C1.ai SOLUTION BRIEF

C1 MCP Gateway

Secure access to AI tools, agents, and MCP servers for fast, governed AI adoption.



ramp instacart zscaler DigitalOcean Brex klaviyo qualtrics XM

AI is shipping faster than identity can govern it.

95% of enterprises already run AI agents that act on their own, most of them in production.[1] To be productive, these agents need to reach company systems, the same way an employee does. But the systems that grant access were built for people: they request access, wait for approval, and get reviewed each quarter. An agent is different. It spins up in seconds, finishes its task, and vanishes, often with no record of who created it or what it touched.

At 47% of enterprises, non-human identities already outnumber employees, and only 22% can see all of them,[1] let alone govern what they reach. And most access models can't separate the two: an agent acting for a person inherits that person's full entitlements, with no way to grant the agent less. The gap between machine-speed access and human-speed control is where shadow AI takes root and rollouts stall.

What C1.ai delivers

Adopt with confidence

AI tools reach the team without standing credentials or ungoverned tool calls.

Speed by default

No one waits days for an AI tool, so no one routes around security to get one.

One audit trail

What an agent touched sits on the same audit log as what a person did, down to the tool call.

C1.ai is the identity platform for the AI era.

C1 MCP Gateway governs every AI tool, agent, and MCP server through the C1 Identity Platform, the same platform that already governs the company's people and workloads. AI clients connect to one URL, not to each downstream server. Each tool call is checked against policy for that identity, passed to the MCP server if it's allowed, and logged with full context. Request, check, call, log.

The C1 Identity Platform ensures the governed path becomes the fastest path. A developer's request clears in seconds instead of sitting in a ticket queue. Credentials stay in C1 Vault and never land on a laptop. Agents reach production with owners and reviews already attached. Security is no longer what slows AI down, and AI is no longer outrunning it.

Fast for the team, governed for security.

Self-service MCP access wherever you work.

A person requests access to any server in a 3,000+ hosted MCP catalog from Slack, Microsoft Teams, the CLI, or a coding agent, and policy approves it in seconds, a process that used to take days of tickets and manual setup. C1 Vault holds the credentials while C1.ai handles sign-in and token refresh in the background, keeping access secure.

Real-time policy on every MCP tool call.

C1 MCP Gateway checks each call inline, enforcing which tools are allowed, which parameters are permitted, and what output to redact. Sensitive actions route to an approver before they run. Harden against tool poisoning, confused-deputy attacks, and supply-chain MCP risk.

Audit-ready by default.

Standardized auditing for every action: tool calls are recorded with a complete identity trail, including the initiator, parameters, governing policy, and outcome. Logs integrate with existing SIEM/SOAR and S3 storage, aligning with SOC 2, HIPAA, GDPR, and ISO 42001.

Agents governed as first-class identities.

Personal AI assistants act under their owner's identity. Enterprise agents run as C1 Service Principals, with their own owner, roles, and access reviews. For MCP servers that support it, C1.ai can issue a scoped, signed token instead of proxying the call.

Make the governed path the fastest one.

AI agents are taking on more work, and each one needs access the moment it acts. Quarterly reviews and manual tickets can't move at that speed, so people wait or route around security to get unblocked. C1.ai governs the tool call itself, for people and agents on one platform, so a team can adopt AI quickly without leaving it ungoverned. This isn't on the horizon. The agents are running today, and C1.ai governs them now together with all human identities.

GET STARTED

Talk to a product expert

Book a demo
c1.ai/demo

About C1.ai

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.

Copyright © 2026 ConductorOne, Inc. All rights reserved.

[1] C1.ai, 2026 Future of Identity Report, a survey of 508 IT and security leaders at U.S. enterprises with 1,000+ employees.