C1 SOLUTION BRIEF

C1 for Agentic Security & Intelligence

Ranked, actionable findings across every human, workload, and agent.

ramp instacart zscaler DigitalOcean Brex klaviyo qualtrics

Identity is where breaches start.

Four in five enterprises had at least one identity-related breach in the past year.[1] Service accounts, workloads, and AI agents now hold access alongside humans, and the risky ones rarely announce themselves. The review meant to find them runs four times a year. Access changes every day in between, and nothing catches what shifted until the next one comes around.

The tools security already runs weren't built to change access. Posture management (ISPM) scores the risk, threat detection (ITDR) raises the alert, and both stop at the handoff: a report for someone else to act on. The distance between finding a risk and fixing it is where the breach happens.

What C1 delivers

Know the blast radius first

One intelligence graph maps what every identity can reach, so the reach is known before a compromise, not after.

Every finding arrives ranked

Findings land in one queue scored by severity, so the team works the highest risk first, not the newest alert.

Fix it where you govern access

The fix runs through the same request, approval, and audit as any access decision, and the finding closes on its own.

How C1 catches and closes risk.

C1 finds identity risk inside the system that governs access. Every identity from every connected system maps into one intelligence graph: humans, service accounts, workloads, and AI agents, including agents in Salesforce Agentforce and AWS Bedrock AgentCore. Each one shows what it can reach, down to the apps, accounts, and entitlements it holds. When something's wrong, C1 raises a finding, ranked by severity in one queue with that full reach attached. Triage starts from an answer instead of an alert.

The fix runs in the same place, as a governed task: reassign the owner, revoke or right-size the access, or certify it in review, through the same approvals and audit trail as any access decision. Nothing changes silently. When the underlying problem clears, the finding closes itself, and the trail shows who acted, what changed, and when.

Catch and close, in one place.

Know what every identity can reach.

C1 maps every identity into one intelligence graph: humans, service accounts, and AI agents, with the apps, accounts, and entitlements each one carries. When one is compromised, the blast radius is already mapped.

Fix the risk where you already govern access.

Every risk C1 catches comes with the fix attached: reassign the owner, revoke or right-size the access, or certify it in review, through the same request, approval, and audit as any access decision. Clear the underlying problem and the finding closes on its own.

One queue for every tool's findings.

Push findings from your other tools through the API. They land in the same queue, with the same routing, governance, and audit as everything C1 raises.

Work the risk, not the noise.

When governance drifts, C1 raises a finding: an identity nobody owns anymore, a service account misclassified as human, a planted decoy credential in use. Each lands ranked by severity in one queue, so the team's energy goes to the highest-risk items first.

Route what matters to the queue your team watches.

Set severity, tag it, quiet what's expected. Then route findings into your automations and webhooks, and on to ServiceNow, Jira, or PagerDuty, audit trail attached.

A finding that ends in a report isn't security.

C1 closes the distance where breaches live, between the system that finds identity risk and the system that can change access, by making them the same system. Each finding arrives with context, leaves with a fix, and lands on the audit trail your reviews already run, across every identity, human and non-human alike. No new dashboard to watch, no report to hand off, no second tool to reconcile at audit time. Caught, ranked, closed, and proven, in one place.

GET STARTED

Talk to a product expert

Book a demo
c1.ai/demo

DigitalOcean

"Having a tool that can do this in a timely fashion, iteratively and repeatedly, without manual inputs and outputs enables very real security control. This will improve our security posture at the end of the day."

Tim Lisko Director of Product and Infrastructure Security, DigitalOcean

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.

© 2026 ConductorOne, Inc. All rights reserved. ConductorOne and C1 are trademarks of ConductorOne, Inc.

[1] C1, 2026 Future of Identity Report, a survey of 508 IT and security leaders at U.S. enterprises with 1,000+ employees.