columns for App, Source, Total accounts, SSO, Login form, Risky users, Identify risks, Risk level, and Label. The applications listed are Credly, AITracks, Miro, Logwork, Teamwork, Microsoft Login, Microsoft, and Roku.

App	Source	Total accounts	SSO	Login form	Risky users	Identify risks	Risk level	Label
Credly		218	-	100%	172	Weak (16), Reused (143), Shared account (6)	+1	High
AITracks		1	-	100%	1	Compromised (1), Reused (0)		High
Miro		353	91%	9%	35	Compromised (1), Reused (28), No MFA (3)	+1	High
Logwork		9	-	100%	9	Compromised (1), Weak (3), Reused (5)	+2	High
Teamwork		542	21%	79%	316	Compromised (1), Weak (24), Reused (226)	+3	High
Microsoft Login		6.6K	99%	<1%	2.5K	Weak (61), Reused (718), No MFA (134)	+2	High
Microsoft		5.6K	93%	7%	541	Weak (27), Reused (125), No MFA (36)	+2	High
Roku		1	-	-	1	Compromised (1), Reused (0)		High

Source: Savvy, Analyst Demo (07/2024)

Differentiation: Privacy, Customization, and Automation

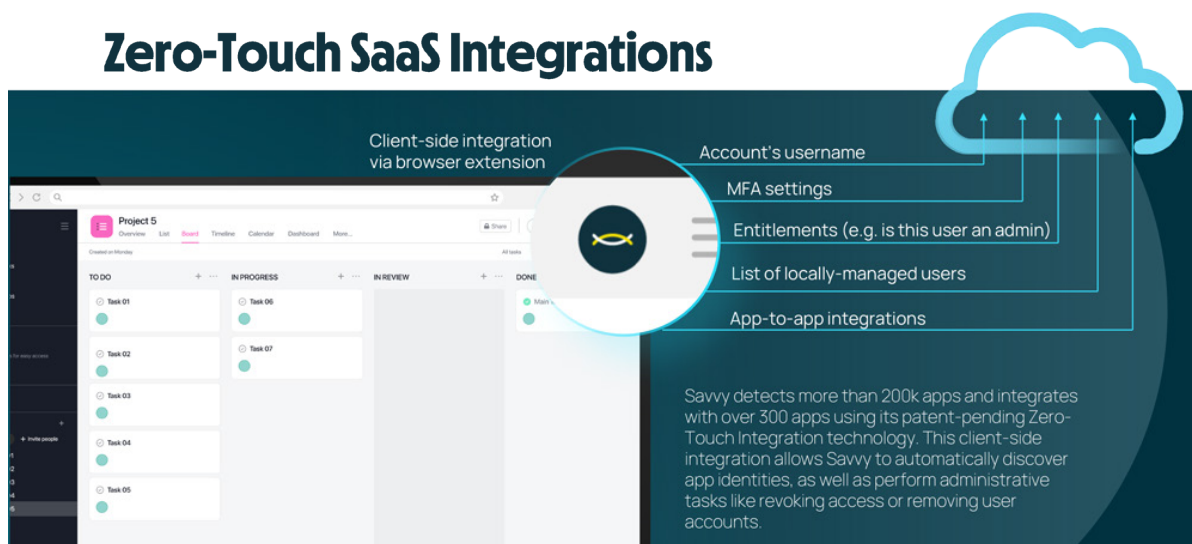
Savvy differentiates itself from other SaaS security vendors through its commitment to privacy, customizable playbooks, and automation capabilities. The platform prioritizes data privacy by never sending or storing clear-text credentials and encrypting all other sensitive information in transit and at rest, ensuring advanced techniques are used to ensure their standards comply with the most stringent regulations. Additionally, Savvy's browser extension performs most of the data processing locally, minimizing the amount of sensitive data transmitted to the cloud. This approach ensures that organizations can leverage Savvy's insights without compromising user privacy.



Source: Savvy, Analyst Briefing Deck (07/2024)

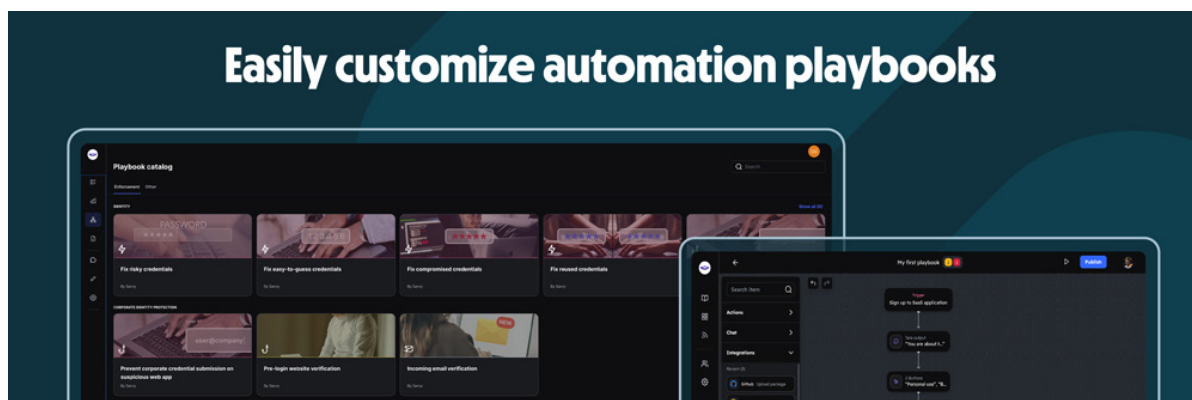
Savvy Security's new zero-touch integrations (ZTIs) revolutionize SaaS app management by eliminating the need for manual server-side configuration. This patent-pending approach leverages existing client-side sessions, enabling seamless integration and configuration of all SaaS apps, both sanctioned and unsanctioned. This not only saves time and resources for security teams but also significantly improves visibility and reduces SaaS identity risks. Key benefits include discovering identity security gaps, controlling SaaS sprawl and shadow IT, gaining visibility into app-to-app connections, supporting accelerated adoption, and managing apps at enterprise scale.

Zero-Touch SaaS Integrations



Source: Savvy, Analyst Briefing Deck (07/2024)

Savvy's customizable playbooks empower organizations to tailor their security responses based on their unique risk profiles and business contexts. The platform provides a drag-and-drop interface for easily creating and modifying playbooks, allowing organizations to define specific actions to be taken in response to different types of security events. A key aspect of Savvy's automation capabilities includes just-in-time security guardrails. These playbooks power the guardrails to interact in real-time with the user at the moment of decision, a differentiating capability that is lacking from other competitors. The automation playbooks can also perform actions similar to a SOAR platform, communicating in near real-time with other systems through APIs and interacting with admins and users through Slack/Teams and email. This flexibility ensures that Savvy can adapt to the evolving needs of each organization.



Source: Savvy, Analyst Briefing Deck (07/2024)

Product Insights: Addressing the Offboarding Challenge

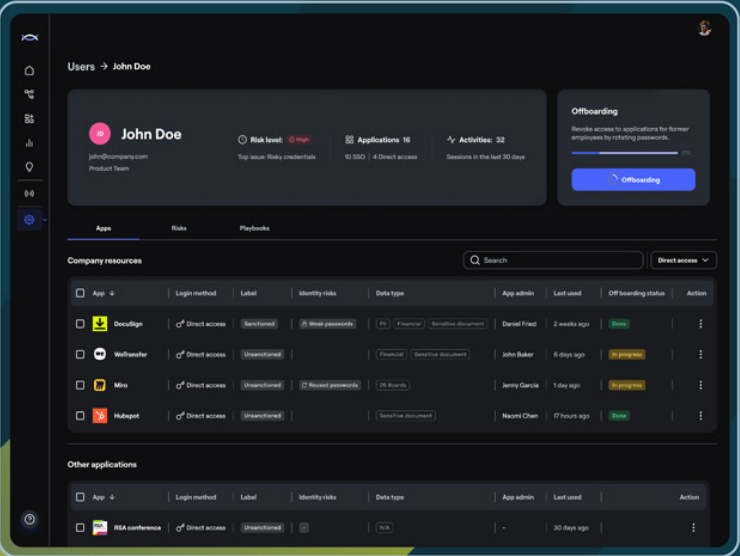
One of the most significant challenges that organizations face is the offboarding process. Savvy tackles this challenge head-on by providing a comprehensive solution for identifying and managing user access to both federated and non-federated applications. The platform's visibility into shadow IT applications, combined with its automation capabilities, enables organizations to quickly and efficiently revoke access for leaving employees, minimizing the risk of unauthorized access and data breaches.



Source: Savvy, Analyst Briefing Deck (07/2024)

Savvy's approach to offboarding goes beyond simply revoking access to federated applications. The platform also addresses the often-overlooked issue of direct access to applications through shared accounts or personal devices. By identifying these risky practices, Savvy enables organizations to take appropriate action, such as closing shared accounts or enforcing multifactor authentication (MFA). This holistic approach to offboarding ensures that organizations can effectively manage user access throughout the entire employee lifecycle without blind spots that would incur significant risks.

Automation is a key component of Savvy's platform, streamlining security workflows and reducing manual effort. The platform leverages robotic process automation (RPA) to automate tasks such as password rotations and account closures during offboarding (leavers). This automation not only saves time but also reduces the risk of human error, ensuring consistent and reliable security practices.



The screenshot displays the Savvy platform's user management interface. At the top, a user profile for 'John Doe' is shown with a risk level of 'High', 16 applications, and 32 activities. Below this, a table lists 'Company resources' with columns for App, Login method, Label, Identity risks, Data type, App admin, Last used, Off boarding status, and Action. The table includes entries for 'DocuSign', 'Webtransfer', 'Miro', and 'Hubspot'. A section for 'Other applications' is also visible at the bottom.

Automate Access Reviews & Offboarding

Uncovered by Savvy
100% of organizations:

- No complete offboarding
- Has shared accounts
- Compromised accounts being used

Automate

- Access Reviews
- Offboarding process of unmanaged SaaS
- SOC2/PCI/SOX Compliance requirements

[Demo](#)

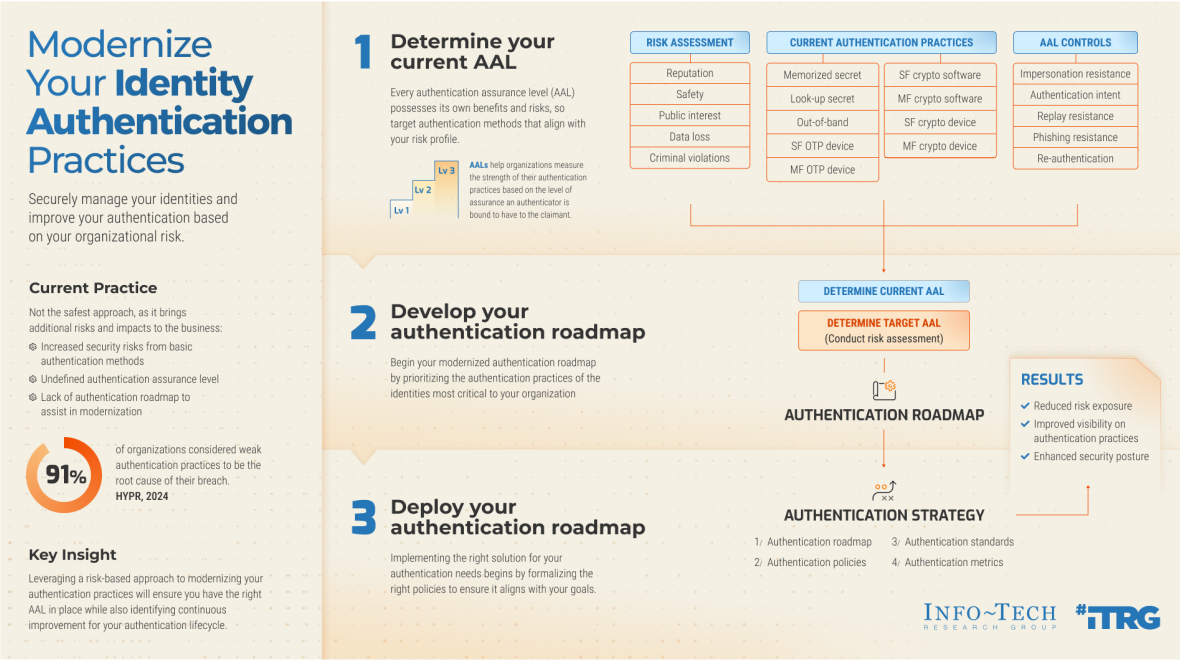
SAVVY

Source: Savvy, Analyst Briefing Deck (07/2024)

SSO Is Not a Silver Bullet

Savvy's platform goes beyond the standard benefits of single sign-on (SSO) by identifying hidden risks associated with user accounts, even those integrated with SSO. For example, Savvy can detect when users, while predominantly using SSO for an application like Salesforce, occasionally log in directly with weak or reused passwords, it can also identify when employees access Salesforce instances the organization might not know about. This behavior might go unnoticed in a traditional SSO environment, but Savvy's browser-level monitoring exposes these vulnerabilities.

Some will argue that with MFA, this is not a big risk. My counter to that is that as long as there are phishable credentials in the authentication loop, passwords are still a concern and should be evaluated to meet expected assurance levels, e.g. NIST SP 800-63B.



Source: ITRG, *Modernize Your Identity Authentication Practices* (07/2024)

Furthermore, Savvy uncovers instances of shared accounts, highlighting potential security gaps. For example, a Salesforce account might be used by multiple employees, some using SSO and others logging in directly with potentially compromised credentials. Savvy's platform not only identifies these shared accounts but also tracks the associated risks, such as password reuse across multiple platforms. Another access pattern observed is when someone uses their corporate identity credentials for personal accounts. Most solutions do not catch this password reuse, but Savvy sees it and connects the risk from those shadow accounts that share the same password as a corporate account. This way, if there is a cyberattack,

you can quickly reference Savvy's identity graph to determine if the compromise could translate risk onto corporate systems. This level of granular visibility empowers organizations to proactively mitigate security threats that extend beyond the capabilities of standard SSO implementations.

Our Take

Savvy is a powerful and versatile SaaS security platform that offers a unique combination of visibility, risk assessment, privacy, customization, and automation. The platform's ability to address the complex challenges of shadow IT and identity governance makes it an invaluable asset for organizations seeking to enhance their security posture and protect their sensitive data. I often talk to members who want greater assurance that their identity lifecycle management practices are robust. Without a way to account for out-of-band access requests and non-monitored access patterns, this will continue to serve as a gaping blind spot in the J/M/L (joiner, mover, leaver) process, especially the offboarding. While Savvy is still a relatively new player in the market, its rapid growth, business acumen, seasoned staff and positive customer feedback indicate that it is poised to become a leader in the SaaS security space.



Manage 3rd-Party SaaS Risk

Uncovered by Savvy

- SaaS integrations to top business apps
- >50% of integrations are inactive for six months
- 40% installed by end users
- 8% of the workforce uses GenAI 14 times a week

Remediate

- Unused access
- Risky Sensitive scopes access
- Toxic account combination

Automate

- Access Reviews
- Compliance Audit
- Real-time policy guidance

Source: Savvy, Analyst Briefing Deck (07/2024)