

Falcon Shield: Comprehensive AI Agent and SaaS AI Security Management

Secure AI now to protect your future ecosystem

As organizations rapidly embrace AI within their SaaS applications and deploy AI agents throughout their environments, securing these powerful tools becomes increasingly critical. The proliferation of AI capabilities — from large language models to autonomous agents — introduces new security challenges that require comprehensive visibility and control.

Key benefits

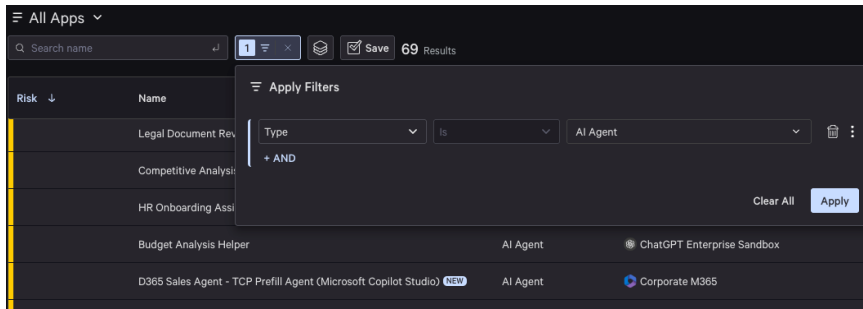
CrowdStrike Falcon® Shield provides comprehensive visibility and security management for AI agents across your organization's SaaS applications and platforms.

Complete Visibility and Control

Gain visibility into your AI agent ecosystem in a single dashboard, revealing what agents are doing, what they're accessing, and who directed them to act. Falcon Shield continuously monitors AI deployments across SaaS platforms, mapping each agent's capabilities and system connections while documenting all interactions to uncover shadow AI before it becomes a threat.

Risk Reduction and Compliance

Proactively identify and remediate AI security risks before they impact your business. Falcon Shield incorporates built-in AI tools that assist with security audits and reporting, supporting compliance tracking and providing visibility to aid in aligning with security frameworks.



Multi-Platform Coverage

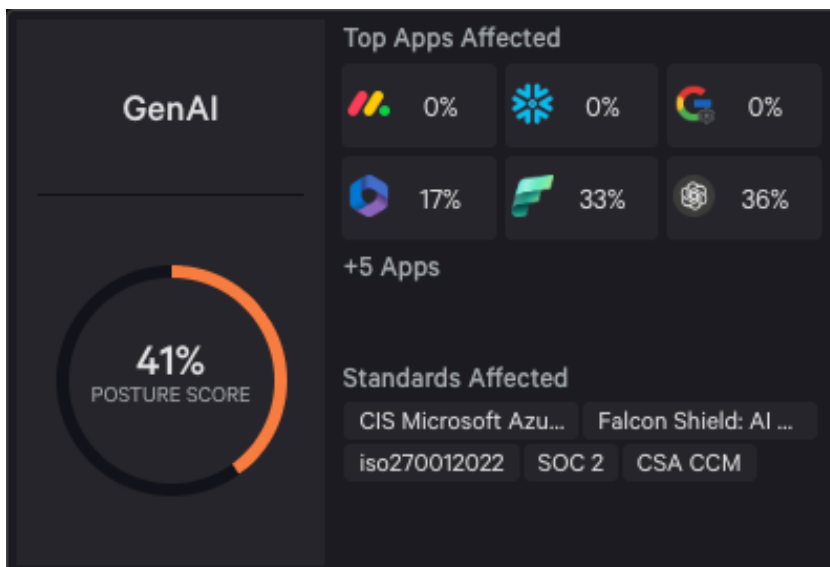
Secure your AI landscape with deep visibility across major SaaS platforms including Microsoft 365, OpenAI, Zoom, and Snowflake through native integrations. Discover all GPTs and Codex agents — including those in ChatGPT Enterprise — while extending protection to development environments where AI agents can access repositories and interact with external systems.

Automated Security Management

Automate the full security lifecycle with continuous monitoring that instantly identifies risky AI agent behaviors and triggers immediate containment actions without manual intervention. Leverage the unified CrowdStrike Falcon® platform to automatically disable compromised agents, revoke excessive permissions, and create tracking tickets — transforming labor-intensive security management into streamlined, policy-driven enforcement.

Example Risk Scenarios

- Unauthorized ChatGPT OAuth connections with high-risk permissions
- AI agents lacking proper access restrictions
- Unmanaged AI feature deployment across platforms
- Data exposure through unsecured AI integrations



Key capabilities

Falcon Shield delivers enterprise AI platform security as a module of the unified Falcon platform.

AI Agent Discovery and Management

Gain complete visibility into your organization's AI footprint with comprehensive discovery capabilities:

- Unified directory of all AI agents across SaaS platforms
- Continuous monitoring of AI access permissions and system connections
- Detailed tracking of agent activities, capabilities, and data interactions
- Real-time security posture assessment with automated remediation workflows

ChatGPT Enterprise Monitoring

Secure your most powerful AI tools while maintaining full audit capabilities with native OpenAI integration:

- Real-time streaming of user conversations and agent interactions
- Complete audit trails documenting all AI agent activities
- Comprehensive GPT discovery in ChatGPT Enterprise with usage analytics and risk assessment
- Continuous monitoring of our systems to maintain compliance

ChatGPT

Status

Unclassified

Risk level

High

Integration

M365 Lab

Overview

Scopes (6)

Consenting Users (1)

Journal

Q Search

Clear

Scope	Write	Read	Access L... ↓
▼ AllSites.Read	⊘	⊙	High
Allows the app to read documents and list items in all site collections on behalf of the signed-in user			
▼ Files.Read.All	⊘	⊙	High
Allows the app to read all files you can access.			
> MyFiles.Read	⊘	⊙	Medium
> Files.Read	⊘	⊙	Medium
> User.Read	⊘	⊙	Low
> offline_access	⊘	⊘	Low

OAuth-Connected AI Discovery

Identify shadow AI and risky integrations before they become security incidents:

- Automatic detection of AI applications connected through OAuth
- Continuous monitoring across Microsoft 365, Google, and Salesforce ecosystems
- Risk assessment of permission scopes and access levels
- Detailed tracking of user access patterns and authentication methods

Development and Data Platform Security

Secure AI throughout the development lifecycle and across data platforms where sensitive information resides:

- Comprehensive security controls for GitHub Copilot and Hugging Face
- Restriction capabilities for code suggestions from public repositories
- Cross-organization access management and governance
- Controlled AI feature deployment with security guardrails
- Integrated security for Snowflake Cortex, Microsoft Fabric, and other data platforms

Status	Security Check	Integration	Impact ↓
	GPTs with Action Capabilities	 ChatGPT Enterprise Sandbox	● High
	Prevent Unauthorized Agent Actions [Copilot Studio]	 Power Platform + Copilot Agent Studio	● High
	Ensure User-Defined Action Messages [Copilot Studio]	 Power Platform + Copilot Agent Studio	● High
	AI Agents Authentication Bypass	 Power Platform + Copilot Agent Studio	● High
	AI Agents with Connected Agent Access [Copilot Studio]	 Power Platform + Copilot Agent Studio	● High
	GPTs with Cross-Organization Access	 ChatGPT Enterprise Sandbox	● Medium
	GPTs with Web-Search Access	 ChatGPT Enterprise Sandbox	● Medium
	Disable Gemini Access for Unlicensed Users	 G-Workspace Admin Plane	● Medium
	Number of Sensitivity Labels [Purview]	 Corporate M365	● Low
	Users With Copilot For M365 License	 Corporate M365	● Low
	AI Assistant Access	 Project Mgmt (Monday)	● Low
	Disable Creation and Sharing of Data Agent Item Types	 Data Eng (Microsoft Fabric)	● Low
	Scope Copilot Access to AI-Prepped Items Only	 Data Eng (Microsoft Fabric)	● Low
	AI Assistant Access	 FS	● Low
	Disable Legacy User API Key Creation	 AI Lab (OpenAI)	● Low
	Roles With Privilege To Snowflake AI	 Data Warehouse (Snowflake)	● Low

Learn more about securing your AI environment:

[How CrowdStrike Secures AI Agents in SaaS Environments](#)

[CrowdStrike ChatGPT Enterprise Compliance API Integration](#)

Contact your CrowdStrike representative to learn more about securing your AI future with Falcon Shield.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: <https://www.crowdstrike.com/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

