Reco
SaaS Security

2024 The State of SaaS Security

An Inside Look at Trends, Risks, and Countermeasures

www.reco.ai

Reco

Table of Contents

Introduction

As the nature of work continues to evolve, SaaS apps have become an integral component in how the world operates. SaaS is heavily relied on across many industries, from transportation and technology and healthcare, to finance. This adoption is only expected to grow further, placing unprecedented responsibility on security teams to understand and address the current state of SaaS security.

The rapid adoption of SaaS solutions, accelerated by trends such as remote work, cloud computing, big data, and more recently, Generative AI (GenAI), has brought significant benefits to organizations. However, this transformation also introduces new attack surfaces and unique challenges for security teams, who must now consider how they can secure the intricate web of SaaS usage across their organization.

Today, the SaaS security landscape is characterized by several key themes and issues:

1. **Credential Theft and Stuffing:** This trend is fueled by dark web marketplaces where breached credentials are bought, sold, and traded, making it easy for attackers to carry out credential stuffing attacks. This is what has led to initial access in many breaches including the 2022 Uber data breach.

2. **Shadow SaaS:** The explosion of unauthorized SaaS apps has led to a rise in employees inadvertently exposing sensitive data. Trial or demo accounts are a main source of shadow SaaS.

3. **SaaS Sprawl:** In 2023, the average number of SaaS apps used by a business reached 473. Our numbers indicate a 3.7% increase this year. Now, consider that each app has unique security settings and considerations and you have yourself a recipe for security overhead.

4. **Data Sprawl:** Given the challenges introduced by SaaS sprawl, shadow SaaS, and more recently the adoption of GenAI, and you have sensitive data residing everywhere. Keeping track of it all is a full-time job on its own.

5. **SaaS Shared Responsibility Model:** While SaaS vendors provide varying degrees of security controls, it's up to customers to configure them correctly. Misconfigurations, like those in the recent Fortinet breach, expose sensitive data and create vulnerabilities. Organizations must take ownership of securing their SaaS environments by properly configuring and monitoring the settings and activity across their applications.

Executive Summary

Drawing from our analysis of **over 6,600 SaaS environments**, this report provides an unprecedented, data-centric view into the SaaS security landscape in 2024.

Our findings reveal critical trends and strategic opportunities that will help shape the future of SaaS security:

1. **The Continued Explosion of SaaS and Unauthorized Use -** Organizations are utilizing an average of 490 SaaS applications per customer—**a 3.7% increase from 2023**. Alarmingly, on average only 229 of these apps are officially authorized, **leaving 261 apps on average** outside the purview of security teams.

2. **The Shadow SaaS Blindspot: 1 in 4 Apps Fly Under the Radar -** With an **average of 129 shadow SaaS apps** per company, **shadow SaaS accounts for 25%** of all SaaS usage within organizations. This significantly expands an organization's attack surface, as well as the risk of data breaches and non-compliance.

3. **The MFA Gap: 1 in 10 Accounts Are Still Vulnerable -** Despite progress, **9.5% of user accounts**—including many administrative accounts—**don't have Multi-Factor Authentication (MFA) enabled**. This poses a significant security risk, especially for overly-privileged accounts.

4. **AI in the Enterprise: The Double-Edged Sword -** Organizations are rapidly adopting Generative AI tools, with the **average company now using 17 GenAI applications**, up from 13 (+30.7%) in July. While beneficial, these tools introduce new security challenges, especially when integrated with critical resources like shared organization storage drives.

5. **Data Leak Dangers: Misconfigurations in SaaS Platforms –** Our analysis across 50+ environments and over 6,600 applications found critical misconfigurations in popular SaaS platforms. **91% of Salesforce instances** had **public file sharing enabled without password protection**, increasing the risk of unauthorized access. Similarly, **78.7% of Snowflake instances** had the **PREVENT_UNLOAD_TO_INLINE_URL** parameter set to false, exposing sensitive data to potential exfiltration. When paired with other misconfigurations, this opens up organizations to potential for data breaches.

These findings illustrate the reality of complexity that security teams must navigate as they secure SaaS usage across their organizations. As SaaS usage continues to grow, it's crucial for organizations to implement security strategies that address unauthorized app usage, identity management, and emerging technologies.

In this report, we'll also provide you with insights and guidance needed to ensure the secure deployment and usage of SaaS apps across your organization. By better understanding these trends and challenges, organizations can leverage the full benefits of SaaS while staying secure.

Methodology

Transparency is of utmost importance at Reco. This section provides a detailed overview of our approach, ensuring that our findings can be properly contextualized and are not misleading in any way.

This report analyzes SaaS environments across 50+ environments of various industries and sizes to provide a comprehensive view of the current SaaS security landscape.

Data Collection

Our multi-faceted approach included:

1. **MFA Coverage Analysis:** Taking a snapshot of Multi-Factor Authentication (MFA) adoption status during customer onboarding and tracking usage over time. We assess user coverage, identify accounts without MFA enabled, and track ongoing posture with security policies.

2. **Application Discovery:** Identifying authorized and unauthorized SaaS apps across organizations.

3. **Configuration Analysis:** Examining security settings across popular SaaS platforms to identify potential vulnerabilities and best practices.

4. **Extended Monitoring Period:** Assessing data points over a span of three months to ensure consistency and identify any anomalies that might skew results.

Data was collected from July to September 2024 to ensure current and relevant findings. This three-month window allowed us to capture evolving trends and provide the most up-to-date insights into the SaaS security landscape.

Limitations

While comprehensive, our methodology had some constraints:

- The sample may not fully represent all industry sectors or company sizes.
- Some security measures, including third-parties, may not be detectable through our analysis methods.

Despite these limitations, we believe our analysis provides valuable insights into the state of SaaS security in 2024.

Glossary

Generative AI (GenAI) Apps: Apps that use AI models to create new content, such as text, images, or audio, by learning from existing data and prompts from the user.

Multi-Factor Authentication (MFA): An authentication process that requires users to provide multiple forms of verification to gain access to a system.

Misconfiguration: Incorrect settings or configurations in a software application that can lead to security vulnerabilities.

Non-Human Identity (NHI): Digital identities assigned to non-human entities, such as apps, services, service accounts, API keys, or devices.

Posture Management: The process of continuously monitoring and managing the security configurations and settings of systems, applications, or networks to ensure they align with best practices and compliance requirements.

Principle of Least Privilege: The concept of granting users the minimum level of access necessary to perform their job functions.

Shadow SaaS: Unauthorized SaaS apps that are used within an organization without IT oversight or approval.

SSO (Single Sign-On): An authentication mechanism that enables users to access multiple related systems or applications with one set of login credentials.

Zero Trust: A security model that requires continuous verification of identity and context for every user and device attempting to access resources, regardless of their location, to minimize risks from both internal and external threats.

Key Findings

1 Generative AI Surge: Balancing Innovation with Emerging Security Risks

Organizations are rapidly adopting Generative AI tools, with the average company now using **17 GenAI applications,** up from 13 (+30.7%) in July. While these apps provide undeniable benefits, they also introduce new security challenges.

Depending on how GenAI apps are deployed and used, they pose a varying degree of risk. SaaS application copilots, like Microsoft's Copilot, are often integrated with crown jewel resources like OneDrive, GitHub, Word, Excel, Teams and PowerPoint. This level of integration exposes vast amounts of sensitive data to AI apps, which elevates the risk of data breaches and the magnitude of them.

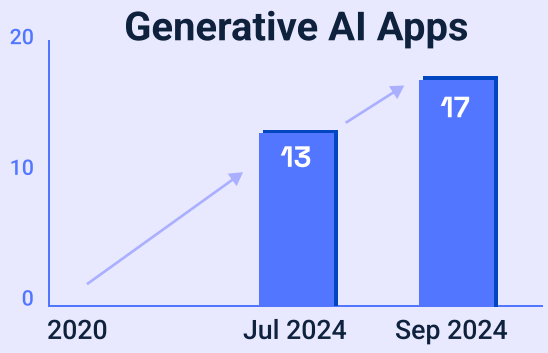
Earlier this year, U.S. Congress banned staff use of Microsoft's Copilot citing their strict security and compliance requirements. That said, not all GenAI apps are created equally. Some pose a more limited risk compared to organizational copilots.

The key to mitigating risks posed by GenAI apps is setting clear policies on AI tool usage, carefully vetting AI vendors for security and compliance standards, implementing data protection measures like data anonymization, and establishing oversight committees to monitor AI use within the organization.

At Reco, we expect the adoption of AI to increase exponentially over the coming years. There is no better time than now to implement a security strategy to secure the use of AI in your organization.

30.7%

There Has Been a 30.7% Surge in GenAI Adoption

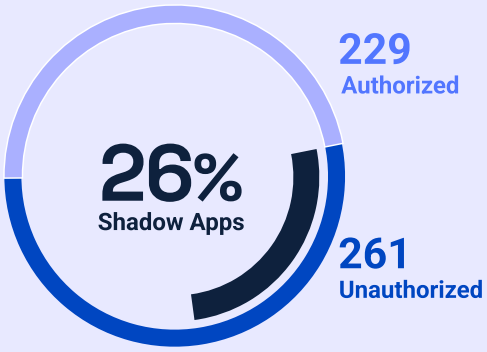


2 Illuminating Shadow SaaS: Understanding the 26% of Unseen Apps

Our analysis reveals that **shadow SaaS applications**—unapproved apps used without IT or Security's knowledge—**account for 26% of all SaaS usage** within organizations. With an average of **129 shadow SaaS apps per company,** these apps bypass established security controls and compliance oversight and significantly increase the risk of data breaches and exposure to unmonitored third-party solutions.

To mitigate these risks, organizations should balance innovation with governance by implementing employee education programs, conducting regular software usage audits, and deploying SaaS discovery solutions to enhance visibility. Key actions include:

- **Establishing a process for employees to request new apps**
- **Creating a self-service portal for accessing pre-approved apps**
- **Streamlining the request and approval process for low-risk apps**
- **Conducting regular SaaS app usage audits**
- **Deploying SaaS discovery solutions to identify unauthorized app usage**



26%

Nearly 26% of Connected SaaS Apps Are Unauthorized

3 The MFA Oversight: Progress, But Still a Ways to Go

Despite great progress in recent years, **9.5% of user accounts**—including many administrative accounts—**don't have Multi-Factor Authentication (MFA) enabled.** This oversight is a significant security risk. Accounts without MFA are easy targets for attackers using phishing or credential stuffing techniques. The risk is especially high with administrative accounts. If compromised, attackers could gain full access to your systems and sensitive data.

Real-world incidents like the Snowflake breach, which affected companies like Santander Bank, AT&T, Ticketmaster, LendingTree, Advance Auto Parts, and impacted over 500 million customer records due to lack of Multi-factor Authentication (MFA) enforcement, highlight the devastating impact of inadequate authentication practices. Not having MFA on all accounts, especially Admin accounts, is like leaving your door and windows open.

Organizations must enforce MFA across all users without exception, prioritize securing over-privileged accounts, provide user training on MFA importance, and consider advanced authentication methods like single sign-on (SSO) and biometrics to enhance access to sensitive data and critical apps.

On the bright side, this finding means that **90.5% of accounts assessed do have MFA enabled.** This is a big win for the cybersecurity industry as this number was much lower even just five years ago. Kudos to major vendors, such as Microsoft, that have been leading the way by enforcing MFA by default.

90.5%

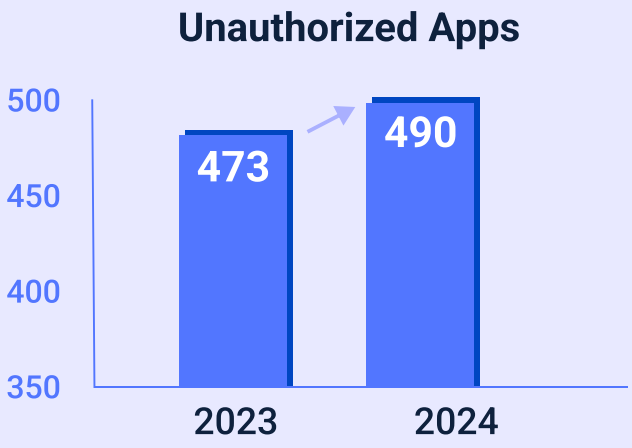
A Positive Sign: Nearly 90.5% of Accounts Have Enabled MFA

4 SaaS Sprawl: The Continued Explosion of Unauthorized Apps

Our analysis reveals that businesses are utilizing **an average of 490 SaaS applications**—a 3.7% increase from 2023. While SaaS utilization is expected to continue to increase, what's most compelling is that **on average only 229 apps are officially authorized** (meaning they have been vetted and approved by the organization's IT or security team for use). This leaves, on average, **261 apps outside of the purview of security teams.**

While securing usage of approved SaaS apps is already difficult enough, it's nearly impossible to secure unauthorized usage. Security teams simply cannot secure what they're not aware of. Unauthorized apps expand an organization's attack surface, making it more susceptible to security breaches, data leaks, and compliance failures. This unchecked expansion of SaaS applications presents a critical challenge for organizations striving to maintain effective governance and data integrity.

To combat this, organizations must implement robust governance and app procurement frameworks, such as centralized SaaS management platforms and stringent approval processes, to effectively oversee this sprawl and mitigate associated security risks.



3.7%

There Has Been a 3.7% Increase in Usage of Unauthorized Apps

5 Data Leak Dangers: Preventing Misconfigurations in Enterprise SaaS

Through our analysis across 50+ environments and over 6,600 applications, we found that two prevalent, critical misconfigurations were frequently identified during the onboarding of our solution. These misconfigurations, if not addressed, could lead to sensitive data leaks.

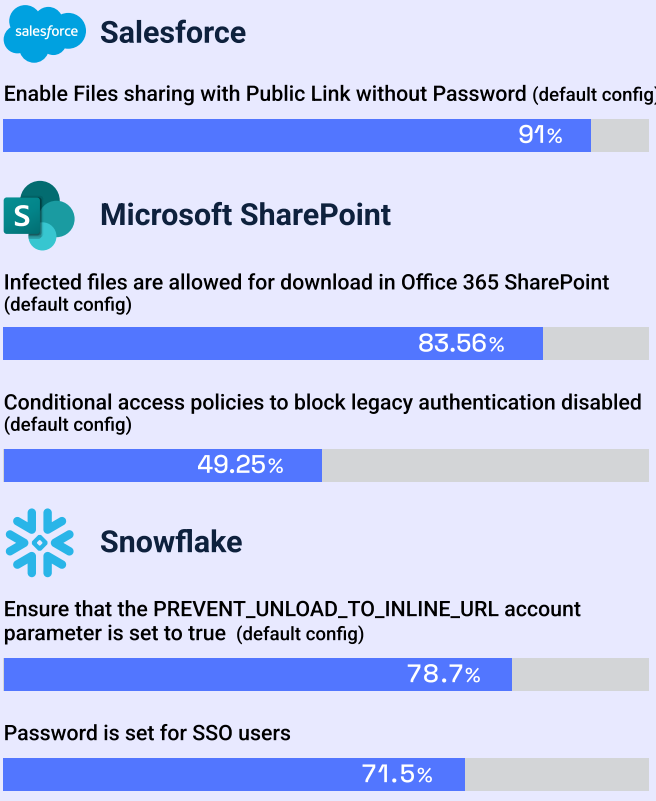
Salesforce Misconfigurations

Remarkably, we found that **91% of Salesforce instances** during onboarding had enabled the option to share files via public links without password protection. This configuration makes sensitive information more susceptible to unauthorized access. Without any password protection, anyone who gets hold of the link can access the files, which is risky if these links are shared widely or carelessly.

Snowflake Misconfigurations

In a similar vein**, 78.7% of Snowflake instances** analyzed during the onboarding phase had the PREVENT_UNLOAD_TO_INLINE_URL account parameter set to false. This setting is essential for bolstering security by preventing data exfiltration. When activated (true), it blocks the execution of COPY INTO <location> commands designed to export data to potentially unsafe or unverified inline URLs. These URLs, being explicitly mentioned in the command rather than referenced through a Storage Integration object, pose a direct threat of data leakage if left unsecured.

Salesforce and Snowflake Are Among The Most Commonly Misconfigured Apps



Recommendations

Implement SaaS environment monitoring and threat detection

Effective monitoring and threat detection are essential for identifying potential risks in your SaaS environment. As adoption of SaaS apps explodes across organizations, it's key to continuously monitor for anomalous activity and vulnerabilities in real time. Monitoring and threat detection can help identify misconfigurations, unauthorized access, and other potential threats. Here are some steps to improve monitoring and detection:

1. **Deploy a SaaS Security Posture Management (SSPM)** solution to automate the detection of misconfigurations, policy violations, and security gaps across all your SaaS apps.

2. **Implement a solution that performs User and Entity Behavior Analytics (UEBA)** to detect anomalous behavior, such as sudden increases in data access or abnormal login locations which could indicate a compromised account.

3. **Leverage threat intelligence feeds that are specific to the SaaS apps in use**. Incorporate this intelligence into your existing monitoring and detection flows to detect and respond to emerging threats.

4. **Monitor audit logs and access reports from SaaS apps** to identify patterns of abuse, signs of privilege escalation, or other attack tactics and techniques.

Implement a SaaS governance program

A SaaS governance program is essential for managing the proliferation of SaaS apps within your organization. It provides a framework for controlling SaaS adoption, usage, and security, ensuring that all applications align with business objectives and compliance requirements.

Whether you're at a startup or large enterprise, below are some tactical tips to help you get started:

1. **Deploy a SaaS inventory management system** to track and monitor all SaaS apps being used within the organization, including shadow SaaS. Use automated discovery tools to detect unsanctioned SaaS usage.

2. **Create and enforce a SaaS procurement policy** that requires security and compliance reviews before any new SaaS application is approved. This should include vendor risk assessments, data privacy checks, and alignment with internal security policies.

3. **Set up a recurring review cycle** (e.g., quarterly) to evaluate the security posture of all SaaS applications, ensuring they are up to date on patches, compliance requirements, and that their configurations adhere to security best practices.

4. **Define roles and responsibilities for SaaS governance**, assigning specific team members to oversee SaaS usage, risk management, and ongoing compliance within their respective departments.

Develop a strong IAM program based on a Zero Trust approach

A strong Identity and Access Management (IAM) program is the foundation of secure SaaS usage. By adopting a Zero Trust approach, organizations can ensure that only authorized users have access to sensitive data and applications, regardless of their location or network. Below are several recommendations that can help supercharge your IAM program regardless of where you're at in the journey:

1. **Enforce multi-factor authentication (MFA)** for all users across all SaaS apps, especially for administrative accounts and users handling sensitive data.

2. **Use Single Sign-On (SSO)** to streamline access management, providing users with a unified login while centralizing control. Integrate SSO with identity providers that support Zero Trust policies to ensure continuous validation of user trust.

3. **Adopt the principle of least privilege** by setting granular access controls for each SaaS application. Ensure users only have access to the resources they need for their job functions, and implement just-in-time (JIT) privilege escalation for temporary access where available.

Develop an AI governance program

As teams across organizations increasingly adopt emerging technologies like Generative AI (GenAI), it's crucial to develop a security strategy that mitigates risks while maximizing their benefits to support the business. New technologies can exponentially supercharge a team's productivity whether it be for development, data analytics, operations, and more. In most cases, there's no way of stopping adoption of new types of technology, so having a plan in place to reduce the risk is paramount.

Below are a few tips to ensure a secure integration of GenAI into your SaaS environment:

1. **Conduct a detailed threat model** for each GenAI tool, evaluating data input/output flows, attack vectors, dependencies and potential implications in case of a breach. Based on the findings, mitigate the risks based on the business' risk appetite.

2. **Upon onboarding the solution, review and properly configure security settings,** and always use the enterprise tier with enhanced security features, if possible. Look for settings like data encryption, API access controls, user permissions, and public asset sharing.

3. **Implement strict user permissions for employees** interacting with GenAI apps. Ensure that only authorized users can upload data or access AI-generated outputs by following the principle of least privilege.

4. **Establish clear policies** for the usage and governance of GenAI apps, including guidelines on acceptable use and data protection.

Prioritize secure onboarding and remediation

Securing SaaS apps starts with a thorough procurement and onboarding process that assesses and verifies the security of the app being onboarded. Equally important is the ability to remediate security issues quickly to minimize exposure and risk of breach.

Here are a few actionable steps to enhance onboarding and remediation:

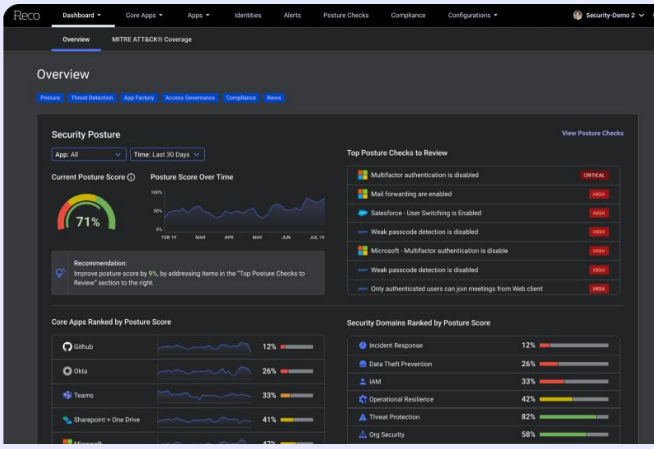
1. **Create and follow a checklist for SaaS onboarding** that includes verifying encryption standards, identifying security features (such as MFA/SSO), and other controls required for strong security and compliance.

2. **Set up automated remediation workflows** using security orchestration tools to instantly detect and address common SaaS misconfigurations (e.g. insecure sharing settings, open APIs). As with all automation, assess the potential downstream implications to prevent any inadvertent errors or system downtime.

3. **Establish clear offboarding protocols** that automatically revoke access to SaaS applications for departing employees, ensuring no lingering access.

Conclusion

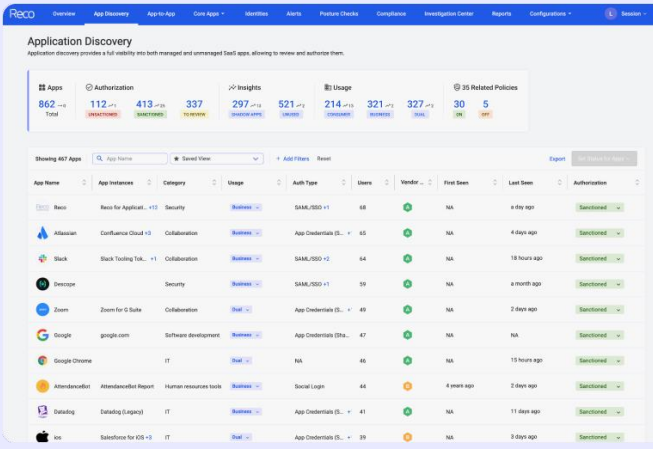
Reco - a Complete Solution for SaaS Security



As evident by the findings in our report, there's a critical need for a comprehensive, proactive, and intelligent SaaS security solution that can effectively handle the heavy lifting of securing SaaS applications. The rise of unauthorized SaaS applications, identity risks, misconfigurations, and the rapid adoption of AI pose critical challenges for security teams.

Reco stands out as the trusted partner capable of addressing these challenges head-on, with a product tailored to meet the most pressing needs of today's SaaS environments. Let's break down exactly how Reco can help solve the problems highlighted in this report.

Comprehensive SaaS Visibility



One of the biggest issues identified in this report is the lack of visibility into SaaS environments, especially with unauthorized and shadow SaaS apps running rampant. Reco addresses this with:

- **Full SaaS Discovery:** Reco continuously discovers all applications, sanctioned and unsanctioned, providing an always-updated inventory of apps across your organization.
- **Shadow SaaS Visibility:** Reco identifies hidden or unauthorized apps that bypass traditional security controls to bring these apps under management and reduce risk.

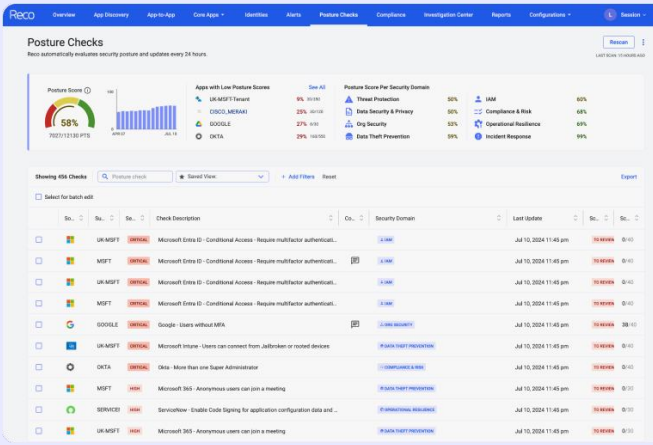
The Reco Difference: Without visibility, you can't secure what you don't know exists. Reco shines a light on every corner of your SaaS environment, empowering teams to regain control and minimize risks.

SaaS Security Posture Management

Misconfigurations in SaaS apps are a major driver of data breaches, as seen in high-profile incidents like the Snowflake misconfigurations. Reco's Posture Management feature provides:

- **Continuous Security Posture Monitoring:** Reco continuously assesses the security configurations of SaaS apps to ensure compliance and reduce exposure.
- **Actionable Alerts on Misconfigurations:** Reco identifies misconfigurations across 100+ integrations and provides immediate steps for remediation.

The Reco Difference: Reco acts as your always-on security partner, continuously monitoring your SaaS environment to prevent costly misconfigurations.

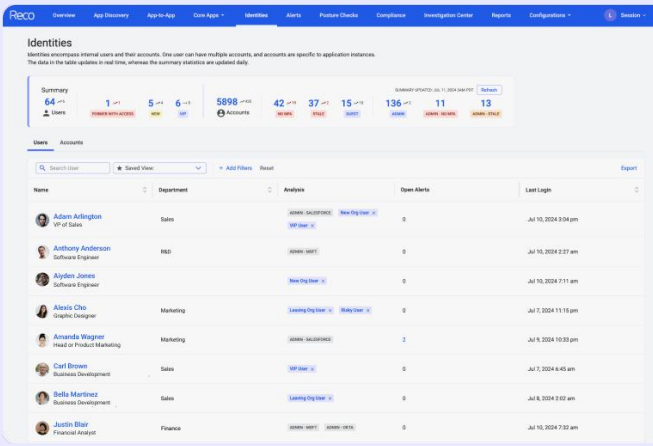


Identity Security Posture Management

With misconfigured access permissions and accounts without MFA a leading cause of data breaches, securing identities is paramount. With the rise of AI and SaaS usage, the identity sprawl only continues to grow. Reco's identity security posture management provides:

- **Detailed Identity Mapping:** Reco monitors for both human and non-human identities across SaaS environments.
- **MFA and Privileged Access Enforcement:** Reco identifies accounts without MFA and provides actionable insights to enforce MFA across the board, especially for Admin accounts.

The Reco Difference: In a landscape where identities can be easily compromised, ensuring that the right users have the right access—and nothing more—is critical. Reco makes that process seamless and secure in all SaaS ecosystems.

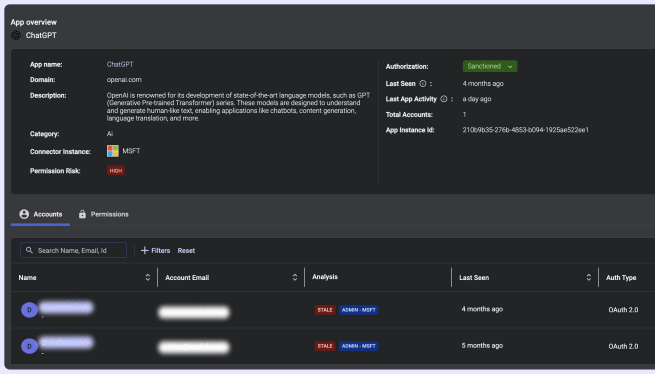


Generative AI Governance

With the rise of Generative AI in SaaS apps, the risks associated with sensitive data exposure and unvetted tools are a growing concern. Reco helps mitigate these risks with:

- **Shadow AI Detection:** Reco detects the use of AI copilots and other GenAI tools within SaaS environments, even if they are unauthorized.
- **Data Protection and AI Governance:** Reco provides security teams with visibility into which AI tools are accessing sensitive data, enabling organizations to implement clear policies and governance frameworks for AI use.

The Reco Difference: Reco gives you the power to harness the potential of AI without sacrificing security. With full visibility and governance over AI tools, you can innovate confidently, knowing that sensitive data remains secure. Reco ensures that AI adoption drives growth—not risk.

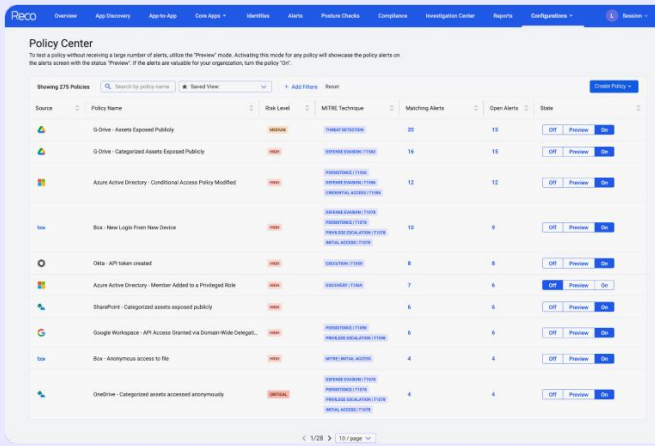


Real-Time Threat Detection & Response

Threats in SaaS environments are ever-evolving, from credential stuffing to misconfigurations in critical SaaS apps. Reco's real-time detection capabilities ensure swift action when threats are detected:

- **AI-Powered Threat Detection:** Using AI-based analytics, Reco identifies risky behaviors, compromised accounts, and potential threats as they occur.
- **Automated Remediation (through SIEMs or SOARs):** Reco integrates with SIEMs and SOAR solutions for automatic remediation of common security misconfigurations, such as insecure file sharing or improperly configured APIs.

The Reco Difference: By leveraging graph-based AI to detect risky behavior and high-precision remediation, Reco helps you stay one step ahead of attackers. This real-time protection means your security team can act before vulnerabilities become breaches, saving time, resources, and protecting your reputation.



Full SaaS Lifecycle Management

Beyond the individual, next-gen features highlighted, Reco provides end-to-end management of your entire SaaS ecosystem, helping you secure your SaaS applications from onboarding to offboarding:

- **Rapid Integration with 120+ SaaS Apps:** Reco offers comprehensive SaaS application coverage, from core applications to long-tail applications. Our low-code/no-code development approach means we are constantly adding new integrations. We currently add 3-5 new integrations every week.
- **Seamless Offboarding:** Automatically revoke access for users when they leave the organization, ensuring no lingering access to sensitive data.
- **Ongoing Monitoring:** Continuously track new SaaS apps, configuration changes, and emerging threats in the headlines.

The Reco Difference: From onboarding new apps in just days to securely offboarding employees, Reco reduces complexity and ensures that no risks fall through the cracks, keeping your organization secure as it grows.

Why Reco is the Best Choice for SaaS Security

By leveraging Reco's advanced AI-driven capabilities, organizations can move beyond reactive security measures to a proactive, intelligent approach that adapts to their business and the growing complexities of the modern SaaS landscape. Reco offers:

1. **Scalable integration with the most popular SaaS applications,** helping organizations stay agile and secure in a fast-changing environment.
2. **Full visibility and control over the SaaS ecosystem** from approved apps to shadow AI tools and identities.
3. **Compliance-ready SaaS posture management** to avoid costly misconfigurations.
4. **Identity and access security with Zero Trust principles**, ensuring only authorized users access critical resources.
5. **Real-time threat detection and automated remediation**, addressing risks the moment they arise.

By choosing Reco, your organization gains the visibility, intelligence, and control needed to thrive in today's SaaS-driven world. **Reco is the key to unlocking secure, scalable SaaS growth**—empowering your teams to change the world while keeping the business secure.

On this journey, Reco can serve as your advisor and partner. You can learn more about Reco or book a demo at www.reco.ai.