

From Alert Overload to AI-Powered Insight

Optimize your security operations with AI-powered analytics that enhance threat detection, streamline alert processing, and provide contextual intelligence for informed decision-making. Transform your security team from reactive into strategic security leaders with Reco AI Agents that cut through alert noise and deliver actionable insights.

Elevate Your Security Operations



Operational Transformation

Transform your security team from reactive firefighters to strategic interventionalists through AI-driven prioritization that surfaces only what matters across your SaaS environment.



Expertise Amplification

Empower your Tier 1 analysts to perform as Tier 3 analysts by effectively detecting, analyzing, and responding to complex threats without requiring deep expertise across multiple security domains.



Cognitive Load Reduction

Eliminate alert fatigue by having AI independently process complex data, connecting user behaviors, SaaS activities, and risk signals into actionable intelligence.



Streamlined Response Workflow

Accelerate threat remediation with context-rich alerts, clear timelines, recommended action steps, and multi-channel delivery via Reco, SOAR (PAWN, Torq, Tines, Splunk), email, and Slack.

True AI Agents For SaaS Security

Reco AI Agents bridge the SaaS Security Gap through:



Context-Rich Intelligence

Our Knowledge Graph connects the dots between user behaviors, SaaS activities, and risk signals for unmatched contextual understanding.



Autonomous Processing

Unlike basic AI assistants that help with tasks, our agents independently analyze data and surface actionable insights.



Knowledge Graph

Uses adaptive learning to continuously evolve with your dynamic SaaS environment, beyond static rule-based approaches.



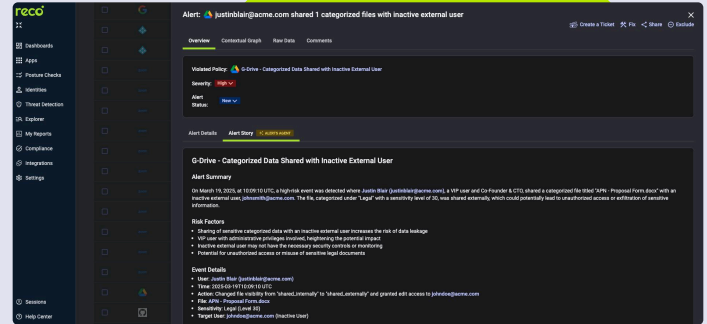
Unified Intelligence Layer

Correlates insights across SaaS activities, user identities, and risk factors in real-time.

Intelligent Automation

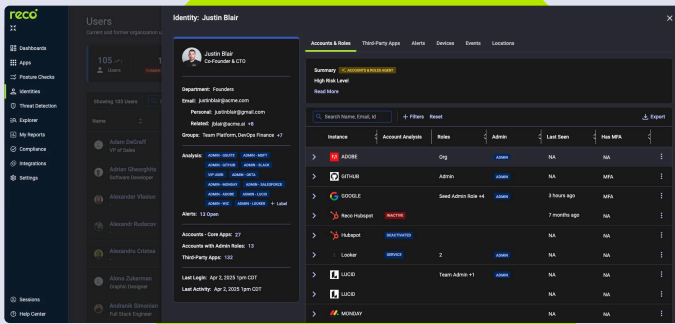
Alerts Agent

- Delivers comprehensive alert timelines with full contextual details for swift remediation
- Implements AI-driven prioritization to filter noise and focus on critical threats
- Provides detailed risk assessments with clear remediation steps
- Facilitates cross-team collaboration through easily shareable, digestible summaries



Identities Agent

- Performs continuous identity risk assessment across SaaS infrastructure
- Identifies excessive permission allocations and unauthorized system access
- Detects former employees with persistent active access credentials
- Monitors local account creation outside centralized identity management



SPECIALIZED Agents

Shadow Application Detection Agent

Discovers unauthorized SaaS tools and AI applications operating outside IT governance to mitigate data exposure risks and compliance violations.

Anomalous Access Pattern Detection Agent

Identifies suspicious user behavior patterns including impossible travel, unusual login times, and atypical resource access to detect potential account compromise or insider threats.

Security Posture Analysis Agent

Continuously evaluates your SaaS security configurations against industry best practices to identify misconfigurations, excessive permissions, and potential vulnerabilities.

Third-Party Application Risk Assessment Agent:

Evaluates the security posture of connected third-party applications based on permissions requested, data access, and known vulnerabilities to quantify supply chain risk.

Policy Implementation Agent

Automates the creation and deployment of security policies based on your organization's risk profile, compliance requirements, and industry standards.

Compliance Verification Agent

Maps your current SaaS security controls to regulatory frameworks including SOC 2, ISO 27001, HIPAA, and NIST CSFR to identify compliance gaps and streamline audit preparation.

Secure Insights without Data Access

Reco AI Agents deliver powerful security insights while maintaining strict data privacy. Our AI models never train on customer data, all information remains securely within your tenant, and our architecture is designed with rigid boundaries preventing the ability to read or modify your data. This zero-access approach allows us to provide sophisticated AI-driven security analytics and remediation recommendations while ensuring complete data sovereignty and control remains with your organization.

AI-Powered Insights Outcomes

NAVAN

"Our Governance, Risk, and Compliance team has experienced improved insight generation and incident routing, enhancing collaboration between Security and SOC departments."

Ricky Waldron

CISO, Navan

"Reco's Knowledge Graph and AI agents have enabled our organization to identify and address identity threats across our SaaS ecosystem in minutes rather than months."

**Chief Information Security Officer,
Fortune 500 Financial Services**

WATCO

"Implementation of Reco AI Agents has reduced our average alert response time by 7 minutes per incident."

Gregg Robbins

CISO, Watco



"The contextual information provided significantly improves operational response by clearly identifying access permissions, systems affected, security implications, and required remediation steps, resulting in more effective action."

Neda Pitt

CISO, Belk

Ready to transform
your security
operations with
AI-powered insights?

Contact us at
info@reco.ai