reco

Empower Your Users with Secure Access.

Identities multiple faster than they can be tracked. Every forgotten contractor account, over-privileged user, and shared admin credential widens the SaaS Security Gap. While your Security team drowns in alerts, the real threats slip through unnoticed. Dynamic SaaS Security by Reco ensures access privileges are minimized, and accounts remain secure.

End Identity Proliferation

We unify identities across SaaS apps so you can discover admins, over-permissioned users and service accounts. Understand critical exposure gaps from stale accounts, MFA violations, devices, events, and impossible travel that can lead to a breach.

Minimize Excessive Permissions

Keeping accounts secure while minimizing access privileges is unfeasible with the relentless proliferation of identities. We automatically flag risky permission combinations and enforce least-privilege across your entire SaaS ecosystem.

Detect Identity Security Failures

Discover every account missing MFA, using weak passwords, sharing credentials, or stale accounts still lurking with admin access. We identify security gaps before security attackers do, providing actionable alerts to fix the issues that matter.

Maintain Ongoing Identity Hygiene

Say goodbye to spreadsheets. Initiate continuous access reviews with relevant stakeholders in your organization to certify entitlements across your SaaS apps. Generate reports on access status and de-provisioning activities for audits.

App Discovery
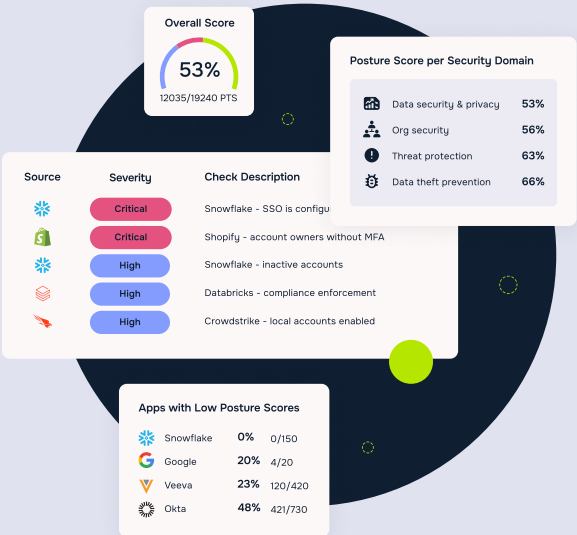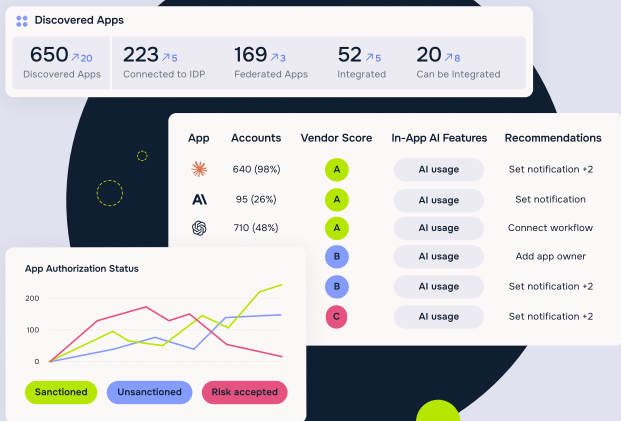
SSPM+

Identity & Access Governance

Identity Threat Detection & Response

reco

How We Close the Gap Created by Identity Sprawl

Continuous identity monitoring

tracks every permission change in real-time

Overall Score

53%

12035/19240 PTS

Posture Score per Security Domain

Data security & privacy	53%	
Org security	56%	
Threat protection	63%	
Data theft prevention	66%	

Source	Severity	Check Description
	Critical	Snowflake - SSO is configu...
	Critical	Shopify - account owners without MFA
	High	Snowflake - inactive accounts
	High	Databricks - compliance enforcement
	High	Crowdstrike - local accounts enabled

Apps with Low Posture Scores

Snowflake	0%	0/150	
Google	20%	4/20	
Veeva	23%	120/420	
Okta	48%	421/730	

Discovered Apps

650 ↗20	223 ↗5	169 ↗3	52 ↗5	20 ↗8
Discovered Apps	Connected to IDP	Federated Apps	Integrated	Can be Integrated

App	Accounts	Vendor Score	In-App AI Features	Recommendations
	640 (98%)	A	AI usage	Set notification +2
	95 (26%)	A	AI usage	Set notification
	710 (48%)	A	AI usage	Connect workflow
		B	AI usage	Add app owner
		B	AI usage	Set notification +2
		C	AI usage	Set notification +2

App Authorization Status

Sanctioned | Unsanctioned | Risk accepted

Dynamic SaaS Security

evolves with your identity landscape, no matter how fast it grows

Knowledge Graph

provides business context so you understand which identity risks actually matter

Department: R&D
Email: chris_w@gmail.com
Groups: Team star, Grow US

Identities Summary

31 ↗1	2 ↗1
Admin - no MFA	Former with access

Activites

Deleted | Downloaded | Shared externally
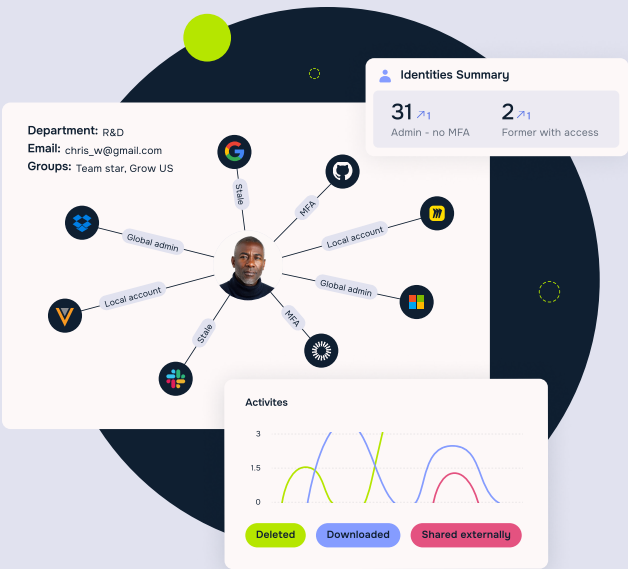
Reco's Dynamic SaaS Security Delivers Results

62%
of identities have excessive permissions that violate least-privilege principles

27%
of dormant accounts still retain sensitive data access

8x
increase in identity-based attacks targeting SaaS applications

reco

reco.ai

Secure Every SaaS App

Reco secures 150+ apps

eleos

You have a single pane of glass through which you can get as deep an understanding as you want. Every click takes you to a different place, and you can understand the entire story of that user.

Raz Karmi

CISO, Eleos Health

belk

And then if I have a risky user, somebody that potentially is getting ready to leave the organization or something, then I can see activity in a much cleaner path and be able to tie back if there's an issue.

Neda Pitt

CISO, Belk

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

reco