

Proofpoint AI Security for Discovery



Gain a Comprehensive, Continuous AI Asset Inventory across the Organization

AI in the enterprise operates across every form factor at once. Employees work in desktop clients such as Claude Desktop, ChatGPT, and Cursor, use coding agents, command-line interface (CLI) tools, browser extensions, and IDE plugins, and connect them to enterprise systems through Model Context Protocol (MCP) servers, connectors, and agent skills they configure themselves. Development teams deploy custom agents across Kubernetes, serverless, and managed platforms, and SaaS vendors embed agents in the applications the business depends on. Much of this activity never passes through a network proxy or a browser, and software inventories do not record which models an application calls, which MCP servers it connects to, or which data it accesses.

Proofpoint AI Discovery and Inventory gives security teams complete, continuous discovery of all AI in use across the enterprise. It discovers AI applications, agents, thick clients, CLI tools, browser extensions, IDE plugins, connectors, agent skills, local models, and MCP servers, and records how each one connects to models, tools, and enterprise data. Discovery operates at the system level on endpoints and at the workload level in the cloud, so coverage holds across every browser mode, network path, and agent framework without developers instrumenting their code. Every discovered asset is risk-scored and attributed to the user or process behind it.

Security Teams Can Act on AI Risk as Soon as Discovery Is Deployed

Security Teams See All AI in Use, Sanctioned and Unsanctioned

Discovery surfaces AI applications, agents, and MCP servers across endpoints, SaaS applications, and cloud workloads, including AI features embedded in approved applications and the connectors and skills employees add to their assistants.

Risk Is Prioritized before a Single Policy Is Written

Each AI service carries a risk profile built from its data handling, retention, vendor trust posture, tier of service, access scope, and usage, and agents and MCP servers carry their own risk classification, so security teams know which services, agents, and servers warrant action first.

Audit Evidence Is Ready when Auditors, Regulators, and Boards Ask for It

Per-provider compliance status and exportable inventory reports document which AI the organization uses, who uses it, and what data it accesses.

Deployment Takes Hours and Requires Nothing from Development Teams

The security team deploys and controls discovery directly, with no application code changes and no SDK integration.

Discovery Covers Every Form Factor of Enterprise AI

Proofpoint discovers and inventories AI across every category below, on employee devices and in cloud environments.

Category	Coverage
AI Applications and Services	Web-based AI services, AI-native SaaS applications, and AI features embedded in sanctioned SaaS applications, including Google Workspace, Databricks Genie, Workbuddy, Madison AI, Doximity, and OpenEvidence, with AI-native services distinguished from AI-enabled features. Custom and private AI providers are added through HTTP Archive (HAR) capture.
Thick Clients	Claude Desktop, ChatGPT for macOS and Windows, the Microsoft Copilot desktop app, Cursor, Windsurf, and other desktop AI applications, along with the MCP servers and connectors configured inside each one.
Coding Agents and CLI Tools	Claude Code, OpenAI Codex, GitHub Copilot in VS Code, and other AI coding agents and CLI tools that call models directly from developer workstations.
Browser Extensions and IDE Plugins	AI browser extensions and IDE plugins, with discovery maintained in incognito and private browsing modes.
Assistants, Plugins, Connectors, and Agent Skills	GenAI assistants, plugins, connectors, and agent skills inventoried as distinct object types, with each skill scored on source trust and permitted actions and inspected for high-privilege commands and hardcoded secrets.
MCP Servers	Local, remote, and hybrid MCP servers across devices, networks, and cloud environments, mapped to the clients that connect to them, the tools they expose, the data sources they access, and whether they enforce authentication and encryption. Discovered servers onboard dynamically into the MCP server registry.
Locally Hosted Models	Ollama and other local model runtimes on employee devices.
Custom Agents and AI Applications	Agents built with LangChain, LangGraph, CrewAI, AutoGen, or custom code, deployed on Kubernetes (EKS, AKS, GKE), Linux virtual machines, serverless functions, and managed platforms such as Amazon Bedrock, n8n, and Ray, with the LLM providers, tools, MCP servers, and data sources each agent uses.

Every Discovered Asset Is Risk-Scored and Attributed to a User or Process

Each AI service is profiled by its data flows, vendor trust posture, retention policy, access scope, tier of service, model type, and usage volume, and each provider carries a full risk dossier with compliance status and a view of its capabilities and the policies it supports. Agents are classified as low, high, or critical risk based on their tool access, data connectivity, and behavioral scope. For agents on employee devices, posture assessment identifies which LLM endpoints each agent calls, which MCP servers it has configured and whether they require authentication

and encryption, whether credentials are stored outside organizational control, and which tools and data sources fall within its scope. Findings are unified across employee AI access, agents, and AI infrastructure, carry prescribed remediation, and export to Proofpoint data security. Usage is attributed to the users, teams, and processes behind each asset, so security teams know which parts of the organization adopt each AI tool and where risk is concentrated.

Discovery Maps How AI Connects to Enterprise Data and Systems

A list of AI services does not show exposure, so Proofpoint records the relationships between assets. Inventory captures each agent’s LLM providers, tools, MCP server connections, data sources, and external service calls. The application

graph maps agent-to-agent and agent-to-tool connections from observed runtime activity, which surfaces architectural risk such as an agent that holds access to sensitive internal data along with the ability to send data externally.

Deployment Requires No Code Changes and No Developer Involvement

Discovery produces one consistent inventory across every deployment method. The Proofpoint endpoint agent discovers AI at the system level on macOS, Windows, and major Linux distributions, covering desktop applications, CLI tools, and browsers in every mode, with a macOS driver for applications that do not support proxy auto-configuration (PAC). The endpoint agent and browser extension are unified with Proofpoint data security, so organizations already using Proofpoint data security add AI discovery to their existing deployment. The browser extension covers browser activity where no endpoint agent is deployed, agentless coverage extends through secure enterprise browsers and Slack

and Microsoft Teams plugins, and hardened proxy chaining provides discovery through existing secure access service edge (SASE) proxies. Where an organization does not permit a persistent agent, a dissolvable agent collects a point-in-time inventory and removes itself.

In the cloud, kernel-level eBPF instrumentation deploys as a DaemonSet on Kubernetes and as a Linux service on virtual machines, and the AI Security Gateway covers serverless functions and managed platforms. None of these methods requires application code changes, SDK integration, or participation from development teams.

Organizations Often Upgrade from Discovery to Full Runtime Enforcement

Organizations often license discovery across the workforce, add runtime inspection and enforcement for the users and agents that need it first, and expand as their policies mature. Because the endpoint agent and proxy chaining

deliver discovery and enforcement through one deployment, the upgrade to full runtime inspection and enforcement across applications, agents, and MCP servers requires no new deployment.

Complete Discovery Is the Foundation of Proofpoint AI Security

Proofpoint AI Discovery and Inventory gives security leaders a continuously updated account of all AI in the enterprise, the data and systems it accesses, and the risk each asset carries. To see discovery in your environment, request a demo.

Get the Details

Talk to your Proofpoint or Microsoft account team to structure your private offer. They’ll walk you through pricing, terms, and next steps.



About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint’s collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently. Learn more at www.proofpoint.com

Connect with Proofpoint: [LinkedIn](#)

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.