From AI Blind Spots to Complete Agent Control

Thousands of AI agents are operating autonomously across your SaaS ecosystem right now accessing sensitive data, executing actions, and traversing systems without oversight. Unlike traditional SaaS applications, AI agents act independently with broad permissions, exponentially increasing risk when misconfigured or unmanaged.

AI Agent Security gives you complete visibility and control over every AI agent in your environment—from Copilot and ChatGPT to Salesforce Agentforce, Make, n8n, and custom automation tools—all within your unified SaaS security platform.

Solve the AI & Agent Security Blind Spot

AI Sprawl Meets Agent Sprawl

Organizations don't just have hundreds of connected SaaS apps—they have **thousands of connected AI agents** operating in the background.

The Problem

- AI agents operate without direct human interaction
- They possess access to sensitive systems and data
- They connect across multiple SaaS applications
- They operate beyond IT and security team oversight

The Risk

Traditional SaaS security tools weren't built for autonomous AI agents. You can't see what AI agents are running, what permissions they hold, what data they access, or which applications they touch.

Comprehensive AI Agent Security

Complete Inventory

Automatically discover every AI agent across your SaaS ecosystem:

- Microsoft Copilot
- ChatGPT and Claude
- Salesforce Agentforce
- Make, n8n, Zapier
- Custom automation tools
- Embedded AI agents in SaaS apps

Access & Permissions Mapping

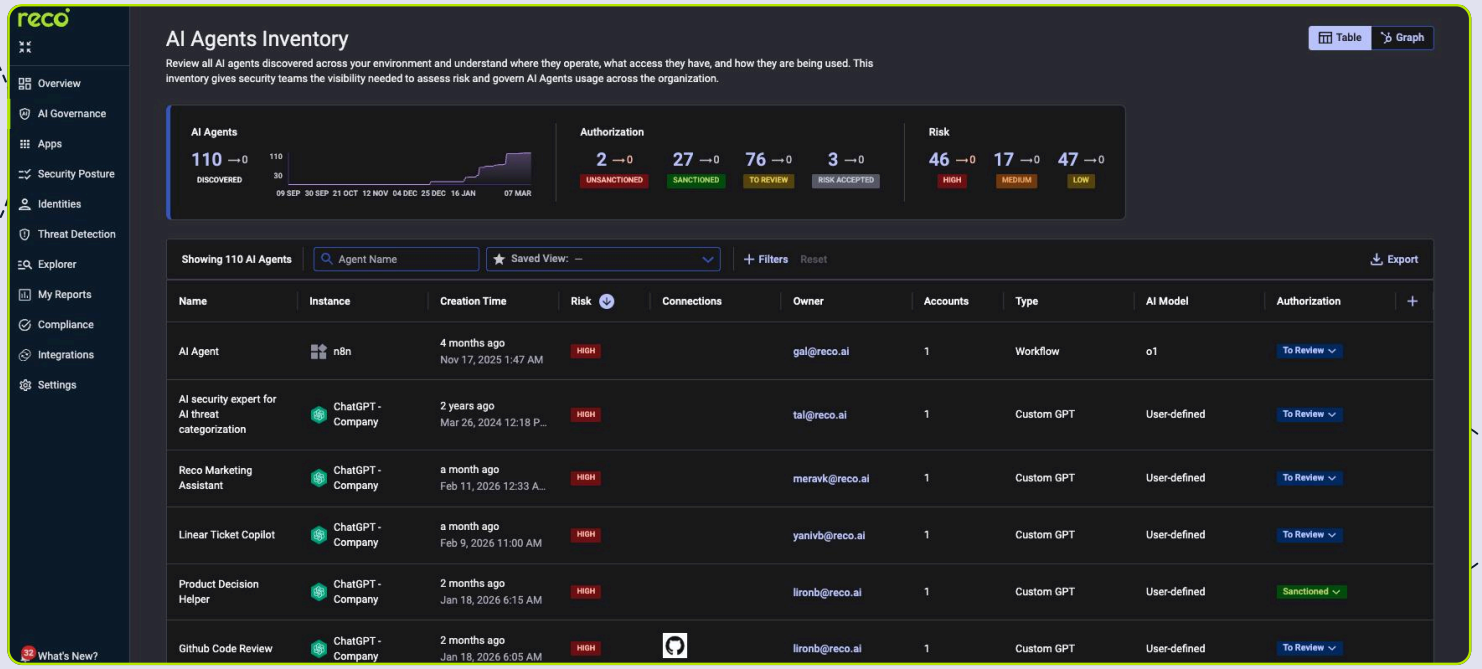
Understand exactly what each agent can do:

- Which identities agents operate under
- What data agents can access
- Which SaaS applications agents connect to
- Permission scope and privileges granted

Risk Identification & Prioritization

Surface the agents that matter most:

- Agents with excessive permissions
- Exposed or shared credentials
- Unauthorized or shadow AI agents
- High-risk vendor connections
- Policy violations and compliance gaps



Guided Remediation & Response

Take immediate action on high-risk agents:

- Revoke excessive permissions
- Disable unauthorized agents
- Trigger automated response workflows
- Integrate with existing security tools and ticketing systems

Governance Controls

Enforce policies across your AI agent landscape:

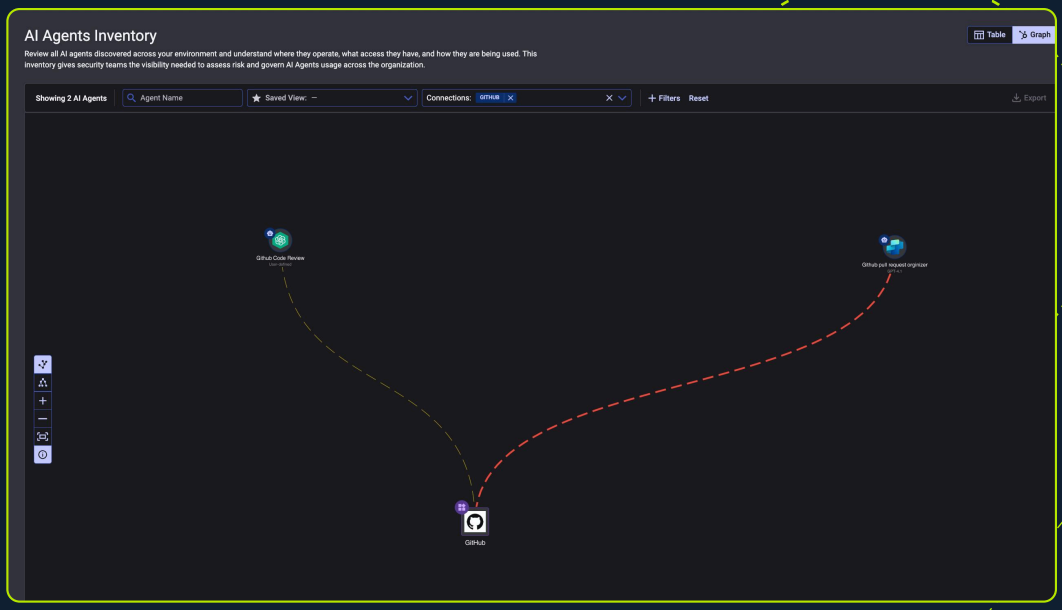
- Sanction approved agents
- Block unauthorized agents
- Apply conditional access policies
- Enforce least-privilege principles
- Maintain compliance requirements

AI Agent Governance & Knowledge Graph

Reco's Knowledge Graph correlates:

- Application connections and data flows
- Security context and risk signals
- Historical behavior patterns
- Cross-system relationships

Why Reco AI Agent Security is Different



Unified Platform

Unlike point solutions, Reco secures SaaS AI, apps, and agents in a single platform. Agent security lives in the same framework you use for SaaS governance.

Built for SaaS

Other AI security tools focus on cloud workloads and model protection. Reco addresses AI sprawl and agent sprawl in SaaS, where modern enterprise risk actually lives.

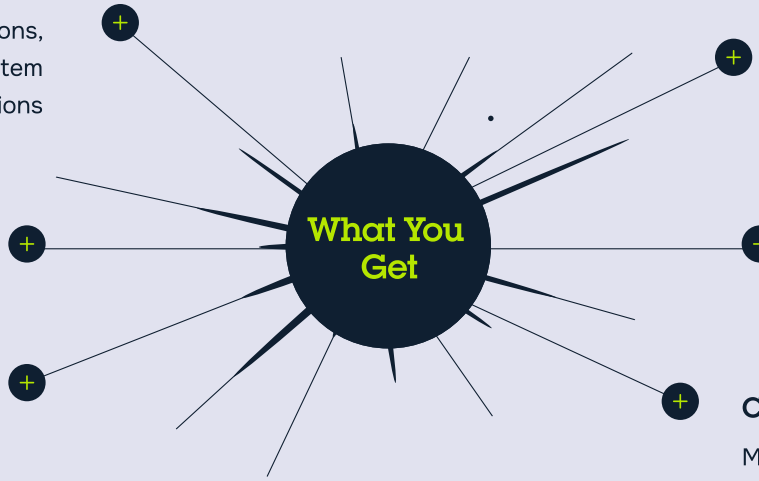
Immediate Value

Available now for existing and new customers with built-in integrations and continuous delivery of new agent support.

Autonomous & Intelligent

Powered by Reco's Knowledge Graph, our platform correlates agent activities with user behaviors, application context, and risk signals. Actionable intelligence, not just visibility.

Key Capabilities at a Glance



Mapping

Visualize agent permissions, data access, and system connections

Risk Assessment

Prioritize agents by risk based on permissions and behavior

Discovery

Automatically inventory all AI agents across your SaaS stack

Remediation

Take action with guided workflows and automated responses

Governance

Enforce policies to sanction, restrict, or block agents

Compliance

Maintain audit trails and demonstrate control for regulators

Business Impact

Reduce Risk

Eliminate blind spots created by autonomous AI agents with excessive permissions and cross-system access.

Accelerate Response

Identify and remediate high-risk agents in minutes with automated discovery and guided workflows.

Enable Innovation

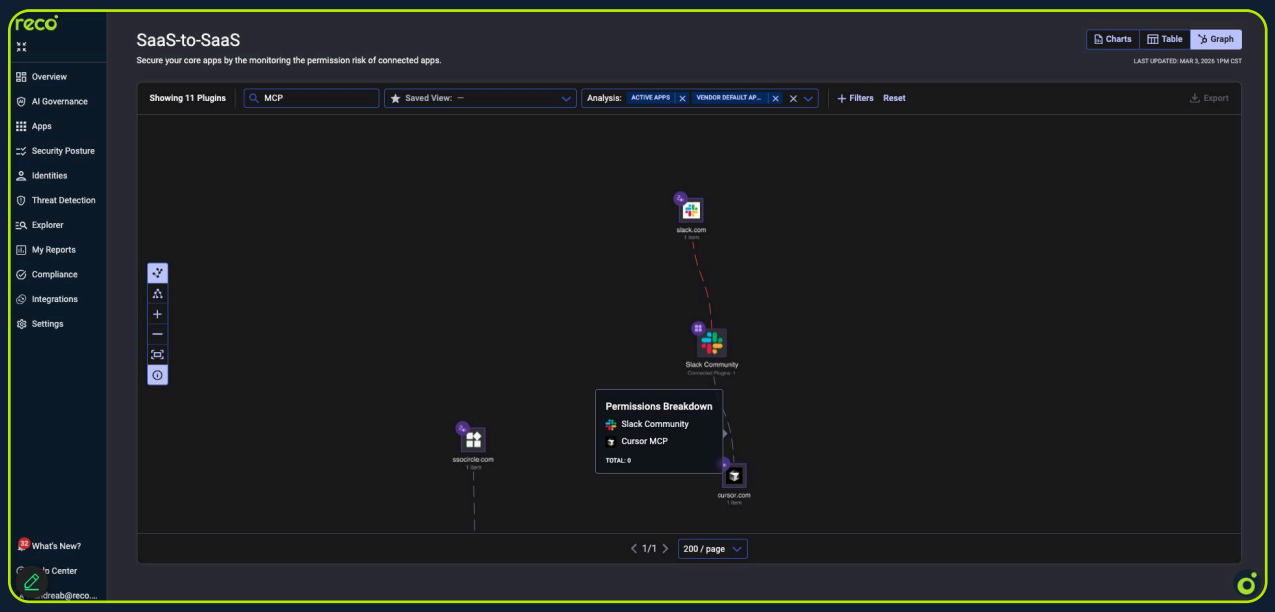
Confidently adopt AI across your organization while maintaining security and compliance controls.

Streamline Operations

Manage AI agent security within your existing SaaS security platform—no new tools or workflows required.

Built on Reco's Knowledge Graph

Reco AI Agent Security is powered by our industry-leading Knowledge Graph:



Context-Rich Intelligence

Understand relationships between agents, identities, applications, and data

Adaptive Learning

Continuously evolve with your dynamic SaaS environment

Unified Intelligence Layer

Correlate insights across all security signals in real-time

Autonomous Processing

Surface actionable insights without manual investigation

Secure Insights without Data Access

Reco AI Agent Security delivers powerful visibility and control while maintaining strict data privacy. Our architecture is designed with rigid boundaries preventing the ability to read or modify your data. All agent metadata and security context remains securely within your tenant, ensuring complete data sovereignty and control.

Support & Availability

Available Now

AI Agent Security is available immediately for existing and new Reco customers as part of the unified SaaS & AI security platform.

Built-In Integrations

Available with support for Copilot, ChatGPT, Salesforce Agentforce, Make, and n8n. Additional agents and custom automation tools added continuously.

Seamless Deployment

No additional infrastructure required. AI Agent Security activates within your existing Reco platform with no performance impact.

Ready to discover and control every AI agent in your SaaS stack?

Contact us at info@reco.ai
Visit reco.ai to learn more about Reco AI Agent Security

About Reco

Reco is the solution trusted by modern enterprises to secure SaaS AI, applications, and agents. Our SaaS & AI security solution provides complete visibility and control across your entire SaaS ecosystem—from traditional SaaS applications to the latest AI agents—enabling security teams to keep pace with the speed of AI adoption while maintaining robust security and reducing risk.