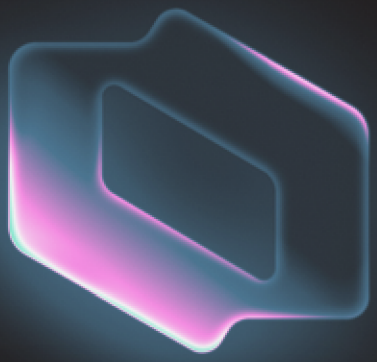
C1 SOLUTION BRIEF

Agentic Vault

Quantum encrypted. Governed like an identity.



ramp instacart zscaler DigitalOcean Brex klaviyo qualtrics XM

Every credential is a key to something.

AI agents run on credentials: model-provider keys, cloud roles, database logins, tokens to every system they touch. Most of those secrets live where the work happens, pasted into config files, environment variables, and prompts, and they stay valid long after the task that needed them. An agent that authenticates still walks away holding the key, and whatever holds a key can leak it.

Traditional secrets managers were built beside the identity system, not inside it, so the vault stores the key while the rules about who may use it live somewhere else. Stored secrets also face a longer clock: ciphertext harvested today can be decrypted once quantum hardware matures, and Executive Order 14412 has already set U.S. federal agencies on a post-quantum migration, with deadlines for the most sensitive systems stretching to 2030 and 2031.[1]

What Agentic Vault delivers

Agents governed like your most privileged users

Agents get access under the same policies and audit trail as human admins, but the secret never reaches the model. A compromised agent can't leak what it was never given.

Quantum-resistant from day one

MLS group cryptography protects every vault against "harvest now, decrypt later" attacks, and maps directly to the federal post-quantum migration mandate.

One identity loop instead of vault sprawl

Agentic Vault lives inside the identity layer, provisioning, cycling, and destroying credentials at machine speed, improving security posture.

Agentic Vault, built into identity governance

Agentic Vault is built inside identity governance, and membership is the access control. Each vault is an encrypted group: granting access places a member cryptographically, and removing one revokes access immediately and re-keys the vault, locking the removed device out of every future change, by construction. Every grant runs through the same policy engine, approvals, and audit trail as the rest of your access, logged down to the individual retrieval.

Issuance replaces possession. A trust rule lets a workload exchange its signed identity for a short-lived credential: scoped to specific permissions, pinned to an IP range if you choose, bound with proof-of-possession, and gone when the task ends. The vaulted value stays sealed out of the model's context, and pointing agents at the vault is an SDK or CLI drop-in: no key rotation to manage, no plumbing to build.

Built for AI agents.

Vault and replace, straight from the endpoint.
C1 finds an exposed credential on the endpoint and secures it: the secret moves into encrypted custody, and the plaintext becomes a managed reference that resolves at runtime.

Post-quantum ready from day one.
Every vault runs on zero-knowledge architecture with MLS group cryptography, and a hybrid key exchange pairs today's proven encryption with a NIST-standardized post-quantum algorithm, so stored secrets resist harvest-now, decrypt-later attacks from the moment you save them.

Decoys turn credential theft into an alert.
C1 vends credentials that look real but belong to no legitimate workload, each authenticating against C1-monitored endpoints. Any use, anywhere, fires a high-confidence finding tied by fingerprint to the exact plant, and response runs through the queues your team already works.

Short-lived credentials through workload federation.
An agent authenticates as itself and receives a scoped, expiring credential at the moment of use. No plaintext key handed over, nothing standing to steal.

C1 can't read your secrets.
Secrets are encrypted on the device before anything reaches C1. What C1 stores is ciphertext and governance metadata: enough to govern grants and inventory what exists, never enough to read a value.

Give agents access. Keep the secrets locked away.

Agentic Vault creates one governed process for every secret. An exposed key on a laptop is brought into custody. Its replacement is governed like an identity: requested, approved, and audited. An agent gets a short-lived, scoped credential for the task, never the raw vaulted secret, and it is post-quantum ready right from day one. No need to slow down AI adoption to stay safe or trade control for speed. The secure path and the fast path are the same. Adopt AI, fearlessly with the Agentic Vault.

GET STARTED

Talk to a product expert

Book a demo
c1.ai/demo

DigitalOcean

"C1 is innovating in an area underserved by the technology industry, and solving problems a lot of teams have to do manually."

Heather Cannon Security Engineering Leadership, DigitalOcean

About C1

C1

C1 is the control plane for the agentic enterprise, empowering companies to adopt AI fearlessly. Our platform secures human and non-human identities, automates access, and accelerates AI adoption. Companies like Ramp, Zscaler, Qualtrics, and Instacart trust C1 to power their agentic transformation. Learn more at c1.ai.

Adopt AI, fearlessly.

[1] Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, The White House, June 2026.