

BUYER BRIEF

Every Decision Begins With Authority

The execution-time authority, governance and evidence layer for AI agents and enterprise systems.

Every Decision Begins With Authority.

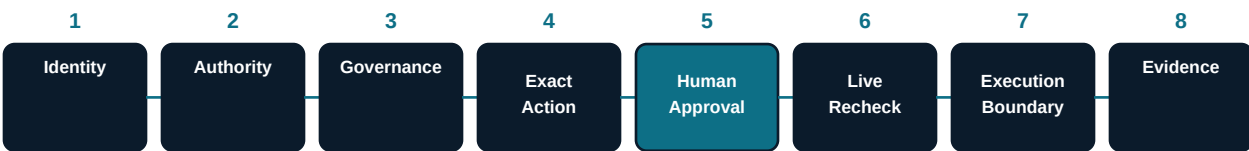
Version 4 · October 2026 · Trace Continuity Labs · tracecontinuity.com
Patent Pending — U.S. Provisional Patent Application No. 64/137,172. Not a certification.

1 · What Trace is

Trace Continuity is an execution-time authority, governance and evidence layer for AI agents and enterprise systems. It determines whether an actor is authorized to perform a specific action at the moment of execution, enforces that decision at the execution boundary, and produces verifiable evidence of what was authorized and what occurred.

Most systems authenticate once and trust the session afterwards. AI agents make that gap expensive: an agent can act for hours on authority that was withdrawn minutes after it started. Trace answers a narrower and harder question at the moment it matters: may this actor perform this exact action, right now, in this tenant — and can we prove what happened afterwards?

2 · How it works



Human approval applies when the action requires it. Authority is re-checked live at the boundary.
Evidence is recorded at every step and signed; tenant-wide checkpoints can be retained outside Trace.

Identity establishes who is asking. Authority establishes what they may do, including the whole delegation chain. Governance applies policy, conditions, matters, ethical walls and legal holds. The exact action is fixed by a fingerprint. If the action needs a human, the approver sees that exact action. Immediately before execution, authority is re-checked live. The enforcement point at the execution boundary redeems a single-use permission and reports the outcome. Every step becomes evidence.

3 · What Trace covers today

Capability	What it means
Execution-time authority	Authority verified on every governed request, never cached from login.
Allow / Deny / Transform	Every governed decision has one of three outcomes, recorded as evidence.
Delegation-chain enforcement	A delegate can never exceed its grantor in tenant, scope, execution rights or lifetime.
Suspension and permanent revocation	Suspension is reversible through governed controls; revocation can never be undone.
Person offboarding	Suspend a person and the authority, keys, agents and pending approvals that depend on them.
Governed API keys	New keys require expiration, enforced at execution; extending lifetime needs a second person; legacy keys flagged.

Capability	What it means
Agent registry	Registered agents with owner, purpose, bound keys and suspension.
Matters, ethical walls, legal holds	Enforced on the same execution-time path.
Governed derived information	Reported lineage lets upstream changes govern summaries, embeddings and facts.
Governance-over-governance	Weakening an important protection requires a second administrator's approval of the exact change.
Human approval	High-risk actions can require approval; the approver sees the exact action; no self- or dependent approval.
Exact-action authorization	Single-use, time-limited permission bound to one action by a canonical fingerprint.
Live recheck and enforcement points	The registered enforcement point redeems only after authority is re-checked live, atomically.
Outcome evidence	Authorized, executed, failed and could-not-establish remain distinct.
Signed evidence packages	Ed25519-signed, verified offline against Trace's published public keys.
Tenant-wide signed checkpoints	Chained checkpoints over the whole evidence history; anchors retained outside Trace.
Refusal to sign altered history	Trace re-verifies committed history before signing or checkpointing and refuses on mismatch.
Compromised-key handling	A compromised key never signs again; its trusted boundary is pinned and can only narrow.
Stale-access visibility	Read-only, tenant-scoped view of stale keys, agents, authorities and orphaned delegation.
Tenant isolation; sensitive-data protection	Tenant boundaries throughout; identifiers tokenized before storage.
Non-bypassable governed path	One decision path; a build-blocking scanner fails the build on any bypass.

4 · Why buyers care

- **Offboarding that actually stops access.** When a person leaves or is suspended, the authority, keys, agents and approvals that depended on them stop working at the next governed request.
- **Approvals that mean something.** An approval binds one exact action. Change the amount, the recipient or the target and it no longer applies.
- **No quiet weakening.** One administrator cannot switch off an important protection alone.
- **Evidence a third party can check.** Signed packages verify offline. Customers can retain checkpoint anchors so later deletion or rewriting of committed history is detectable.

5 · Stated limits

- Signed checkpoints do not prevent a database owner from changing data. They make later alteration or deletion of committed history detectable against checkpoints retained outside Trace. Activity after the most recent retained checkpoint is covered only once a later checkpoint is retained.
- If a database owner erased every Trace-held record of earlier checkpoints, only checkpoints retained outside Trace would reveal it. Retaining anchors is part of the control.
- External-action enforcement is non-bypassable when the protected credential or action is placed behind the Trace enforcement point. A credential left outside it can be used without Trace; Trace can only show that no Trace authorization exists for that use.
- Signing keys are held in platform secret storage today, not an HSM or KMS. There is no independent timestamping or transparency log.
- Reviewers must obtain Trace's public keys through a channel they trust; an old copy of the key list will not show a later key compromise.
- Trace evaluates the state reported to it. It does not discover changes in outside systems that nobody reported.
- No SOC 2, HIPAA or other certification, and no third-party penetration-test certification, is claimed.

6 • Proof

October 10, 2026: the database-owner validation run passed 567 tests across 35 files with zero failed and zero skipped, on an isolated PostgreSQL cluster built from all 55 migrations. The ordinary run passed 427 tests with 140 special-environment skips. The build-blocking bypass scanner reported no bypass, and the production build succeeded. These results validate application and database rules; they are not a certification, a formal penetration test or customer acceptance testing.

Two proof surfaces are open at tracecontinuity.com: the Playground, which shows why a request was allowed, denied or transformed, and the Break Arena, which invites direct attempts to defeat the governance layer.

7 • A scoped pilot

A pilot places one high-risk workflow behind Trace: real authority and delegation, one or two governed actions behind an enforcement point, human approval where required, and evidence the customer retains and verifies independently. Identity-provider offboarding, key custody and network controls are configured in the customer's deployment.

Not a certification

Trace provides controls and evidence. It does not certify compliance with any regulation or framework.