reco

Mitigate Potential Threats, Quickly.

Critical security incidents are hiding in plain sight, buried in thousands of meaningless alerts. While your analysts struggle to separate signal from noise, real security incidents—data theft, account compromise, and malicious insider activity—continue undetected. Dynamic SaaS Security by Reco delivers the speed and business context needed to identify what truly matters.

Cut Through the Event Noise

Instantly identify what matters in the sprawl of SaaS events. Alerts generated in Reco have a guided remediation strategy including the validity and accuracy of the event itself. Reco catches what traditional tools miss.

Detect Threats in Real-Time

Identify suspicious data access and exfiltration attempts as they happen before critical information walks out the door. Reco's context-based alerts utilize the power of our Knowledge Graph to alert on exposure. Your team can effectively prioritize and mitigate.

Stop Data Exfiltration

Our ITDR capabilities enforce policies, detecting data theft, account compromise, and configuration drifts while filtering out noise. Reco provides complete oversight of your SaaS ecosystem, including a visual mapping of policies to the MITRE ATT&CK framework.

Respond Automatically

Seamlessly integrate Reco with your existing SIEM, SOAR, or ticketing system. Correlate and automate events, reducing overall risk automatically and eliminating manual intervention. No waiting, no wondering—just immediate action.

App Discovery
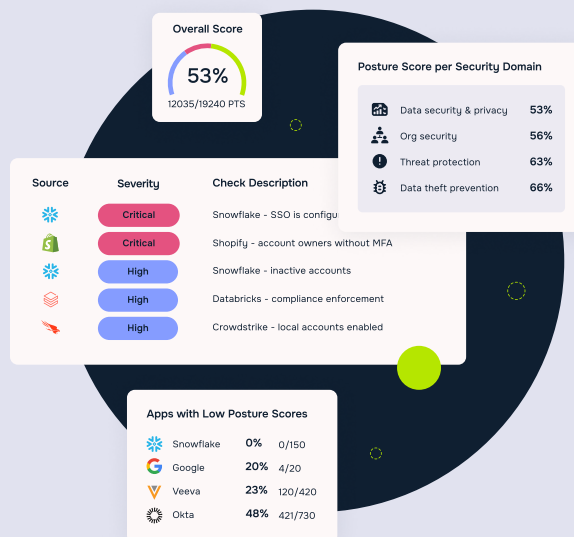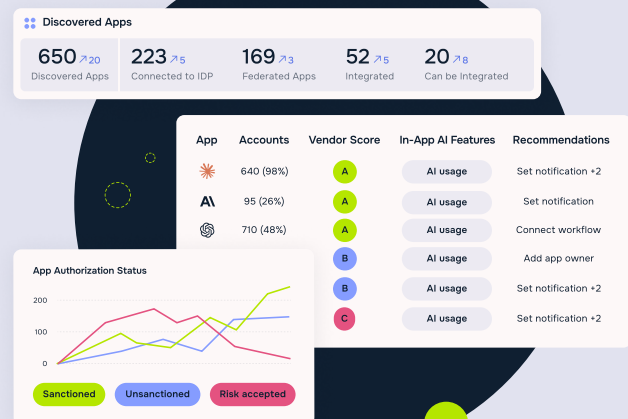
SSPM+

Identity & Access Governance

Identity Threat Detection & Response

reco

How We Close the Gap Created by Event Sprawl

Hundreds of pre-built detection controls

identify threats across your SaaS landscape

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

200
100
0

Sanctioned   Unsanctioned   Risk accepted

Automated response workflows

integrate with your existing security stack to take immediate action

Knowledge Graph

provides eureka-grade context so you understand which alerts actually matter

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

Stale · MFA · Local account · Global admin · Local account · Global admin · Stale · MFA

Identities Summary

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

Activites

3
1.5
0

Deleted   Downloaded   Shared externally

Reco's Dynamic SaaS Security Delivers Results

95%

reduction in false positives compared to traditional SaaS monitoring

Minutes

not days, to detect and respond to SaaS security threats

Zero

configuration needed to start detecting threats in your environment

reco

reco.ai

Secure Every SaaS App

Reco secures 150+ apps

solar**edge**

The drastic reduction in unclear alerts saved over 50% of our team's time, freeing them to focus on more important tasks. Reco's AI-based solution provided the missing context we needed to understand what actions we needed to take quickly and accurately. The immediate impact on our team's productivity was undeniable.

Timer Stenzler

Director of Cybersecurity

Ui|Path™

We knew the power of our robots, and how they could make our Sentinal SIEM more powerful. By automating the access removal process by passing Reco's contextual detections to our SIEM, we have saved thousands of hours of work, reduced the risk of data exposure across multiple SaaS shared drives, and now continue to reduce data exposure risks.

Mihau Faur

CIO, UiPath

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

reco