C1.ai SOLUTION BRIEF

C1 Egress

Give agents network access without giving up the credential.



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

Every credential in an agent's environment is a potential attack path.

The standard way to give an application or agent access to another service is to paste a credential into its environment. From there it spreads: into a repository, a container image, an agent's context window, a screenshot. Setting an environment variable and hoping the agent respects it isn't enforcement; code that wants to get around an environment variable finds a way around it. And an agent that can reach the open internet can just as easily be tricked into reaching an internal address or a cloud metadata endpoint, handing over the one credential that was supposed to stay put.

What C1.ai delivers

Nothing to steal.

The workload never holds the credential, so there's nothing for an attacker to find.

Denied by default.

Internal addresses and cloud metadata endpoints are blocked automatically, regardless of policy.

A record, not a guess.

Every call is logged with source, destination, and decision, never the secret itself.

Turn every outbound call into one C1.ai already governs.

C1 Egress sits between an application or agent and the outside world. It's the only thing on that path that ever touches the real credential, the actual password or key the app would otherwise need. The app itself never holds it: for each request, C1 Egress inserts the real credential, sends it only to the one destination policy allows, then denies everything else by default.

That default-deny extends to the places attackers go first: internal network addresses, and a cloud provider's metadata service, the address that would hand back a cloud account's own master keys.

Those requests never reach a policy check; C1 Egress blocks them automatically. That matters because most credential theft today isn't a break-in from outside. It's a compromised or tricked application reaching somewhere it was never meant to reach from the inside.

Every request is still logged in full: where it went, what it was for, what C1 Egress decided, but the credential itself never appears in that record. That's what makes the protection hold even against code written specifically to route around it: there's no credential sitting in the environment to find.

Runtime control for every outbound call.

The credential stays out of the workload.

C1 Egress keeps it secure and adds it only when the agent makes an approved request.

Default-deny egress.

Requests to internal addresses and cloud metadata endpoints are blocked automatically, regardless of policy.

Enforcement an agent can't opt out of.

Traffic is captured at the network layer, not an environment variable code can unset or route around.

A secret-free audit trail.

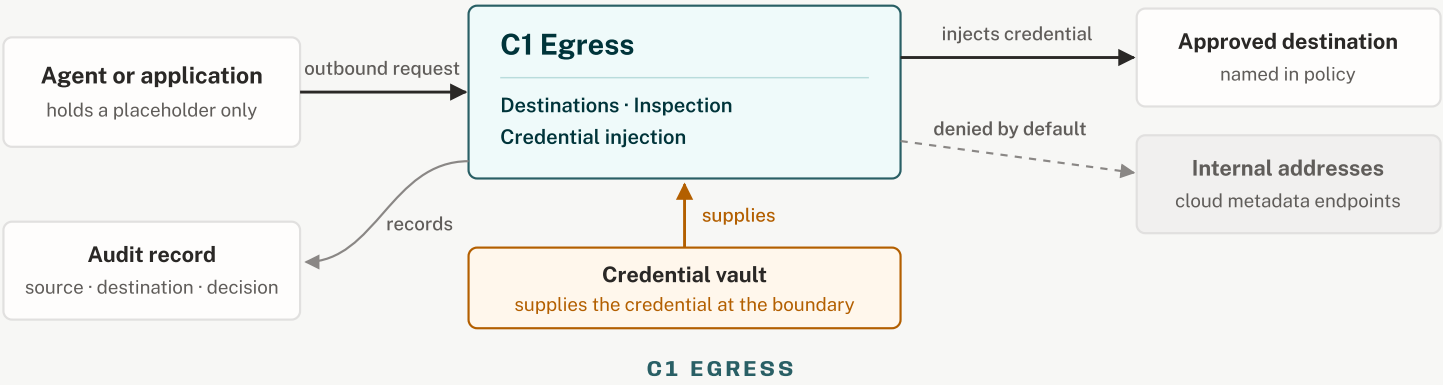
Every call is logged with source, destination, and decision. The credential itself is never recorded.

Credentials added only when needed.

C1 Egress adds the real credential as the request leaves the workload, and only for the approved destination.

Secure access by default.

Agents can connect to the systems they need while credentials stay protected outside the workload, preventing prompt-injection attacks.



Put AI agents to work.

C1 Egress lets teams put agents to work across real systems without handing over credentials or slowing builders down. Network-level policy controls where each agent can connect, credentials stay outside the workload, and every request is recorded automatically. The result is faster deployment, less manual review, and the confidence to expand agent access as the business grows.

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.

© 2026 ConductorOne, Inc. All rights reserved. ConductorOne and C1 are trademarks of ConductorOne, Inc.