ENTERPRISE EVALUATION

Pilot, Technical FAQ & Security Questionnaire

A controlled evaluation plan and current answers on authority, outcomes, coverage and security.

Every Decision Begins With Authority.

Version 1 · 17 November 2026 · Trace Continuity Labs · tracecontinuity.com
Patent Pending — U.S. Provisional Patent Application No. 64/137,172. Not a certification.

Trace Continuity Labs — Enterprise Pilot, Technical FAQ & Security Questionnaire

Version 1 · 17 November 2026 · Current partner-facing reference

This guide uses the same capability and limitation model as Buyer Brief v5, Technical Brief v9 and Architecture Brief v6. It is not a certification, legal opinion or guarantee of security.

1. The three evaluation questions

Who authorized the action?

Trace resolves the presented credential to a tenant and pinned authority, then checks person and agent status, key expiry, reversible suspension, permanent revocation, delegation ancestry, scopes, execution rights, policy, current conditions and matter boundaries at execution time. High-risk actions can require a different eligible person to approve the exact action. Redemption checks live authority again.

What actually happened?

Trace does not collapse the answer into “success.” It records authorization, single-use execution consumption, dispatch, enforcement-point-reported outcome and optional target-backed confirmation separately. A resolved request is dispatch, not proof of completion. A target-confirmed state requires an explicit target receipt, read-after-write or reconciliation report from the bound enforcement point. Missing, failed or unavailable checks remain unknown or unconfirmed.

Was the operation covered by required enforcement?

Governance → Coverage compares append-only route and inventory declarations with registered enforcement bindings and Trace-observed operations. It surfaces unregistered live keys, multiple credentials, unmapped observed operations, stale reviews, ambiguous selectors and incomplete sources. A registered enforcement point alone does not prove every customer execution path is governed.

2. Controlled pilot plan

Scope

Choose one consequential synthetic workflow: for example, a record change, payment-shaped action or disclosure. Use one requesting agent credential and a separate enforcement-point credential. Define the operation, tool, target type, policy, required approval, expected evidence and customer-owned target check.

Preparation

1. Provision a synthetic tenant, narrow delegated authorities and expiring keys.

2. Register the agent and enforcement point; keep credentials server-side and separate.
3. Configure default-deny policy and any exact-action human approval.
4. Declare the pilot inventory scope and protected route in Governance → Coverage.
5. Remove alternate synthetic credentials and disable alternate execution paths that the pilot claims to govern.
6. Arrange signed evidence/checkpoint export and retain public keys and anchors outside Trace.

Acceptance sequence

Test	Required observation
Valid action	Authorization issued; live redemption succeeds once; executor runs once
Changed action	Fingerprint mismatch; executor does not run
Replay	Second redemption refused; no second execution
Wrong credential or enforcement point	Refused; executor does not run
Mid-action suspension or revocation	Redemption refused; no execution
Dispatch only	Dispatch recorded; target outcome remains not checked
Target check unavailable	Unknown/could-not-establish remains visible; never upgraded to confirmed
Target receipt or read-back	Append-only target-confirmation evidence, attributed to the enforcement point
Undeclared observed operation	Reported as missing from the declared route inventory
Nonexclusive credentials	Known bypass risk remains visible even when governed traffic is observed
Evidence export	JSON coverage report plus audit entry; signed package/checkpoint verification remains VERIFIED, FAILED or INCOMPLETE as applicable

Pilot exit criteria

Review the exact route inventory, credential custody, every observed refusal, dispatch/outcome/target states, report truncation flags and customer-side gaps. Do not convert a scoped synthetic pass into production readiness, enterprise-wide coverage or certification.

3. Technical FAQ

Does authorization prove execution?

No. Authorization records a decision. Atomic consumption records that the single-use execution permit was redeemed. Dispatch and outcome are separate reports.

Does dispatch prove the target completed the operation?

No. Dispatch means the request was sent or the executor returned. Use an explicit target receipt, read-after-write or reconciliation when the intended effect matters.

Is target confirmation independent observation by Trace?

No. The bound enforcement point supplies the target-check method, evidence hash and observation time. Trace preserves and attributes that report; it does not independently observe arbitrary external systems.

What does a registered enforcement point prove?

It proves a registered binding that can participate in the exact-action protocol. It does not prove all customer APIs, jobs, integrations, credentials or manual paths use it.

Can Trace automatically discover ungoverned routes?

No. The report compares customer declarations with operations Trace observed and registered credentials. It can reveal unmapped observed operations and unregistered live Trace keys, but it cannot see actions entirely outside Trace.

Does multiple-credential visibility prove a bypass occurred?

No. Multiple live keys are a review signal. The report keeps credential custody and observed route coverage separate.

What happens when the inventory is incomplete or stale?

The report labels incompleteness, staleness and unknown coverage. It does not produce a blanket protected claim or a misleading enterprise-wide percentage.

Are coverage reports exported?

Yes. The authenticated Governance → Coverage screen supports JSON export, and every generated report writes an audit entry. Automatic email or paging alerts are not implemented.

Does Trace provide governed memory as well as action control?

Yes. Governed memory includes execution-time authority, policy and condition checks, sensitive-data tokenization, tenant-scoped encrypted vault handling, retrieval rechecks and reported derivation lineage. Trace governs reported lineage only.

What is the difference between suspension and revocation?

Suspension is reversible through governed controls and stops the next governed request. Permanent revocation cannot be undone. Neither recalls data already released or an external effect already completed.

Does Trace integrate with ServiceNow?

Trace provides the public exact-action API used by a separately built ServiceNow application. Trace staging records support ten governance cycles on 26 October. There is no built-in ServiceNow connector inside Trace, ServiceNow certification or Store listing claim.

Are LangChain, CrewAI, n8n or MCP enterprise adapters included?

No turnkey enterprise framework adapter or MCP proxy is claimed. Any server-side framework can call the documented HTTPS/JSON boundary. The standalone Red-Team Lab's synthetic integrations are separate from enterprise production connectors.

4. Security questionnaire

Credential and authority binding

Each Trace API key identifies a tenant, creator and pinned authority. Offboarding preserves that pin through the person-suspension route and configuration gate, preventing fallback to another eligible authority held by the same administrator. New keys require expiry; lifetime extension is a protection reduction requiring second-person approval.

Protected evidence reads

Audit list, condition history and provenance lineage require live `memory:read` / `read` authority. External-action evidence requires `external:execute` / `execute`. Matter-bound rows are screened before return. Missing or unreadable matter state fails closed. These evidence checks do not add work to authorize or redeem.

Matter-wall and preservation failures

Matter, ethical-wall, access-grant and preservation lookup errors deny distinctly. A query error is not treated as “no wall,” and unknown preservation state blocks destruction.

Protected-memory reads

Ordinary authenticated and anonymous client roles have no direct protected-memory SELECT. A migration makes the revocation explicit, and a fresh isolated-database test verifies direct reads fail. Application reads still use the execution gate and live evidence-read controls.

Bypass scanning

The source scanner covers governed memory, configuration, person suspensions, coverage declarations, provenance and exact-action approval details. It is defense-in-depth for the repository, not discovery of customer infrastructure or proof that every future route is safe.

Evidence integrity

Per-action evidence is hash-chained. Signed packages verify offline. Tenant-wide signed checkpoints commit to committed history; customers should retain anchors outside Trace. Trace refuses to sign when its committed-history check fails. Database owners can still alter data; the control is tamper evidence, not absolute prevention.

Key custody

Signing secrets are in managed platform secret storage, not an HSM. Tenant vault keys are in the application database. External KMS/HSM custody is not deployed. No independent timestamping or public-ledger anchor is claimed.

Tenant isolation

Tenant identity comes from the credential, not the request body. Cross-tenant bindings are refused, and isolated tests exercise direct access and cross-tenant route/enforcement-point references. External October testing covered specific cross-tenant read scenarios, not every possible route or storage-layer attack.

5. Fresh verification record

Reverified on 17 November 2026:

- **572 passed, 195 skipped** in the complete ordinary serial suite; skipped owner-dependent suites are not counted as passes.
- **16/16** enforcement-coverage and external-action tests passed on a newly initialized isolated database after 66 migrations.
- **51/51** focused coverage, evidence-read and bypass-scanner checks passed.
- Static gate scan passed.

These are synthetic source and isolated-database results, not production acceptance, an accredited assessment or certification. The October external register remains 14 PASS / 3 FAIL / 1 BLOCKED plus 2 PASS / 1 NOT TESTED. F-01 was retested on staging; F-02/F-03/F-04 remain reported staging repairs without independent retest or production parity confirmation.

6. Remaining limitations

- Trace cannot detect or prevent actions completely outside its visibility and control.
- Customer credential custody, route completeness, network egress and target reconciliation determine real deployment coverage.
- No evidence for 1,000 or 10,000 simultaneously active agents; the November staging benchmark reached concurrency 50 only.

- No automatic agent or hidden-lineage discovery, external process termination or recall of completed effects.
- Pattern-based sensitive-data detection is not exhaustive recognition of arbitrary prose.
- No self-hosted distribution, turnkey MCP proxy, built-in SIEM connector, formal uptime objective or compliance certification is claimed.