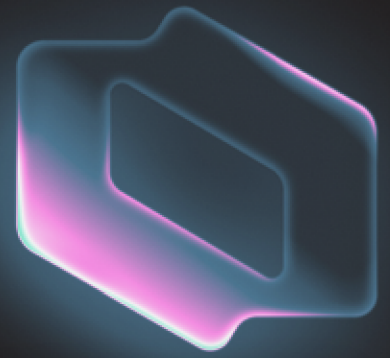




SOLUTION BRIEF

C1 for Credential Security

Give agents credentials. Keep control.



ramp ↗

✱ instacart

zscaler

DigitalOcean

Brex

klaviyo

qualtrics^{XM}

Vaults only protect the secrets they hold. Most never get there.

Secrets leak faster than teams can rotate them, and AI agents multiply both sides of the problem. 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 Every agent that needs a key gets one, and most get it the fast way: pasted into a config file, an environment variable, or a prompt.

Each of those keys is standing access with nobody watching it. 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 delivers



Less standing access, less risk

Exposed credentials are vaulted in place and replaced with a managed reference, and the move is fully reversible.



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 governs every secret like an identity.

C1 closes the loop from exposure to expiration. Shadow AI discovery surfaces the credentials sitting exposed on developer machines and across the estate, and agentic vault, C1's secrets vault built inside identity governance, takes custody: the secret is encrypted on the device, the plaintext becomes a managed reference, and the move is reversible. From that point on, the secret runs through the same requests, approvals, and reviews as the rest of your access.

Access is the control point. People and agents get short-lived, scoped credentials at the moment of use, under the policies you already run, while the raw key stays sealed in the vault, out of prompts and configs. 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 finds exposed credentials on developer machines and vaults them in place, without disrupting the workflows and pipelines that use them. The plaintext is gone, a managed reference takes its place, and the move is fully reversible.



Protect against prompt-injection data theft

Agents get short-lived, scoped credentials at the moment of use, never the raw key. Nothing standing to steal, nothing sitting in a prompt.



Decoy credentials that catch theft instantly.

Turn an attacker's first move into an immediate alert by placing decoy credentials that trigger high-confidence warnings the moment they are touched.



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 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 runs that workflow on the same control plane as the rest of your access, with Agentic 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



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.

