

ISPM AI Agent Discovery: Strategy & Interface

Executive Summary

The rapid rise of autonomous AI agents has created a **visibility gap** where non-human identities access sensitive data without oversight. **Okta ISPM** closes this gap through a dual discovery strategy:

- **Shadow Apps - Unknown Agents & Apps:** Detects when users grant external AI tools access to corporate platforms via the browser.
- **AI Agent Platforms Visibility:** Uses API integrations with enterprise builders to inventory sanctioned agents, map permissions, and assign human accountability.

Pillar 1: Unknown Agents and Apps – Okta Browser Plugin

The Use Case: Employees independently adopt external AI tools and authorize them to access corporate data via OAuth without IT oversight, leading to unmanaged data exposure.

CLIENT APP	RESOURCE APP	BROWSER USERS	CATEGORY	LAST SEEN	FIRST SEEN	ACTIONS
ChatGPT	Google Drive (Acme.google.com)	18	AI	2 months ago	2 months ago	Details & Actions
Salesforce	Google Workspace	16	---	2 months ago	2 months ago	Details & Actions
Microsoft Copilot	api.linear.app/oauth/authorize	16	AI	2 months ago	2 months ago	Details & Actions
nla.zapier.com/oauth/	Google workspace	12	---	2 months ago	2 months ago	Details & Actions
n8n	miro.com/oauth/authorize	10	AI	4 months ago	4 months ago	Details & Actions
Jira	Slack	2	---	4 months ago	4 months ago	Details & Actions
retool.internal.corp/	api.stripe.com/oauth/au...	2	---	4 months ago	4 months ago	Details & Actions
GitHub	Slack	2	---	12 months ago	12 months ago	Details & Actions
Slack	Acme.salesforce.com	2	---	12 months ago	12 months ago	Details & Actions

Business Value

- **Detect Shadow Apps:** Identifies unauthorized AI tools that were not added by the Okta Admin as an approved SSO app.
- **Scope Visibility:** Reveals exactly what data an external agent can access, such as Google Drive or Slack.
- **Contextual Risk:** Quantifies risk by tracking the number of users involved and the

specific permissions (read, write, execute) granted.

Technical Overview: Browser OAuth Grants

- **The "How":** The **Okta Secure Access Monitor** plugin captures OAuth grant telemetry as users or non-human identities log in or grant permissions.
- **Navigation:** In the sidebar, navigate to **Inventory > NHIs & AI Agents > Browser OAuth grants**.
- **Interface:** Each row represents a connection between a **Client App** (e.g., ChatGPT) and a **Resource App** (e.g., Google Workspace).
- **Detailed Drawer:**
 - **Browser Users Tab:** Lists every individual who granted access, their "Last Seen" activity, and authorized **Scopes**.
 - **Actions Tab:** Offers remediation steps: **Register the AI agent in Okta**, **Connect to Okta SSO**, or **Contact the users or block access**.

Pillar 2: AI Agent Platforms Visibility and Risk Analysis

The Use Case: While organizations build agents in approved platforms, security teams are held accountable for a "blast radius" they cannot actually audit or see in one place.

The screenshot shows the Okta AI Agents dashboard. On the left, there's a sidebar with navigation links like Dashboards, Issues, Inventory, Accounts, NHIs & AI Agents (which is currently selected), Service accounts, Workload identities, and AI Agents. The main area has a search bar at the top. Below it, there are two cards: 'Agents by agent builder' and 'Agents by platform resources'. The 'Agents by agent builder' card shows 32 AI Agents of 36, with a bar chart for each builder. The 'Agents by platform resources' card shows counts for SharePoint, Salesforce, OneDrive, and PowerPoint. Below these cards is a table with columns: AGENT NAME, OWNERS, PERMISSIONS, PLATFORM RESOURCES, STATUS, and MANAGE IN OKTA. The table lists various AI agents with their owners, permission counts, platform resources (represented by icons), status (Active), and a 'Register' button. At the bottom, there are pagination controls for rows per page (10) and pages (1-10 of 88).

Business Value

- **Discovery & Detections:** Provides a central inventory for agents, permissions, owners, and risks across platforms like **Microsoft Copilot Studio** and **Salesforce Agentforce**.
- **Permission Transparency:** Surfaces specific internal "Roles" and "Scopes" that define the agent's power.
- **Accountability:** Maps every agent to a specific human **Owner** or **Sponsor** to ensure accountability.

Technical Overview: AI Agents

- **The "How":** Direct API-to-API connectors ingest critical security metadata, including agent names, status, and the human identities behind them.
- **Navigation:** In the sidebar, navigate to **Inventory > NHIs & AI Agents > AI Agents**.
- **Interface:** Each row represents an autonomous agent, showing its **Agent Builder**, **Owners**, and **Platform Resources** (e.g., SharePoint, Salesforce).
- **Detailed Drawer:**
 - **Overview Tab:** Displays the functional description, **Agent ID**, status, and the specific **Agent Identity** it operates under.
 - **Permissions Tab:** Translates raw technical strings into readable **Permission Names, Types** (e.g., Role, Delegated), and **Target platform resources**.