Protect Your SaaS Stack

SaaS is in AI overdrive. Your employees are connecting AI tools to your core systems with reckless abandon. Meanwhile, your sanctioned apps are quietly embedding AI features that access sensitive data. The AI Sprawl is real. And it's outpacing your security. Reco Dynamic SaaS Security empowers security teams to identify, assess, and govern generative AI usage across the enterprise – bridging the gap between innovation and security at SaaS speed.

How AI Sprawl Outpaces Security

Shadow AI Everywhere

Your employees are connecting AI tools without oversight. Every department has their favorite. Marketing uses one for content generation. Sales deploys another for call transcription. IT experiments with a third. You have no idea what data they're accessing or where it's going.

OAuth Connections Running Rampant

Every AI connection is a potential backdoor. OAuth tokens grant excessive permissions that bypass traditional security controls. When employees authorize these connections, they're bypassing years of security architecture in a single click.

AI Configuration Drifting

Who's checking if that AI agent has admin access? Is your sensitive data being fed into public training models? Default settings in AI platforms are designed for convenience, not security – creating a ticking time bomb of misconfigurations.

Non-Human Identities Multiplying

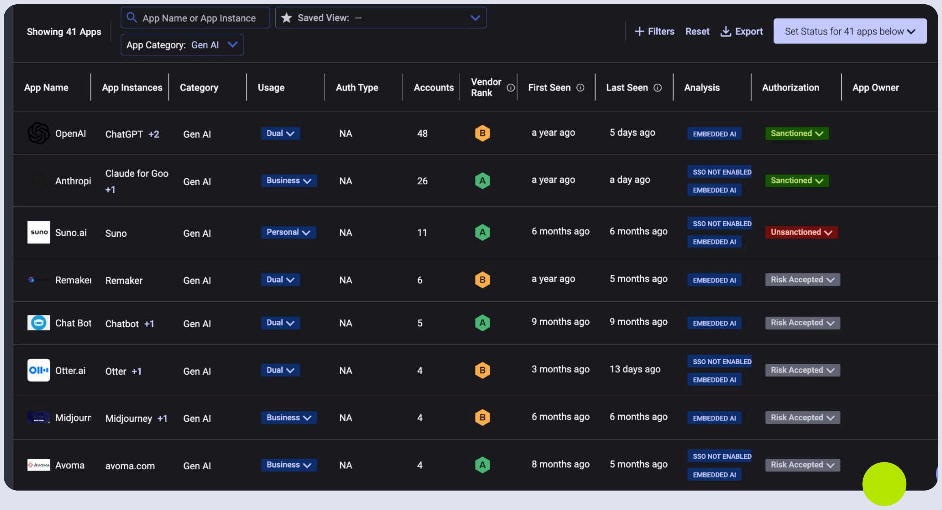
Service accounts, AI agents, and automated processes are proliferating across your SaaS systems. These non-human identities often have privileged access with zero oversight – breaking every identity governance principle your organization has established.

Reco Provides True Agentic AI Security for the SaaS Era

Reco's AI security framework delivers end-to-end control.

Shadow AI Discovery

Uncover shadow AI usage, embedded AI features, and tools like OpenAI, Claude, and Glean — before they become security nightmares. No other platform discovers AI with Reco's precision.

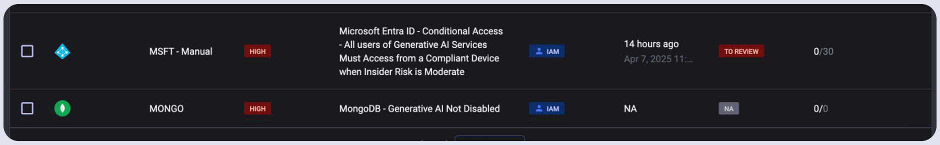


Showing 41 Apps | App Name or App Instance | Saved View: – | App Category: Gen AI | + Filters | Reset | Export | Set Status for 41 apps below

App Name	App Instances	Category	Usage	Auth Type	Accounts	Vendor Rank	First Seen	Last Seen	Analysis	Authorization	App Owner
OpenAI	ChatGPT +2	Gen AI	Dual	NA	48	B	a year ago	5 days ago	EMBEDDED AI	Sanctioned	
Anthropi	Claude for Goo +1	Gen AI	Business	NA	26	A	a year ago	a day ago	SSO NOT ENABLED EMBEDDED AI	Sanctioned	
Suno.ai	Suno	Gen AI	Personal	NA	11	A	6 months ago	6 months ago	SSO NOT ENABLED EMBEDDED AI	Unsanctioned	
Remaker	Remaker	Gen AI	Dual	NA	6	B	a year ago	5 months ago	EMBEDDED AI	Risk Accepted	
Chat Bot	Chatbot +1	Gen AI	Dual	NA	5	A	9 months ago	9 months ago	EMBEDDED AI	Risk Accepted	
Otter.ai	Otter +1	Gen AI	Dual	NA	4	B	3 months ago	13 days ago	SSO NOT ENABLED EMBEDDED AI	Risk Accepted	
Midjourr	Midjourney +1	Gen AI	Business	NA	4	B	6 months ago	6 months ago	EMBEDDED AI	Risk Accepted	
Avoma	avoma.com	Gen AI	Business	NA	4	A	8 months ago	5 months ago	SSO NOT ENABLED EMBEDDED AI	Risk Accepted	

Posture Management at Scale

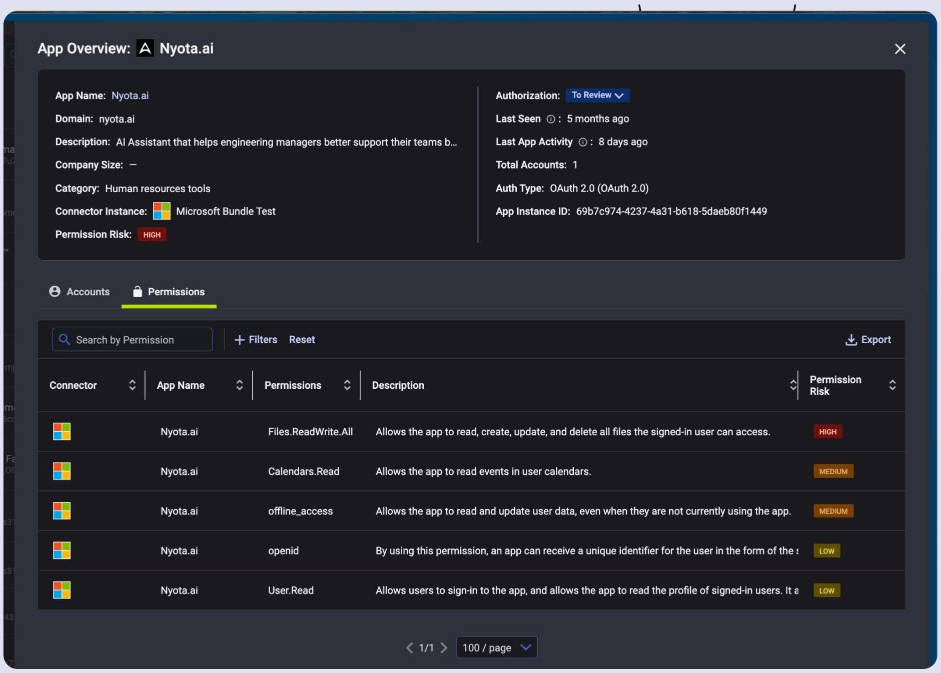
AI settings, permission scopes, and API access policies are continuously evaluated against best practices to prevent drift, overreach, or compliance violations.



□		MSFT - Manual	HIGH	Microsoft Entra ID - Conditional Access - All users of Generative AI Services Must Access from a Compliant Device when Insider Risk is Moderate	IAM	14 hours ago Apr 7, 2025 11:...	TO REVIEW	0/30
□		MONGO	HIGH	MongoDB - Generative AI Not Disabled	IAM	NA	NA	0/0

OAuth Connection Monitoring

Every AI tool leaves a trail. Track every OAuth or token-based integration with third-party AI tools — including what they can access, who authorized them, and what they're doing.



App Overview: Nyota.ai

App Name: Nyota.ai
Domain: nyota.ai
Description: AI Assistant that helps engineering managers better support their teams b...
Company Size: –
Category: Human resources tools
Connector Instance: Microsoft Bundle Test
Permission Risk: HIGH

Authorization: To Review
Last Seen: 5 months ago
Last App Activity: 8 days ago
Total Accounts: 1
Auth Type: OAuth 2.0 (OAuth 2.0)
App Instance ID: 69b7c974-4237-4a31-b618-5daeb80f1449

Connector	App Name	Permissions	Description	Permission Risk
	Nyota.ai	Files.ReadWrite.All	Allows the app to read, create, update, and delete all files the signed-in user can access.	HIGH
	Nyota.ai	Calendars.Read	Allows the app to read events in user calendars.	MEDIUM
	Nyota.ai	offline_access	Allows the app to read and update user data, even when they are not currently using the app.	MEDIUM
	Nyota.ai	openid	By using this permission, an app can receive a unique identifier for the user in the form of the s	LOW
	Nyota.ai	User.Read	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It a	LOW

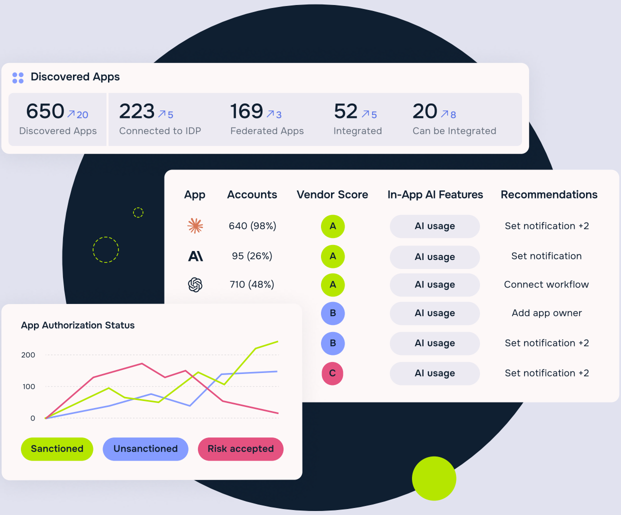
Non-Human Identity Visibility

AI agents operate autonomously across your SaaS systems, often with privileged access. Reco ensures these "non-human" identities play by the same security rules as everyone else.

Why Reco Stands Apart

App Factory™

Our proprietary no-code/low-code engine supports new applications in days rather than quarters, ensuring your security keeps pace with rapidly evolving AI technologies.

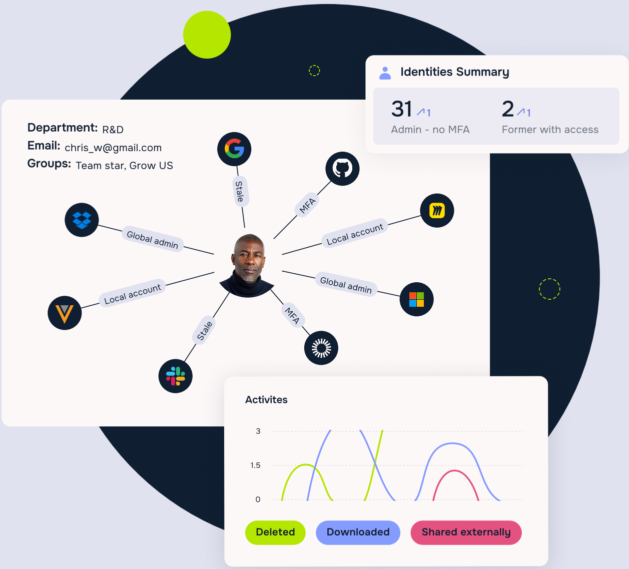


Discovered Apps

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



Identities Summary

31 ↗1 Admin - no MFA

2 ↗1 Former with access

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

Activites

Knowledge Graph

Our advanced contextual engine processes vast amounts of SaaS data in real-time, mapping relationships between users, applications, and data to provide actionable security insights without false positives.

The Business Impact of AI Security

70%

reduction in AI-related security incidents within 90 days of deployment

85%

faster response to AI security threats with automated detection and context-rich alerts

60%

improvement in compliance posture against emerging AI regulations

Outcomes Powered by AI

> Reco gave us the visibility we needed to confidently adopt AI — without risking our data.
>
> **Raphael Meyara, CISO, Altshuler Shaham**

> Before Reco, we didn't even know how many AI tools our employees had connected. Now we have full visibility, posture control, and alerts on AI risk.
>
> **CISO at leading legal firm**

> Reco's AI Access Governance saved us from a critical incident involving a rogue AI bot with excessive file access.
>
> **VP of Information Security at large healthcare system**

AI is already in your environment. Reco makes sure it's secure.

Ready to take control of your AI footprint?
To learn more, email us at info@reco.ai or visit reco.ai