

Shadow AI Discovery

AI in your enterprise: found, owned, and governed.



ramp 

 instacart

 zscaler

 DigitalOcean

 Brex

klaviyo[™]

qualtrics^{XM}

Shadow AI is a top security risk for enterprises.

Shadow AI has moved from a policy concern to a source of breaches. 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 Most shadow AI starts small. An employee installs ChatGPT or Claude Code, connects the tool to an MCP server over the weekend, and pastes in a live API key to make the connection work. Meanwhile, IT and security are completely unaware.

That blind spot is structural: the legacy tools IT and security teams run weren't built to govern AI. PAM guards human sessions, EDR watches processes, and CASB and DLP watch sanctioned SaaS. Each assumes an identity is a person or a sanctioned app. Shadow AI is neither. Agents, MCP servers, and exposed keys are identities that nobody inventoried and no one owns, and their number is growing. In C1.ai'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

How C1.ai surfaces shadow AI.

Shadow AI lives in two places: your cloud and identity systems, and your employees' laptops. C1.ai covers both. C1 Connectors enumerate agents in Salesforce Agentforce and AWS Bedrock AgentCore, plus service principals, service accounts, and tokens across Entra, Okta, GCP, GitHub, Snowflake, Active Directory, and more. On laptops, C1.ai finds the AI tools employees have installed and the MCP servers those tools are configured to use, including ones running locally.

What C1.ai delivers



Find what's already running

Find unsanctioned AI tools, AI agents, MCP servers, and exposed credentials across the cloud and endpoints.



Every discovery gets an owner

Each one is linked to an owner. Unowned, misclassified, or otherwise risky accounts are flagged.



Adoption keeps moving

Once every agent, tool, and credential is visible and owned, the governed path becomes the fast path.

Each finding becomes an access item on the C1 Identity Platform, the same system that already runs requests, approvals, and access reviews. Assign an owner, route it through request and approval, certify it in a review, and deprovision it when it goes stale.



Discovery that leads to governance.



See every agent your teams use.

C1 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 an owner and the identity it runs as.



Know which identities carry risk.

Humans, service accounts, agents, and secrets, each linked to an owner. Unowned or misclassified accounts are flagged, and expired, expiring, and unused secrets surface before they become standing risk.



Govern every agent from discovery to deprovisioning.

A discovered agent, service account, or credential becomes a real access item. Assign an owner, route it through request and approval, certify it in a review, and deprovision it when it goes stale. Governance becomes a lifecycle, not a switch.



Find credentials AI tools leave on disk.

AI tools write API keys and tokens to plaintext config files. C1.ai records each by type and location, never its value. C1 Vault pulls the secret into a governed vault and strips the plaintext from the config.



Catch unsanctioned MCP servers.

See the MCP servers each AI tool is configured to use, including ones running locally, with approved servers told apart from shadow ones. The gap is your shadow AI footprint.



Give teams an approved alternative.

Give teams approved AI tools and MCP servers in C1 AppHub, with every tool call checked by C1 MCP Gateway, so no one needs a workaround to get work done.

Every ungoverned agent is a future incident report.

Shadow AI happens when approved tools are harder to get than unapproved ones, and banning the tools just pushes them further out of sight. C1.ai makes it easy to find and govern shadow AI. Each discovered agent, MCP server, and exposed key gets an owner, a lifecycle, and a place in the reviews you already run, with every discovery, ownership change, and action logged, so the AI your teams already use becomes AI your IT and security teams can stand behind.

GET STARTED

Talk to a
product expert

Book a demo

c1.ai/demo

About C1.ai



C1.ai is the identity platform for the AI era. Our platform connects humans and agents to enterprise systems with scoped access, enforced policies, human approval, and a record of every action. With C1.ai, the fastest path to AI adoption at scale is the governed path — giving organizations visibility and control without sacrificing security or slowing innovation. Companies such as Ramp, Zscaler, Qualtrics, and DoorDash trust C1.ai to govern identity, secure agents, and empower their teams to put AI to work.

Put AI to work.

