

C1 Bridge

Govern on-prem systems and MCP servers from C1.ai, with no inbound ports and nothing exposed to the internet.



Your most sensitive systems are the hardest to govern.

On-prem apps, private databases, and a growing number of internal MCP servers sit behind the firewall on purpose. Some of those MCP servers are built in-house to wrap sensitive data or a team's own tools. Others ship with software you run yourself, from a self-managed ERP to an on-prem code platform. In financial services, healthcare, and critical infrastructure, regulation often requires that these systems stay inside the network.

That is what keeps them safe, and what makes them hard to govern. A cloud identity platform has no network path in to request, approve, or audit access, and the usual workarounds fall short. Exposing the server is a non-starter. A VPN or reverse proxy adds infrastructure to own and still moves packets without governing who sits on the other end. Doing nothing leaves a server that agents can already reach with no one watching, which is how shadow MCP turns into a finding in the next audit.

Reach without exposure.

C1 Bridge is C1.ai's outbound connectivity layer: a lightweight agent that runs inside your network beside the systems C1.ai needs to reach. Nothing inbound is required: no firewall rule, no public hostname, no change to the network's posture. Once connected, a private MCP server appears in C1.ai like any other: C1.ai discovers and classifies the server's tools, and AI clients reach the server through C1 MCP Gateway. Private apps and databases connect through supported C1 Connectors, joining the access requests, approvals, and certifications you already run.

What C1.ai delivers



Nothing exposed to the internet

The bridge client opens and maintains the connection to C1.ai, so your network needs no inbound listener or firewall exception.



One bridge, many services

A single bridge carries traffic for multiple connectors and MCP servers, each with its own name, port, path, and transport.



Private access, fully audited

Access to every private system is requested, approved, and audited like any other entitlement.

Private connectivity, governed like everything else.

Connect apps, infrastructure, and MCP servers.

Reach on-prem apps, infrastructure, and databases through supported C1 Connectors, and bring private MCP servers under C1 MCP Gateway.

One scoped, revocable credential.

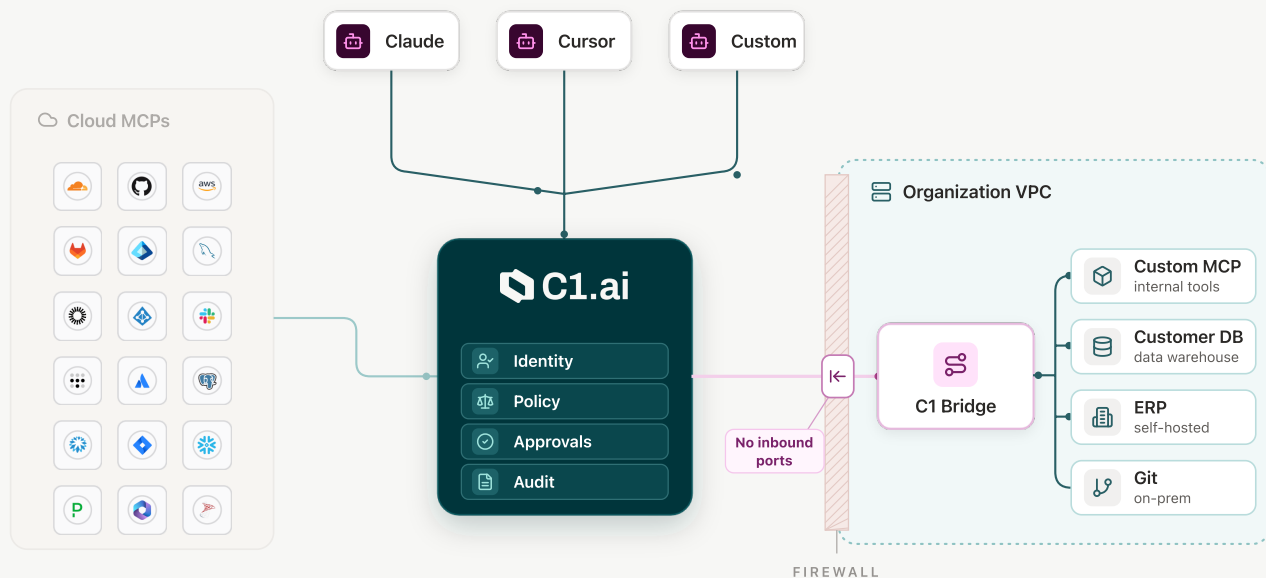
The bridge makes no access decisions of its own. If the bridge is ever compromised, cut it off in a single action.

No inbound firewall rules needed.

C1 Bridge connects outbound to C1.ai, so there is no port to open, no public hostname, and no change to your network's posture.

Runs where your infrastructure runs.

Deploy bridge-client as a container or binary on a VM, Kubernetes, Docker, or bare metal. bridge-client validates its configuration before starting, so a platform engineer can have the bridge running in an afternoon without filing a networking exception.



Reach is plumbing. Governance is the point.

Bringing a server under governance should never require opening it up. The servers organizations keep off the internet on purpose are often the ones closest to sensitive data. For environments where regulation forbids inbound exposure of a protected zone, such as PCI-DSS or NERC CIP, an outbound-only design is often the only way to connect them without breaking the control. C1 Bridge closes the hardest case: the servers organizations keep off the internet on purpose now sit under one control plane, across every system and every architecture.

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.

