BUYER BRIEF

Every Decision Begins With Authority

Authority, execution evidence and enforcement-coverage visibility for AI agents and enterprise systems.

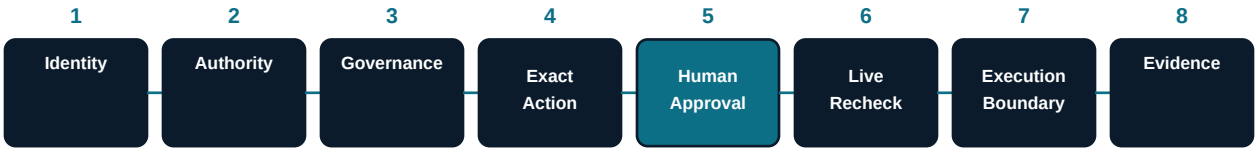
Every Decision Begins With Authority.

Version 6 · 18 November 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 answers three separate questions: who authorized the action, what actually happened, and whether the operation was inside the required enforcement coverage. It provides governed memory, exact-action enforcement and verifiable evidence without claiming visibility or control over systems that never pass through Trace.

2 · The execution path



Authority is re-checked live. Approval applies only when required.

Outcome and coverage remain separate evidence dimensions after the execution boundary.

Identity establishes who is asking. Authority and governance decide whether the exact action may proceed. A separate enforcement point redeems a single-use permission immediately before execution. Evidence then answers what was consumed, dispatched, reported and target-checked. Coverage reporting separately asks whether the route was declared and observed.

3 · Current capabilities

Capability	Current implementation
Execution-time authority	Live credential, person, agent, authority, delegation, scope and execution-right checks
Governed memory	Policy/conditions, tokenization, encrypted vault handling, retrieval rechecks and reported lineage
Suspension and revocation	Reversible suspension stops the next governed request; permanent revocation cannot be undone
Exact-action enforcement	Canonical fingerprint, separate enforcement-point credential, live recheck and atomic single use
Outcome verification	Authorization, consumption, dispatch, reported outcome, target check and unknown states remain separate
Historical evidence	Saved single-statement captures reconstruct recorded knowledge at capture; arbitrary past wall-clock views are refused
Enforcement coverage	Declared routes compared with observed operations, credential mappings and registered bindings
Evidence and exports	Hash-chained evidence, signed packages, checkpoints, coverage JSON and report-generation audit entries
Governance over governance	Protection-reducing changes require a second administrator's approval of the exact change
Matter boundaries	Matters, ethical walls, legal holds and screened evidence reads fail closed

4 · What happened is not one status



Each state answers a different question. None is silently promoted to the next.

Dispatch ≠ target completion. Confirmation requires an explicit target-backed check.

Unknown or unavailable evidence remains unknown or unconfirmed.

State	What it establishes	What it does not establish
Authorization	Live authority and governance permitted one exact action	Execution, dispatch or target completion
Execution consumption	The bound enforcement point atomically redeemed the single-use permit	That the executor ran or the target changed
Dispatch	The request was sent or the executor returned	Successful completion of the intended effect

State	What it establishes	What it does not establish
Reported outcome	The enforcement point reported confirmed, failed or unknown	Independent observation by Trace
Target confirmation	The bound enforcement point supplied a target receipt, read-back or reconciliation; optionally an Ed25519 receipt signed by the target system or a connector, verified by Trace against a governed registered key	Universal proof about arbitrary external systems
Unknown / unconfirmed	The necessary outcome or target evidence is absent, failed or unavailable	A hidden success or a hidden failure

5 · Why buyers care

- **Authority at the moment of consequence.** A login or earlier approval is not treated as permanent permission.
- **Honest execution evidence.** A sent request is not represented as a completed target effect.
- **Coverage you can review.** Known and unknown enforcement gaps remain visible rather than disappearing behind a green badge.
- **Evidence a reviewer can check.** Signed packages, offline verification and externally retained checkpoint anchors support independent checking.
- **Governance over governance.** One administrator cannot quietly weaken an important protection alone.

6 · A scoped pilot

Use one synthetic consequential workflow with separate agent and enforcement-point credentials. Declare the route and inventory scope; test allow, deny, tampering, replay, wrong credentials, mid-action suspension, dispatch without confirmation, explicit target verification and an undeclared observed operation. Export the coverage JSON and signed evidence. Review customer-side credential and route gaps before any production claim.

7 · Verification

Reverified 18 November 2026: 633 ordinary tests passed with 208 environment-dependent tests skipped; 838 isolated-database tests passed with three port-gated affiliate tests skipped, and those three passed separately. Twenty-nine named historical-evidence checks passed, including atomic rollback, privacy, concurrency, replay, tamper and later-key-revocation cases. Live production synthetic memory write/read, cross-tenant refusal and revoked-key refusal passed. The full hosted signed external-action flow remains unestablished because no external-action authority or action records are provisioned. These are not certification results.

The separate 4 November internal staging benchmark remains a staging result: approximately 1.5 seconds per complete authorize → redeem → outcome → evidence workflow, approximately 3.17 workflows/second, concurrency 10, 25 and 50, and 160/160 successful workflows. Replay, cross-tenant and mid-action suspension attempts were refused; that run reported 714/714 security tests. It was not rerun for this brief and does not establish production capacity, sustained throughput or support for 1,000+ agents.

8 · Stated limits

- Trace cannot detect or prevent an action occurring entirely outside its integration and network visibility. Customers must control credentials, IAM, network egress, jobs, alternate APIs and manual paths.
- A registered enforcement point or an observed governed request does not prove that all customer routes are governed. Inventory completeness and exclusive credential custody remain customer declarations until independently established.
- Target confirmation is attributed to the bound enforcement point. An unsigned target-evidence hash fingerprints reported content only. A signed receipt is verified by Trace against a registered key and labeled target-system-signed or connector-signed; it cannot prove the signer's key was never stolen.
- Signed checkpoints do not stop a database owner from changing data. Externally retained anchors make later alteration or deletion of committed history detectable; later activity is covered once a subsequent checkpoint is retained.
- Signing keys are held in managed secret storage, not an HSM. Tenant vault keys remain in the application database. No independent timestamping or public-ledger anchoring is claimed.
- Trace evaluates reported state and reported lineage. It does not discover hidden derivations, terminate arbitrary external processes or recall data/actions already released.
- Historical reconstruction requires a previously saved capture. Append-only rows, alleged event dates or an arbitrary as_of time cannot establish what was visible in the past. Signed statements attribute claims; they do not prove physical effects or external wall-clock time.
- Sensitive-data recognition is pattern/context-based and not exhaustive identification of arbitrary prose. No compliance certification or universal security guarantee is claimed.

Evidence, not certification
Trace provides controls and evidence. It does not certify compliance, prove every customer route, or guarantee an external outcome.