C1 SOLUTION BRIEF

C1 for Shadow AI Discovery

Every agent, found and owned.

ramp instacart zscaler DigitalOcean Brex klaviyo qualtrics

Agents are already running.

AI arrived through the side door: a developer installs Cursor or Claude Code, wires it to an MCP server over the weekend, and pastes in a live API key to make it work. None of it filed a ticket. One in five organizations has already reported a breach due to shadow AI, and among those breached through an AI model or application, 97% lacked proper AI access controls.[1]

The tools security already runs weren't built to govern AI. CASB and DLP watch traffic, data, and processes, and each assumes an identity is a person or a sanctioned app. Shadow AI is neither: it's agents, MCP servers, and exposed keys, identities that nobody inventoried and no one owns. In C1's 2026 survey of 508 IT and security leaders, 47% reported more non-human identities than human users, and only 22% said they have full visibility into them.[2]

What C1 delivers

Find what's already running

Endpoint and cloud discovery surface the agents, MCP servers, and exposed credentials your teams already run, sanctioned or not.

Every discovery gets an owner

Each finding lands in one governed inventory, ready to assign to a person who answers for it, not in another report.

Adoption keeps moving

Discovery doesn't mean blocking: sanction what belongs, govern it in one place, and retire what doesn't.

How C1 surfaces shadow AI.

C1 discovers shadow AI on both fronts. On the endpoint, C1 recognizes the AI tools people install, including Cursor, Claude Code, GitHub Copilot, and Ollama, and maps each tool's MCP servers, the plug-in connections AI tools use to reach other systems, local ones included. Connectors pull agents from Salesforce Agentforce and AWS Bedrock AgentCore, and service accounts and tokens from Entra, Okta, GCP, GitHub, Snowflake, Active Directory, and more.

Every discovery lands in the identities & NHI (non-human identity) inventory, classified and tied to an owner that answers for it. Because that inventory sits on the same control plane that runs requests, approvals, and reviews, a found agent becomes a governed one in the same motion, with an owner assigned and a lifecycle attached.

Discovery that leads to governance.

Catch unsanctioned MCP servers.

Instantly surface unauthorized local AI tools, MCP servers, and integrations installed across endpoints before they expose sensitive networks.

Find exposed keys before they leak.

Shadow AI runs on live keys to real systems: model providers, clouds, databases. C1 surfaces each exposed credential and turns it into access you can own, vault, or revoke. The discovery can never become the leak.

Govern every agent from discovery to de-provisioning.

A discovered agent becomes a real access item, governed as a lifecycle rather than a one-time switch. Assign an owner, route it through request and approval, and de-provision what goes stale.

See every agent your team uses.

C1's connectors find agents and service accounts from Salesforce Agentforce, AWS Bedrock AgentCore, Entra, Okta, GCP, GitHub, Snowflake, Active Directory, and more. Each is linked to a verified identity.

One inventory for every identity discovered.

Everything discovered lands in one identities & NHI (non-human identity) inventory: humans, service accounts, agents, and secrets, each with its creator, what it runs as, and its last use. Expired, expiring, and unused secrets surface before they become standing risk.

Every ungoverned agent is a future incident report.

Shadow AI isn't a discipline problem; it's what adoption looks like when the governed path is slower than the ungoverned one. Banning the tools just pushes them further out of sight. C1 makes the found state the governed state: each discovered agent, MCP server, and exposed key gets an owner, a lifecycle, and a place in the inventory you already review, so the AI your teams already use becomes AI your security team can stand behind.

GET STARTED

Talk to a product expert

Book a demo
c1.ai/demo

ramp

"Another huge win for me is the overall visibility. It's so helpful to have one place to check access across hundreds of systems. I don't have to log into ten different places to figure out who has access to what – I can just go to C1."

Paul Yoo Head of Security Platform, Ramp

About C1

C1 is the control plane for the agentic enterprise, empowering companies to adopt AI fearlessly. Our platform secures human and non-human identities, automates access, and accelerates AI adoption. Companies like Ramp, Zscaler, Qualtrics, and Instacart trust C1 to power their agentic transformation. Learn more at c1.ai.

Adopt AI, fearlessly.

[1] IBM, Cost of a Data Breach Report 2025. [2] C1, 2026 Future of Identity Report, a survey of 508 IT and security leaders at U.S. enterprises with 1,000+ employees.