C1.ai
A Workday Company

SOLUTION BRIEF

JIT Access

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

Standing privilege is a risk waiting to be exploited.

In Verizon's 2025 Data Breach Investigations Report, compromised credentials were the initial access vector in 22% of breaches, 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, Microsoft Teams, MCP, the CLI, or the console and get provisioned in under 60 seconds.

Automatic revocation at expiry

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.

Just-in-time (JIT) access grants privileges only when they're needed, scoped to the task, and revokes them automatically when the work is done. Whether it's a developer asking for production in Slack, an SRE escalating from the CLI, or an agent calling an MCP tool, the C1.ai policy engine checks it in real time against the requester's role, on-call status, and risk. It then auto-approves the request 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.ai revokes it with no ticket and no cleanup. The same engine handles people and agents, each with its own entitlements.

A sales rep's role includes write access to Salesforce, but the AI agent acting for that rep doesn't inherit it. The agent gets write access only through a just-in-time request, scoped to one task and revoked when the task ends. 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.ai 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.

Request access where you already work.

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

Zero-touch provisioning.

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

Immediate auto-revocation.

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

Policy-based approval or escalation.

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

Scoped to the task.

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

Governed emergency (break-glass) access.

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

The target is zero standing privilege. C1.ai 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.ai makes that operational across every system humans, workloads, and AI agents touch.

GET STARTED

Talk to a product expert

Book a demo
c1.ai/demo



instacart

"With just-in-time access, we can greatly reduce our blast radius if something happens."

Matthew Sullivan Infrastructure Security Team Leader, Instacart

About C1.ai

C1.ai
A Workday Company

C1.ai, a Workday company, 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.

Copyright © 2026 ConductorOne, Inc. All rights reserved.

[1] Verizon, 2025 Data Breach Investigations Report, April 2025. [2] Cloud Security Alliance, Managing Privileged Access in a Cloud-First World, 2025. [3] Gartner, Gartner Identifies Six Steps to Manage AI Agent Sprawl, press release, April 28, 2026.