ISPM AI Agent Discovery: Strategy & Interface

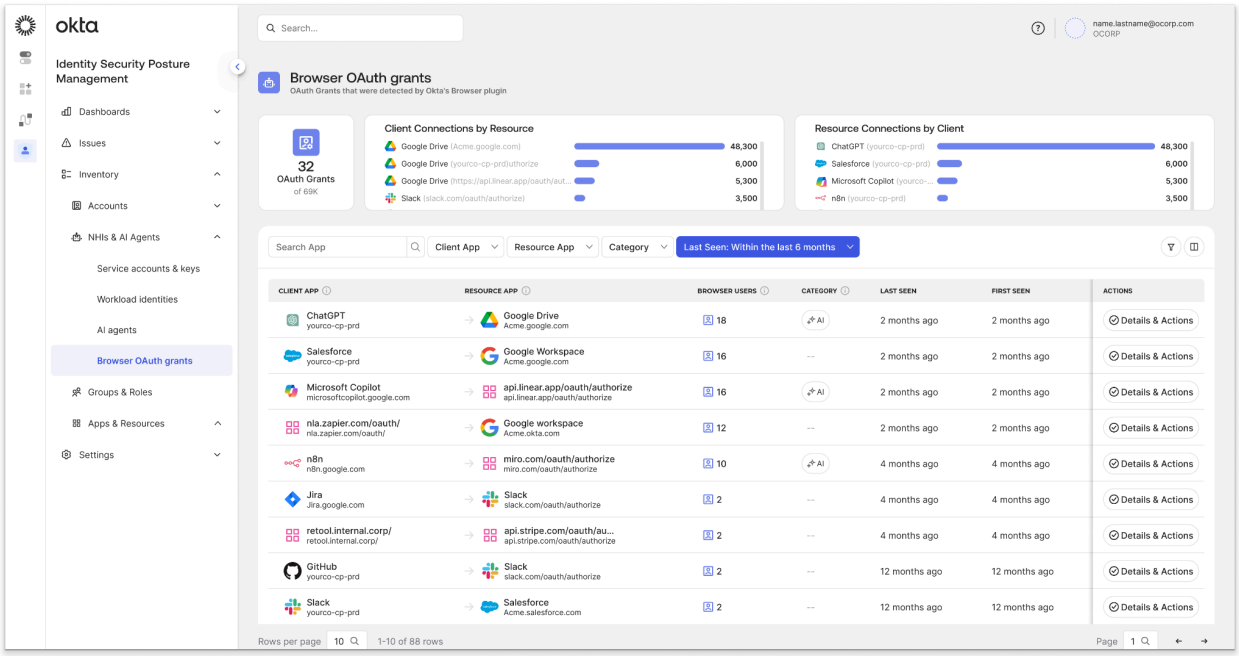
Executive Summary

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.



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

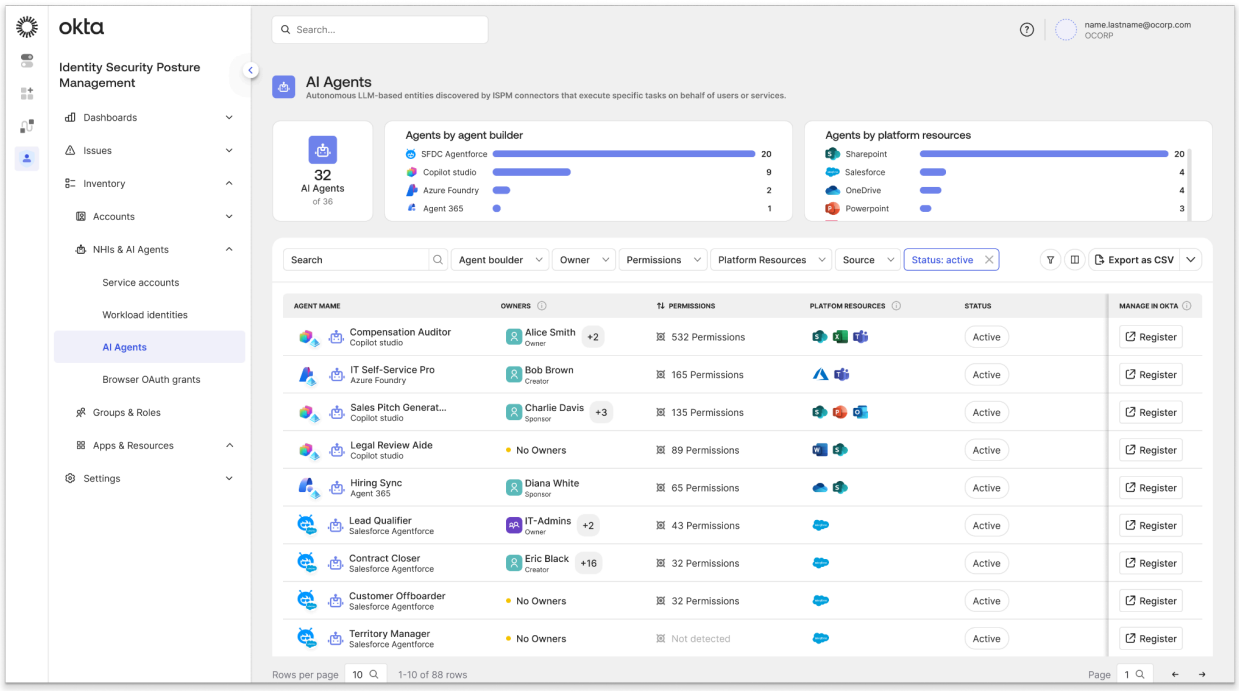
specific permissions (read, write, execute) granted.

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.



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**.