Reco
Secure Your SaaS

Manage SaaS App & Shadow IT Integration Risk

Get full visibility into the applications connected to your SaaS apps, including shadow apps and 3rd-party apps such as GenAI tools. Understand which users have enabled them, and the level of access they've been granted.

Discover All Connected SaaS Tools

Get full visibility into the managed and unmanaged SaaS tools connected to your environment, including shadow apps and 3rd-party apps. Manage them from a single, aggregated view.

Identify Misconfigured & Over-Permissive Apps

Ensure SaaS apps are properly configured to provide the right level of data access and never deviate from business intent. Reco can measure the risk introduced by connected apps that haven't been used, but still retain access to SaaS data.

Prioritize with AI-Based Business Context

Rely on advanced analytics based on a combination of algorithms, models, processes and tools to help you prioritize the riskiest apps. Use this intelligence to remove unused or unsanctioned apps.

Ensure Compliance for All of Your SaaS Apps

Maintain compliance using digital asset inventory for all of your SaaS apps. Continuously evaluate and quantify the severity of each integration's overall risk so you can prioritize which to address first.

**Posture Management & Continuous Compliance**

App Discovery & Shadow Apps

Identity & Access Governance

Threat Detection & Response

Reco SaaS-to-SaaS Discovery Accomplishes This and More

- Discovers both SSO and non-SSO apps, including shadow apps and GenAI tools
- Authorizes/deauthorizes apps and notifies of new risky apps
- Detects all login activities and generates an inventory of all used apps and the users
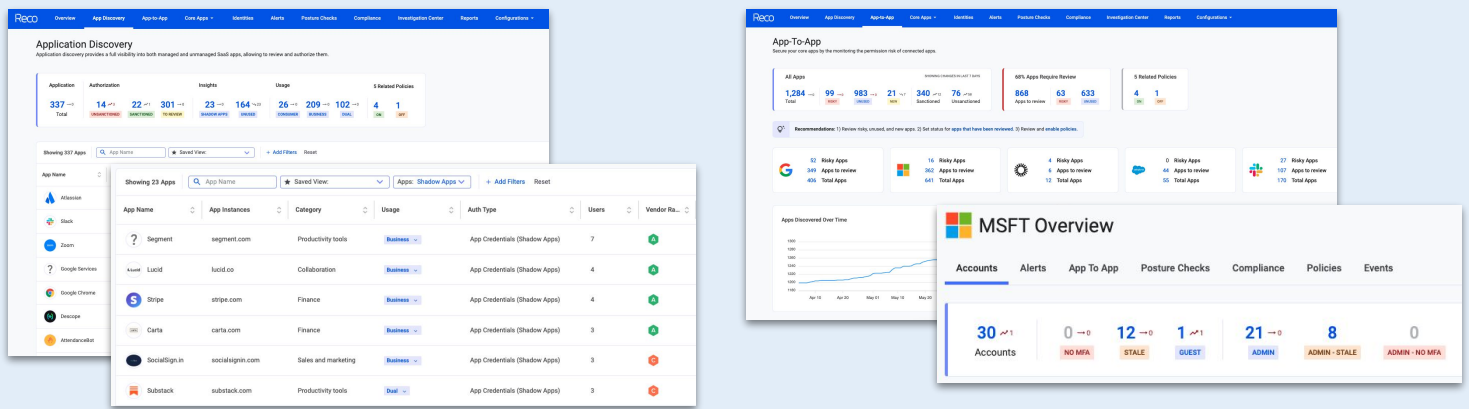
Reco Continuously Monitors for Connected SaaS Applications

+700
apps for org with **~500** employees

+2500
apps for org with **1500+ employees**

~5
new **AI SaaS apps** connected **every week**

Reco Supports These Business-Critical SaaS Applications and More

Organizations Worldwide Trust Reco to Mitigate Risk from SaaS-to-SaaS Integrations

CISO, Cybersecurity Company: "An app connected to our Salesforce instance had permission to view opportunity status fields as well as notes, and automatically sent a letter and flowers to a prospect. How did I not know about that?"

Security Leader, Enterprise Automation Company: "A Sales Rep connected a GenAI tool to our Zoom to summarize prospecting calls and analyze their pitch. The GenAI app automatically changed the configuration of Zoom to record every meeting and upload the file into the GenAI app. These meetings included a highly confidential SEC prep meeting and Board meeting. We had to go through the pain of ensuring that all confidential information within the recordings was deleted and exposed regulated data was removed from the GenAI app."

To learn more, email us at **info@reco.ai** or visit **reco.ai.**