# ATTESTA

## Machine-Readable Trust for Modern Enterprises

| | |
|---|---|
| **Category**<br>Trust Assertion Infrastructure | **Primary surface**<br>ATTESTA : Respond (verified security responses) |
| **Core idea**<br>Versioned, evidence-linked security assertions published through dedicated surfaces. | **Outcome**<br>80-90% reduction in engineering time spent on customer security questionnaires. |

This pack summarises the platform, naming system, surfaces, roadmap, and an implementation plan suitable for pilot customers.

# Overview

**ATTESTA** is Trust Assertion Infrastructure: a governance-grade trust layer that defines what an organisation can claim, proves it with evidence, and keeps those claims consistent over time.

The wedge is not an RFP tool. ATTESTA starts with customer security responses because that is where trust is demanded and time is wasted. The platform wins by making answers provable, repeatable, and conservative under scrutiny.

## Category definition

**Trust Assertion Infrastructure** is the system by which an organisation defines, versions, verifies, and publishes its security and compliance claims in a machine-readable, auditable form.

## Core objects

| Assertion | A formal claim the company makes (e.g., encryption at rest). |
|---|---|
| Control | A security mechanism that backs an assertion (mapped to frameworks). |
| Evidence | Artifacts proving controls (policies, audits, diagrams, tickets). |
| Trust State | Freshness + confidence + review status for each assertion. |

# Surfaces and naming system

ATTESTA is the platform. Everything else is a surface, named as **ATTESTA : [Surface]** to keep the system coherent as it expands.

| Surface | Purpose |
|---|---|
| **ATTESTA : Respond** | Verified security responses for customer due diligence and questionnaires. Evidence-linked answers, conservative flagging, engineer sign-off, and export to Excel/Word/PDF. |
| **ATTESTA : TrustHub** | Customer-facing trust center derived from the same assertions. Controlled disclosure, approved language, and access control. |
| **ATTESTA : Audit** | Audit preparation, traceability, control mapping, and assertion history diffs for security and compliance teams. |
| **ATTESTA : Insight** | Executive reporting on trust state, coverage, drift, and risk deltas for CISO/CTO/Legal and boards. |
| **ATTESTA : API** | Machine-readable assertions for vendor risk automation and AI-to-AI verification (18-24 month horizon). |

## How Respond differs from RFP tools

Traditional RFP platforms store reusable text. ATTESTA stores **assertions with evidence lineage**. Outputs are derived from the assertion registry and are conservative when evidence is missing.

| Dimension | Typical RFP tool | ATTESTA |
|---|---|---|
| Source of truth | Past answers | Assertions + controls + evidence |
| Risk posture | Optimise completion | Flag-first, no bluffing |
| Accountability | Sales-led workflow | Engineer review and sign-off |
| Audit defensibility | Weak | Strong (traceable lineage) |

# Platform roadmap (12-24 months)

Sequencing: sell speed first, earn trust second, become infrastructure third.

**0-6 months** **Respond and export**

- Document ingestion (audits, policies, technical docs) with scoped collections.
- Evidence-linked answers with strict uncertainty flagging.
- Review workflow and robust export to Excel/Word/PDF.
- Consistency enforcement across customers and questionnaires.

**6-12 months** **Assertion registry and TrustHub**

- Canonical assertions with versioning and control mappings (SOC 2/ISO/NIST).
- Customer trust center derived from assertions with controlled disclosure.
- Follow-up response handling and reusable, shareable security answers.

**12-18 months** **Continuous trust**

- Assertion freshness monitoring and drift indicators.
- Audit mode with evidence checklists and change diffs.
- Executive reporting on trust state and risk deltas.

**18-24 months** **Machine trust interface**

- API-first machine-readable assertions.
- Integrations for vendor risk systems and procurement automation.
- Agent-readable trust verification patterns.

## Success metrics to track

| Metric | Target |
|---|---|
| RFP/questionnaire completion time | Reduce by 80-90% |
| Engineer review burden | Review only flagged items; low churn edits |
| Answer consistency | No contradictions across customers |
| Evidence coverage | Growing % of assertions backed by artifacts |
| Sales cycle impact | Shorter security stage; faster deal velocity |

# Pilot implementation plan

A pragmatic plan for a first pilot customer, designed to minimise risk while delivering immediate value.

## Week 1: Scope and ingestion

• Agree initial frameworks and a target questionnaire set (e.g., SOC 2 aligned).
• Ingest authoritative artifacts (policies, audit report, architecture docs).
• Define redaction rules and access permissions.

## Week 2: Assertion registry baseline

• Create initial assertion set (50-150 assertions) from materials.
• Map assertions to controls and tag evidence sources.
• Set trust state defaults and review ownership.

## Week 3: Respond surface operational

• Upload two real customer questionnaires and auto-generate responses.
• Tune templates and approved language, enforce conservative flagging.
• Export and validate with security/engineering sign-off.

## Week 4: Measure and harden

• Measure time saved, flag rate, and edit rate.
• Harden RBAC, audit logs, and retention settings.
• Prepare TrustHub content or reusable response packs if desired.

## Security and deployment notes

Deployment patterns should match document sensitivity: SaaS, VPC, or on-prem. ATTESTA should support scoped collections, redaction, RBAC, approval workflows, and full audit logs. Where required, restrict model access to minimise data exposure.

## Procurement and legal readiness

Provide a standard security summary: data handling, retention, access controls, incident response, and subprocessor list. Emphasise conservative answer behaviour and evidence lineage to reduce customer risk.