

Secrets Management

Give agents credentials. Keep control.



ramp   instacart  zscaler  DigitalOcean  Brex  klaviyo  qualtrics^{XM}

Secrets leak faster than teams can rotate them.

Every API key, token, and password is standing access, and most sit in config files, environment variables, and repos long after anyone is watching. AI agents accelerate the problem: each one needs its own credentials, and each one can leak them through a prompt, a log, or a tool call. GitGuardian counted 28.65 million new secrets leaked on public GitHub in 2025, up 34% year over year, with leaked AI-service credentials up 81%.¹

Breaches involving compromised credentials average \$4.67 million and take 246 days to identify and contain.² A secrets manager stores the key, but it sits beside your identity system, not inside it: the requests, approvals, reviews, and audit trail that govern the rest of your access never touch the secret. Storage was never the hard part. Managing it securely is.

What C1.ai delivers

Less standing access, less risk

Every secret is attributed to the identity that holds it, with alerts on ones that go unused, so standing access doesn't sit unnoticed.

Agents get access, attackers get nothing

Short-lived, scoped credentials are issued at the moment of use, so a compromised agent can't leak a key it was never handed.

Pass the audit without a scramble

Every secret carries an owner and a policy, and every grant and retrieval lands on the audit trail you already run.

C1.ai governs every secret like an identity.

C1.ai closes the loop from exposure to expiration. Shadow AI discovery surfaces the credentials sitting exposed on developer machines and across the estate. The secret is then encrypted on the device, the plaintext becomes a managed reference, and the move is reversible. Each secret is attributed to the identity that holds it, and C1.ai alerts on ones that haven't been used recently. C1 Vault extends that custody toward the places credentials leak, so every secret runs through the same requests, approvals, and reviews as the rest of your access.

Access is the control point. Agents reaching MCP servers get short-lived tokens through enterprise-managed authorization, pipelines calling C1.ai get them through workload federation, and C1 Egress adds the real credential at the network boundary so the workload never holds it. What agents never hold, prompts can't leak, and what expires on its own never becomes standing risk.



One system for every secret: owned, issued, and audited.



Vault secrets where they live.

C1.ai brings secrets under governance where they already live, without disrupting the workflows and pipelines that use them, with every secret attributed to the identity that holds it.



Protect against prompt-injection data theft.

Agents get short-lived, scoped credentials at the moment of use, never the raw key. For outbound calls, C1 Egress adds the real credential as the request leaves the workload, only for the approved destination.



Decoy credentials that catch theft instantly.

Plant decoy credentials where an attacker would look — env files, CI variables, secret managers. Any use raises a critical finding, and whoever's using it just sees an ordinary authentication failure.



Enforce zero standing secret access.

Eliminate long-lived static secrets with assigned owners, lifecycle policies, and expiry dates, all under one audit trail.



Future-proof secrets against quantum threats.

Secrets land in a vault built on zero-knowledge, quantum-resistant cryptography: end-to-end encrypted, post-quantum ready by default, and C1.ai stores only ciphertext, never enough to read a value.

Every secret vaulted. No standing risk.

The secrets problem stopped being a storage problem the day agents started outnumbering people. What protects a credential now is how it's granted: to an owner, for a purpose, for a bounded time, on the record. C1.ai runs that workflow on the same platform as the rest of your access, with C1 Vault holding custody underneath it, so security gets one loop from exposure to expiration, and one trail that proves it.

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.

