Reco
SaaS Security

SaaS Security Solution Comparison Guide

www.reco.ai

Feature	Reco	AppOmni	Obsidian	Adaptive Shield	Grip Security
SaaS App Coverage					
User Behavior Analytics					
Configuration Management					
Threat Detection					
Compliance					
Visibility					
Insider Threat Prevention					
Configuration Drifts Detection					
Shadow Apps Discovery					
SaaS to SaaS Discovery					
Identity Posture Management					
Full Security Context					
Notification Workflows					
API to Extend Security to Any SaaS App					
Rapid App Integrations on Request					
Full Lifecycle SaaS Security					

SaaS App Coverage: Broad support for SaaS applications—including Salesforce, Microsoft 365, and Google—as well as department-specific SaaS apps such as Figma, DocuSign, and GitHub. New integrations made available on a regular basis to keep up with the pace that organizations scale. Integrations are comprehensive, offering full visibility into shadow apps, GenAI tools, and 3rd-party apps, posture checks, compliance mapping, access governance of identities, prioritized alerts, and more.

Visibility: Gain a crystal-clear view into your entire SaaS attack surface including connected SaaS applications (such as sanctioned, GenAI tools, and shadow applications), 3rd-party apps, associated identities, their permission level, and interactions across your SaaS apps.

Shadow Apps Discovery: Gain visibility into connected SaaS applications that have not been approved for use, their utilization by employees, and data access. Assess the security risks including third-party risk management, implement strong access controls, and receive alerts for potential points of exposure.

SaaS to SaaS Discovery: Gain visibility into applications connected to your SaaS apps—including 3rd-party, 4th-party, and 5th-party—their utilization by employees, and data access. Assess the security risks including third-party risk management, implement strong access controls, and receive alerts for potential points of exposure.

Configuration Management: Ensure that SaaS applications are securely configured and continuously monitored. This includes creating security baselines, automating configuration checks, detecting misconfigurations, and managing access controls to improve security posture. Partner with a tool that offers hundreds of posture checks with actionable recommendations across your entire SaaS estate. Be prepared for an IT audit by tracking changes in configuration settings.

Configuration Drifts Detection: Assess posture across security controls continuously using hundreds of one-click checks that score alignment of your critical SaaS apps against recommended security configurations. Be alerted of configuration drifts from baseline security posture.

Compliance: Maintain compliance by aligning security practices with regulatory requirements. Continuously verify your SaaS security posture against out-the-box industry frameworks such as SOC 2 Type 2, CIS, NIST CSF, ISO 27001, PCI, HIPAA, HITRUST, and more.

Identity Posture Management: Unify identities across all applications and monitor for suspicious behavior based on locations, IP addresses, devices, activities, and more.

User Behavior Analytics: Analyze user behavior to detect anomalies that may indicate security threats, such as account compromise or insider attacks. Establish a baseline of normal user activity and flag deviations from that baseline, to enable quicker response to suspicious activities by focusing on how users interact with systems and data.

Insider Threat Prevention: Enforce access control policies, detect suspicious behavior, gain visibility into MFA utilization, and revoke permissions for identities who misuse access before they can cause harm. Have this functionality for all apps managed from a single console.

Full Security Context: Utilize security context automatically mapped and coded using AI to gain a full picture of users and usage. Utilize this security information to quickly respond to security incidents appropriately.

Threat Detection: Send rapid and accurate alerts to your SIEM or SOAR based on new and emerging attack vectors. Access an incident response deep dive into user context and activity. Gain a snapshot of current security coverage compared with the MITRE ATT&CK® framework, including attack techniques mitigated by activated policies.

Notification Workflows: Improve security incident response by integrating automated detection into workflows with your existing tools like Slack, ServiceNow, and Jive. Ensure that alerts are quickly sent to the right team for their response.

APIs to Extend Security to Any SaaS App: Extend SaaS security to any new SaaS application that your organization onboards—including Salesforce, Microsoft 365, and Google—as well as department-specific SaaS applications such as Figma, DocuSign, and GitHub. Support is extended using APIs, no agent in line. Fully connected in minutes, the platform then ingests each layer across SaaS apps, identities, and metadata with zero impact on performance. Once data is aggregated and normalized, posture checks, identities, and then data are delivered.

Rapid App Integrations on Request: Reco is the only SaaS Security solution to release 3-5 app integrations per week (10x quicker than other SaaS security solutions). Reco prioritizes new SaaS applications based on customer requests, and our customers have direct access to our SaaS experts, best practices, and solution architects that accelerate delivery within the platform.

Full Lifecycle SaaS Security: Support the entire lifecycle of securing a SaaS application, from app discovery (including core apps, shadow apps, GenAI, tools, and 3rd-party apps), posture management and compliance, identity access, and threat detection and response.

Start Securing Your Entire SaaS Lifecycle

Reco is a leading SaaS security solution that is redefining the way enterprises secure their SaaS environment by using a full lifecycle approach to security. Connecting in minutes via API, Reco discovers every app (including shadow apps, GenAI tools, and 3rd-party apps), its identities, and their actions to seamlessly prioritize and control the risks in the SaaS ecosystem.

Reco can help CISOs provide the right tools to their security, engineering, and IT teams to prevent the risk of exposure to breaches, by understanding their SaaS applications and identities, while controlling access and permissions. Reco draws security context around persona, actions, interactions and relationships to other users to identify suspicious human behavior patterns. It also enables alerts on exposure from misconfigurations, insider risk, over-permissioned users and compromised accounts.

Reco uses a low-code/no-code development approach to add a few SaaS application in 3-5 days. With Reco, security teams have the insight they need to take swift action to mitigate risk and the right advisors that can accompany you on your growth path.

You can learn more or book a demo at www.reco.ai