C1 SOLUTION BRIEF

C1 AI Access Management

Secure access to AI tools, agents, and MCPs for fast, governed AI transformation.

TRUSTED BY IT & SECURITY

ramp · instacart · zscaler · DigitalOcean · Brex · klaviyo · qualtrics

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, who request it, wait for approval, and get reviewed each quarter. An agent is different. It spins up in seconds, runs for seconds, 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. The gap between machine-speed access and human-speed control is where shadow AI takes root and rollouts stall.

What C1 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 is the identity control plane for AI.

C1 AI Access Management governs every AI tool, agent, and MCP server through one identity-aware control plane, the same platform that already governs the company's people and workloads. An AI client connects through C1's proxy. 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.

So the governed path becomes the fastest path. A developer's request clears in seconds instead of sitting in a ticket queue. Vaulted credentials 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 in Slack, Cursor, or CLI.

A person requests AI MCP access and policy approves it in seconds, a process that used to take days of tickets and manual setup. C1 vaults the credentials and handles sign-in and token refresh in the background, keeping access secure.

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.

Real-time policy on every MCP tool call.

An identity-aware 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.

Agents governed as first-class identities.

A personal AI assistant acts under its owner's identity. An enterprise agent runs as a C1 Service Principal, with its own owner, role assignments, and access reviews, so AI gets governed the way people are.

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 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 governs them now together with all human identities.

GET STARTED

Talk to a product expert

Book a demo
c1.ai/request-demo

About C1

C1 empowers organizations to adopt AI securely and at speed by delivering the right access and context to every human, workload, and agent. Companies like Instacart, Ramp, Zscaler, and Brex trust C1 to accelerate AI adoption with confidence. Learn more at c1.ai.

Scale access at the speed of AI

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