



## SaaS Security Posture Management (SSPM) Data Sheet

# Strengthen your SaaS & AI security posture with Nudge Security

Nudge Security delivers continuous security posture findings and guided remediation for **every** SaaS and AI app in your environment—not just the ones IT already manages. Get complete SaaS and AI coverage in minutes, not months.

### SSPM for your *entire* SaaS & AI ecosystem

Conventional SSPM solutions rely on direct API integrations with SaaS environments to monitor for security misconfigurations and other risks. This means you must *know* which SaaS and AI tools are in use *and* have administrative access to each one. Plus, API functionality is inconsistent. As a result, SSPMs typically cover only a fraction of the full SaaS ecosystem, leaving many shadow SaaS and AI apps, app-to-app integrations, and identities unmonitored and at risk.

Nudge Security takes a different approach. Through patented, perimeterless SaaS and AI discovery, it surfaces risk insights and security posture findings across your entire ecosystem—known *and* unknown—from day one. No network proxies, endpoint agents, or SaaS API integration required to get started.

#### Why Nudge Security for SSPM?

**More value:** Our complete SaaS & AI security governance solution goes beyond standalone SSPM solutions.

**Faster ROI:** Surface shadow SaaS and AI risks with a simple 5-minute setup.

**Holistic security posture management:** 360° risk posture that spans vendors, identities and access, integrations, configurations, and more.

**Full context:** Findings and remediation workflows that understand **your** business context, users, and IT policy.

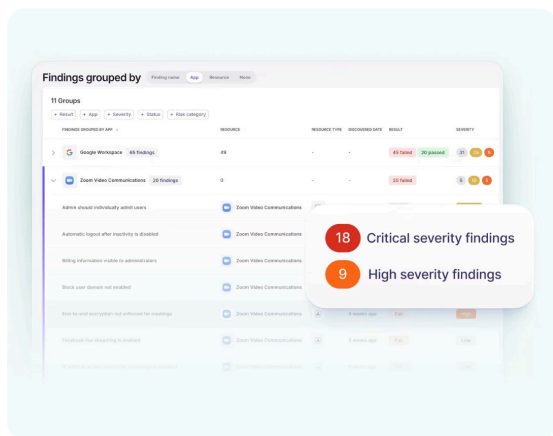
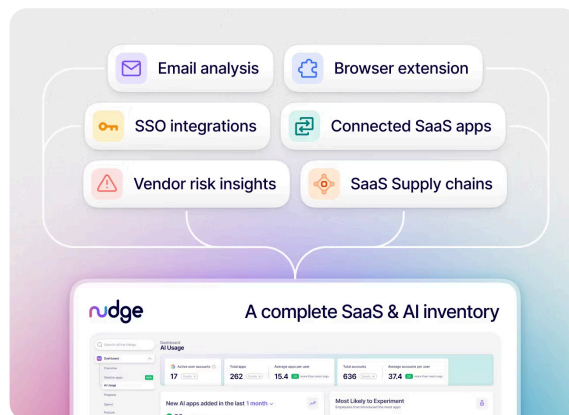
“Nudge Security has been a big win for our security program at Reddit. **Within hours of deployment**, we gained complete visibility into our SaaS footprint across the organization. It's rare to find a solution that's both incredibly powerful and remarkably easy to use.”

—[Fredrick Lee, CISO, Reddit](#)

## Key Features & Capabilities

### Perimeterless SaaS & AI discovery

Multiple vantage points: workspace provider connections (Google Workspace, Microsoft 365), a lightweight browser extension, and connected apps (API) provide continuous visibility and control beyond the network edge.

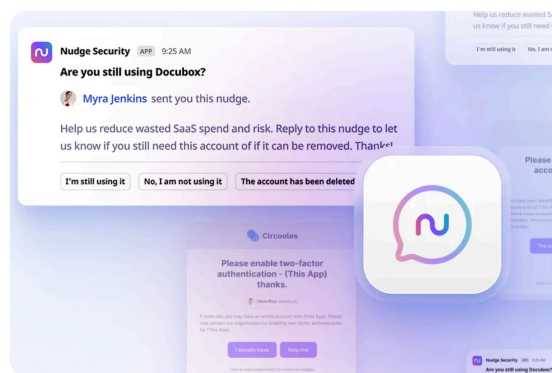


### Context-aware posture findings

Your approved app list, business criticality, data sensitivity, app owners, vendor breach records, and other internal risk factors enrich risk insights, security posture findings, and alerts.

### Last-mile remediation

Where API automation falls short, Nudge Security provides smart human-in-the-loop remediation workflows that guide the right business stakeholders with step-by-step instructions and then automatically verifies the fix, alleviating manual security work and enabling a faster time to resolution.



## 360° SaaS & AI security posture management

While SSPM providers often highlight the size of their SaaS connector libraries or speed of building new or custom connectors, it's not always clear what's actually being monitored. SaaS API limitations and inconsistent availability mean coverage varies significantly. Some SaaS providers restrict API access to enterprise tiers only.

Nudge Security overcomes these limitations through multiple vantage points: workspace provider connections (Microsoft 365, Google Workspace) and a lightweight browser extension add to our growing library of API-based connected apps.

The table on the next page details the SaaS and AI assets, risk insights, events, and security posture findings Nudge Security monitors and what coverage is available.

# SaaS & AI Security Posture Management Coverage

	Any SaaS or AI App	Tier 2 SaaS & AI Apps	Tier 1 SaaS & AI Apps
	<i>Workspace provider- &amp; browser-based discovery, risk assessment, and posture findings for over 200,000 SaaS &amp; AI apps. No connected apps (API) required.</i>	<i>Connected apps (API) provide deeper app context and identity findings for 50+ SaaS &amp; AI apps. See the full list <a href="https://www.nudgesecurity.com/integrations">www.nudgesecurity.com/integrations</a></i>	<i>Vendor-specific misconfiguration monitoring for Okta, Zoom, Github, Atlassian, Cloudflare, Netsuite, Salesforce, ServiceNow, Slack, Snowflake, Workday, and more.</i>
<b>SaaS &amp; AI app discovery</b>			
App Discovery (Shadow + Sanctioned)	✓	✓	✓
Instance Discovery	✓	✓	✓
Accounts Discovery	✓	✓	✓
Account Authentication Methods	✓	✓	✓
SSO Status	✓	✓	✓
App Owner ("Technical Contact")	✓	✓	✓
SaaS Spend Discovery	✓	✓	✓
<b>Third-party vendor risk</b>			
Vendor Security Insights/Alerts	✓	✓	✓
Supply Chain Monitoring	✓	✓	✓
Supply Chain Breach Alerts	✓	✓	✓
<b>Identity risk</b>			
User Activity Monitoring	✓	✓	✓
Login Activity Monitoring	✓	✓	✓
Unused Account Detection	✓	✓	✓
Shared Account Detection	✓	✓	✓
SSO Enrollment	✓	✓	✓
Weak/Reused Password Detection	✓	✓	✓
MFA Bypass Detection	✓	✓	✓
User Role Detection	-	✓	✓
Excessive Permission Detection	-	✓	✓
Privileged Account Monitoring	-	✓	✓
<b>App-to-app Integration &amp; NHI risk</b>			
API Key Detection	✓	✓	✓
AI Integration Detection (MCP)	✓	✓	✓
Service Account Detection	✓	✓	✓
OAuth Grant Detection	✓	✓	✓
Marketplace apps, webhooks, SSH keys and other integrations	-	✓	✓
<b>Data access risk</b>			
File Upload Monitoring	✓	✓	✓
AI Conversation Monitoring	✓	✓	✓
Data Access Findings	✓	✓	✓
Data Retention Findings	-	-	✓
<b>Vendor-specific configuration risk</b>			
App Misconfiguration Monitoring	-	-	✓
Security Config Findings	-	-	✓
Access Control Config Findings	-	-	✓
MFA Configuration Monitoring	-	✓	✓
<b>Alerting &amp; remediation workflows</b>			
Closed-Loop Resolution Workflows	✓	✓	✓
Customizable Alerts & Notifications	✓	✓	✓
Just-in-time Policy Guardrails	✓	✓	✓
Human-in-the-loop Automation	✓	✓	✓