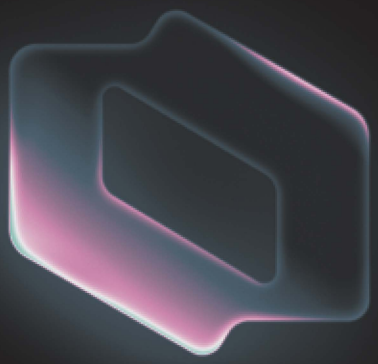
C1 SOLUTION BRIEF

Just-in-Time Access

Replace standing privileges with automated time-bound access.



TRUSTED BY IT & SECURITY | ramp | instacart | zscaler | DigitalOcean | Brex | klaviyo | qualtrics

Standing privilege is a risk waiting to be exploited.

Compromised credentials were the initial access vector in 22% of breaches last year, the leading vector for the second year running.[1] Every long-lived grant is standing exposure, whether it's a production role assigned at hire and never revoked, an admin entitlement inherited through group nesting, or a break-glass account that never breaks the glass. The Cloud Security Alliance (CSA) now calls for a decisive shift away from persistent privileged access toward zero standing privileges.[2]

AI is widening the blast radius. By 2028 the average Fortune 500 will run more than 150,000 AI agents, each one a fresh identity requiring access.[3] Static, role-based entitlements can't scope agent access to a single task or revoke it when the task ends. And every standing permission, human or agent, is a credential an attacker only needs to find once.

Reduce risk without slowing down the business

Zero standing privilege, everywhere

JIT covers every app and entitlement across cloud and on-prem, cutting standing privileges by 95%.

Access without the wait

Users and agents self-serve from Slack, Teams, MCP, CLI, or the console and get provisioned in under 60 seconds.

Access ends with the work

Every grant is revoked the moment it expires, with no cleanup tickets and no quarterly purge.

Turn every privileged grant into a time-bound, scoped event.

Whether it's a developer asking for production in Slack, an SRE escalating from the CLI, or an agent calling an MCP tool, C1's policy engine weighs the request against role, attributes, on-call status, context, and risk in real time, then auto-approves it or routes it to the right human. The grant is scoped to the exact entitlement and the time the work needs, and when the window closes, C1 revokes it with no ticket and no cleanup. The same engine handles the engineer and the agent, so privileged access works the same way no matter who, or what, is asking.

The result is privileged access that behaves the way auditors and CISOs have always wanted. Blast radius shrinks because every grant is scoped and temporary. Engineers stay productive because policy handles approvals in seconds. And IT and security stop carrying the operational burden, because C1 provisions and revokes on its own and writes the audit trail as changes happen, not reconstructed after the fact.

Automated just-in-time access across every identity and system.

Self-service from anywhere work happens.

Users and agents request JIT access from Slack, MS Teams, MCP, CLI, or the C1 console. Approval routing and provisioning happen in seconds.

Policy-based approval or escalation.

Conditional rules assess role, attributes, request context, and risk, then auto-approve, route, or deny.

Zero-touch provisioning.

C1 provisions and deprovisions access automatically. No tickets. No waiting.

Scoped to the task.

Grant JIT access to the specific systems, entitlements, and time windows the work requires. No broad role assignments or carryover.

Immediate auto-revocation.

Every JIT grant expires as set by policy. 100% revocation at expiry, no cleanup tickets, no quarterly purge.

Break-glass that doesn't break governance.

Pre-approved JIT emergency policies let on-call responders move in seconds during incidents, with full audit context captured by default.

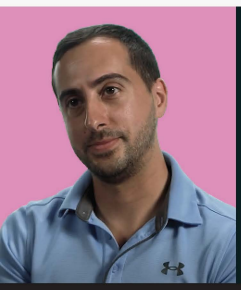
Zero standing privilege. C1 is how you get there.

The industry is converging on a single answer to standing privilege: don't have any. Analysts are recommending phased JIT access adoption, the CSA is publishing about it, and NIST has spelled out per-session, time-bound, dynamically evaluated access as the zero-trust target. The teams that get there first will be the ones whose privileged access decisions look the same whether the requester is a senior engineer in Slack or an AI agent calling an MCP tool. C1 makes that operational across every system humans, workloads, and AI agents touch.

GET STARTED

Talk to a product expert

Book a demo
c1.ai/request-demo



instacart

"With the power of C1's conditional policies, we can auto-approve. People get the access they need right away."

Dominic Zanardi Senior Software Security Engineer II, Instacart

About C1

C1 empowers organizations to adopt AI securely and at speed by delivering the right access and context to every human, workload, and agent. Companies like Instacart, Ramp, Zscaler, and Brex trust C1 to accelerate AI adoption with confidence. Learn more at c1.ai.

Scale access at the speed of AI

[1] Verizon, 2025 Data Breach Investigations Report. [2] Cloud Security Alliance, Killing Standing Privileges: Why Just-in-Time Access is the Future of PAM, December 4, 2025. [3] Gartner, Beyond Agent Sprawl: The Rise of AI Agent Management Platforms, March 2026.