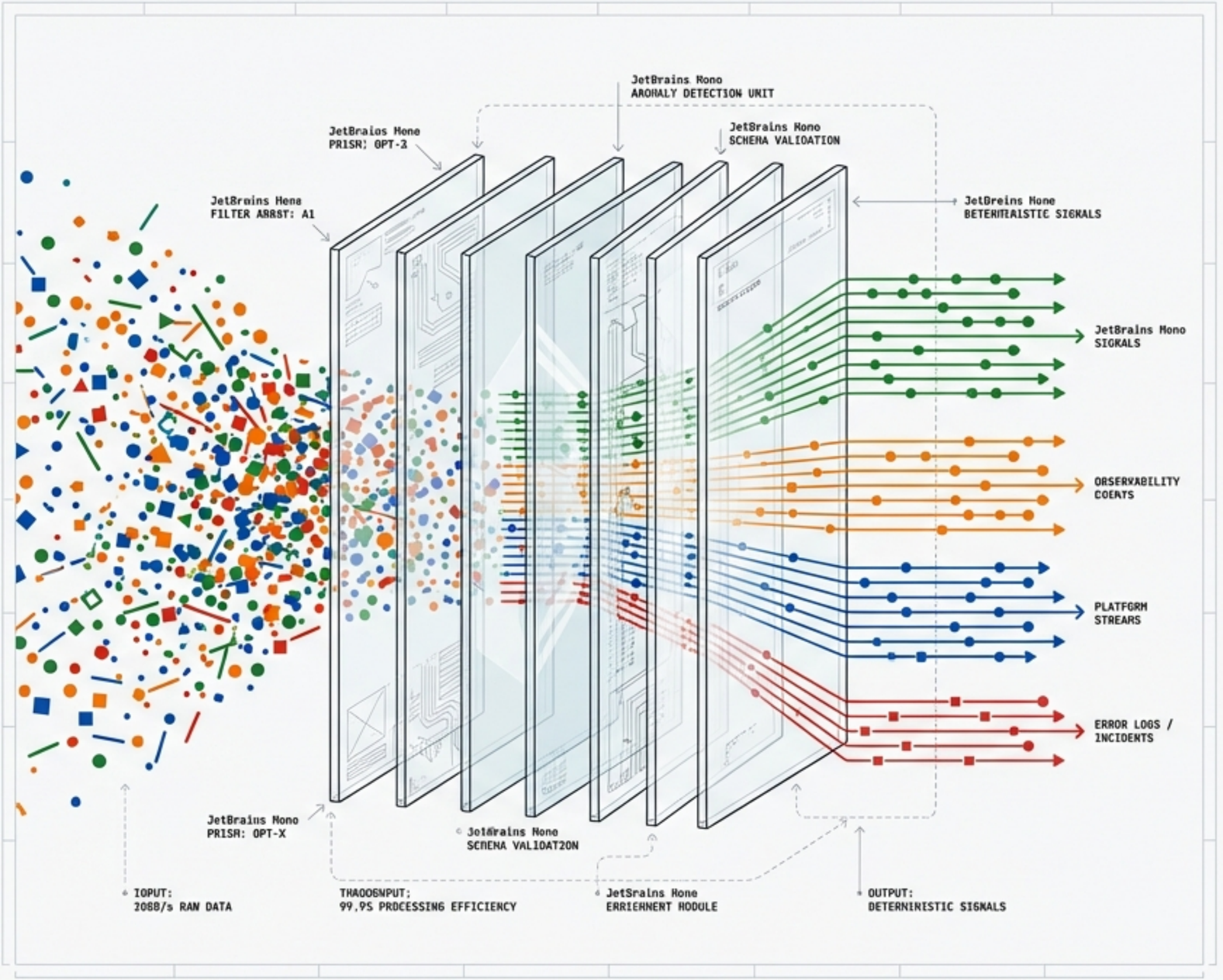
Signal Factory

Out-of-Band Observability Architecture

From Immutable Streams to Deterministic Signals (Pattern 1 Implementation)

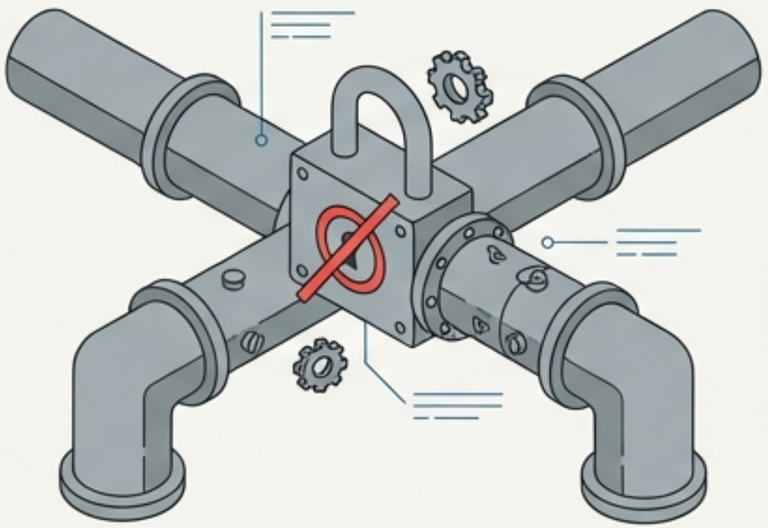


Pattern 1: Out-of-Band Enforcement. Designed for environments where Producers and the Central Streaming Platform are immutable.

NotebookLM

The Constraint Determines the Pattern

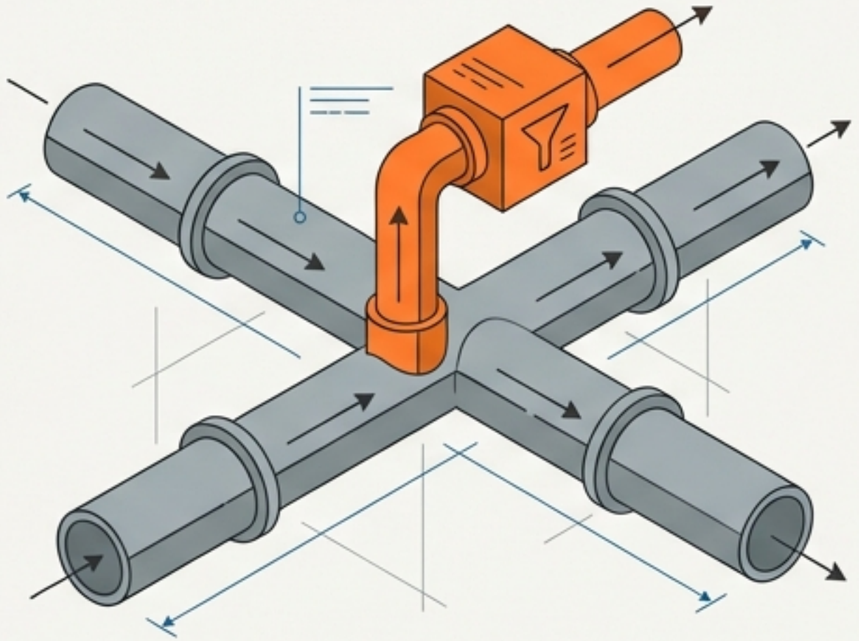
The Constraint



1. **Immutable Producers:** Services cannot be modified to add metadata.
2. **Immutable Platform:** Central Streaming Platform does not support new hooks.

🚫 **Status:** No write-path interception possible.

The Solution: Pattern 1

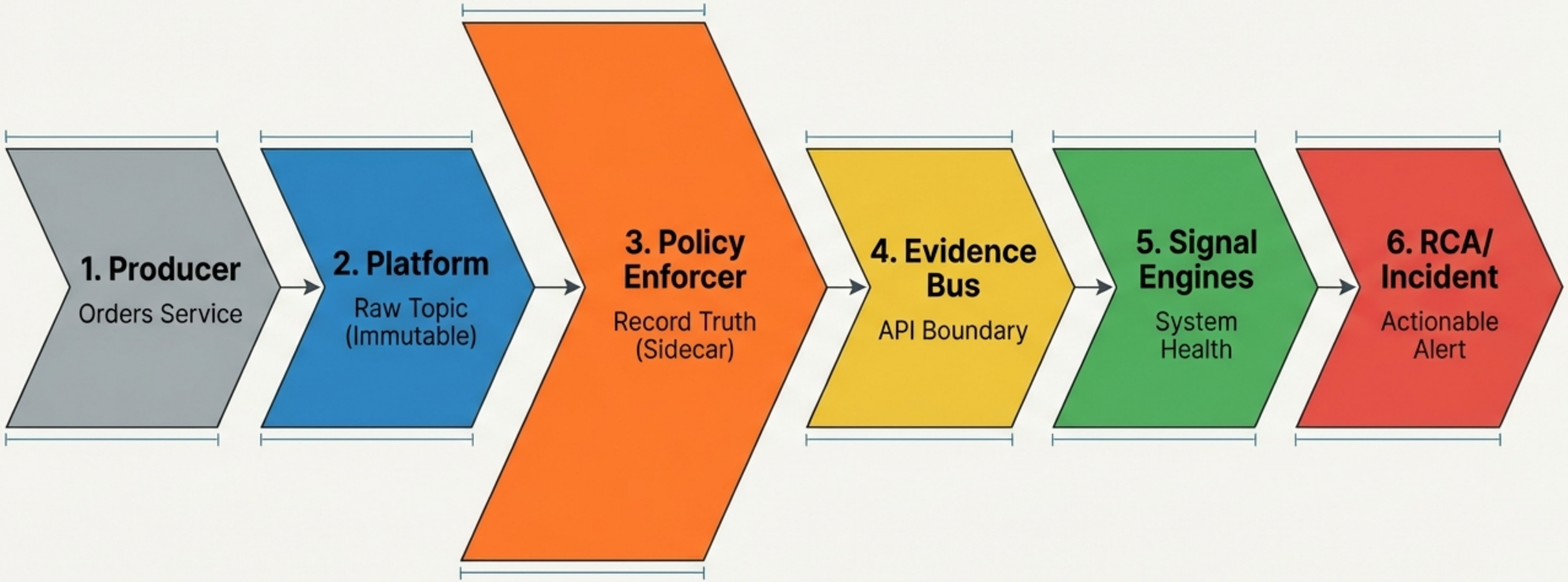


1. **Sidecar Architecture:** Tapping the raw stream post-publish.
2. **Pre-consumption Enforcement:** Logic moves from the write-path to the read-path.

✅ **Goal:** Gateway-grade prevention without Gateway placement.

NotebookLM

The Data Journey: From Raw Event to Incident



The Evidence Bus decouples validation logic (Truth) from alerting logic (Health), preventing logic drift.

NotebookLM

Separating Record Truth from System Health

Policy Enforcer

Question: Is this specific record valid?

Scope: Atomic, per-record.

Functions: Schema validation, Contract checks, PII detection.

Output: Immutable Evidence (**PASS**/**FAIL**).

Signal Engines

Question: Is the system healthy?

Scope: Aggregated, time-windowed.

Functions: Volume trends, Freshness SLAs, Anomalies.

Output: Incidents & Signals.

The Enforcer provides the facts. The Signal Engines provide the judgment.

NotebookLM

Evidence is the Only API

Signal Engines never re-validate payloads. They trust the Evidence Event implicitly.

The Immutable Fact
Definitive PASS/FAIL judgment.

Resolved Identity
Uniquely identifies the data asset.

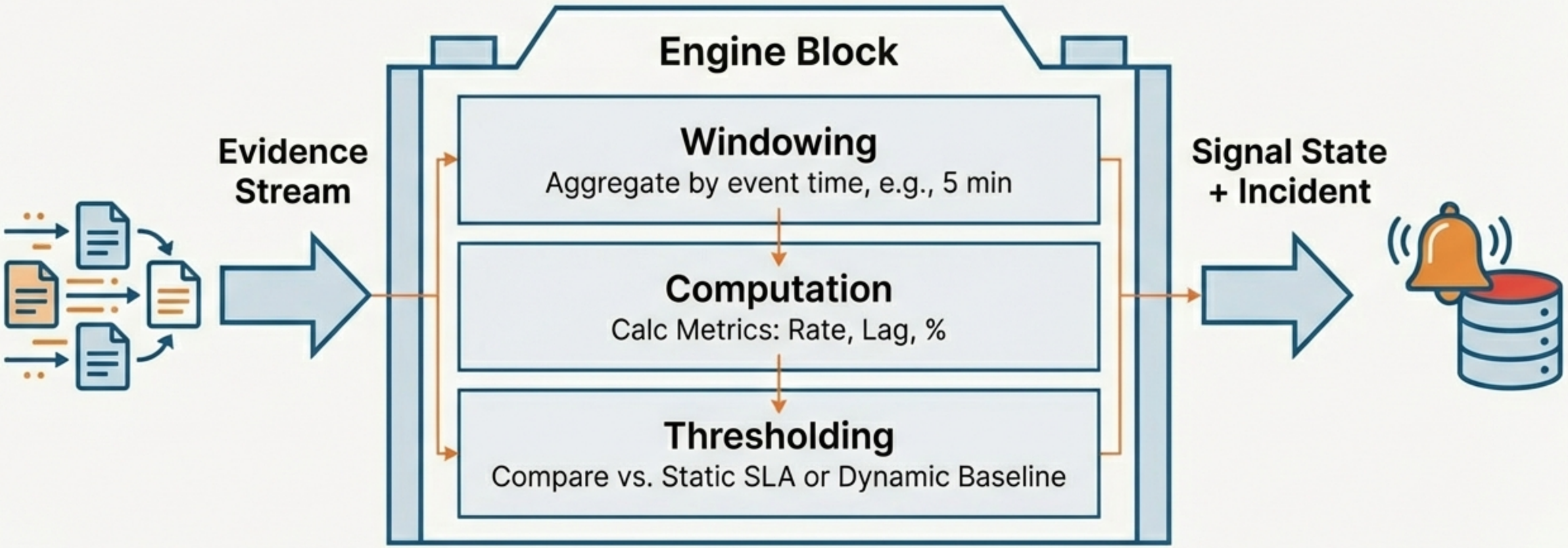
Deterministic Join Keys
Enables precise stream correlation.

RCA Anchor
Links evidence to distributed traces for root cause analysis.

Links evidence to distributed traces for root cause analysis.

NotebookLM

Inside a Signal Engine

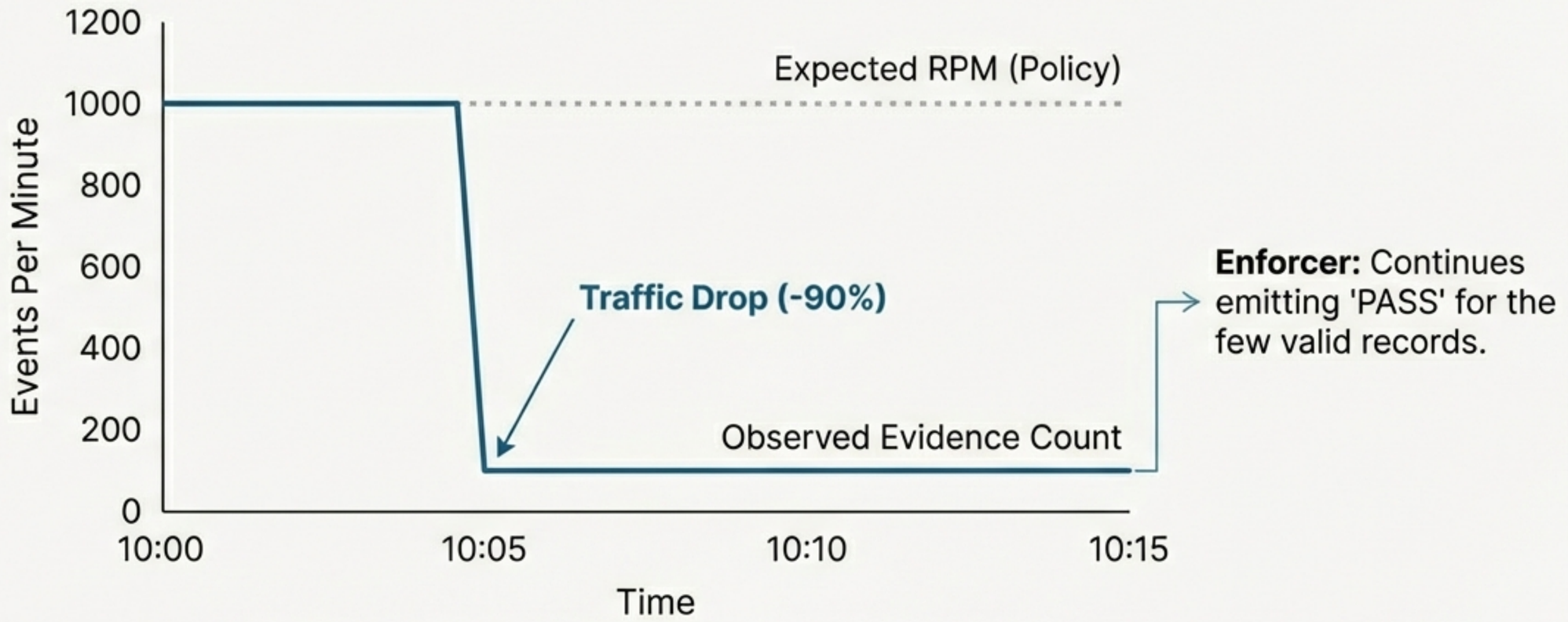


Constraint: Signal Engines consume Evidence, never raw payloads.
They manage thresholds, severity, and alerting logic.

NotebookLM

Scenario 1: The Volume Engine

Detecting Traffic Anomalies on the Orders Service

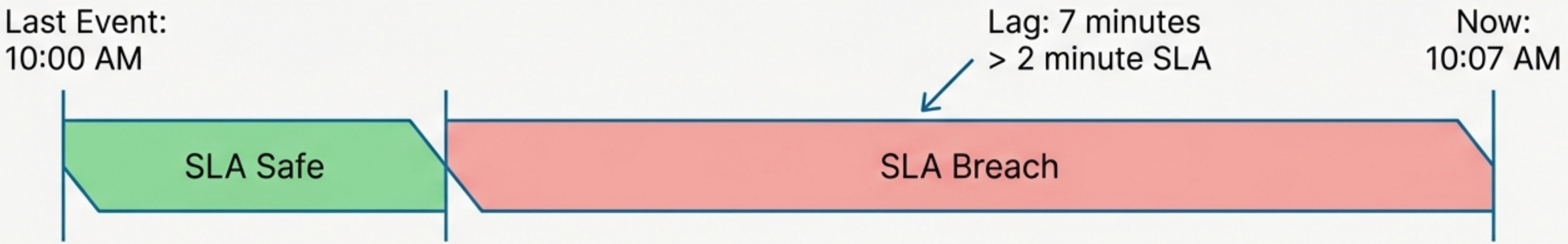


Trigger: VOLUME_DROP Incident (Sev-1)

NotebookLM

Scenario 2: The Freshness Engine

Distinguishing Silence from Failure



Step 1: Compute `now - last_pass_timestamp`

Step 2: Evaluate vs SLA

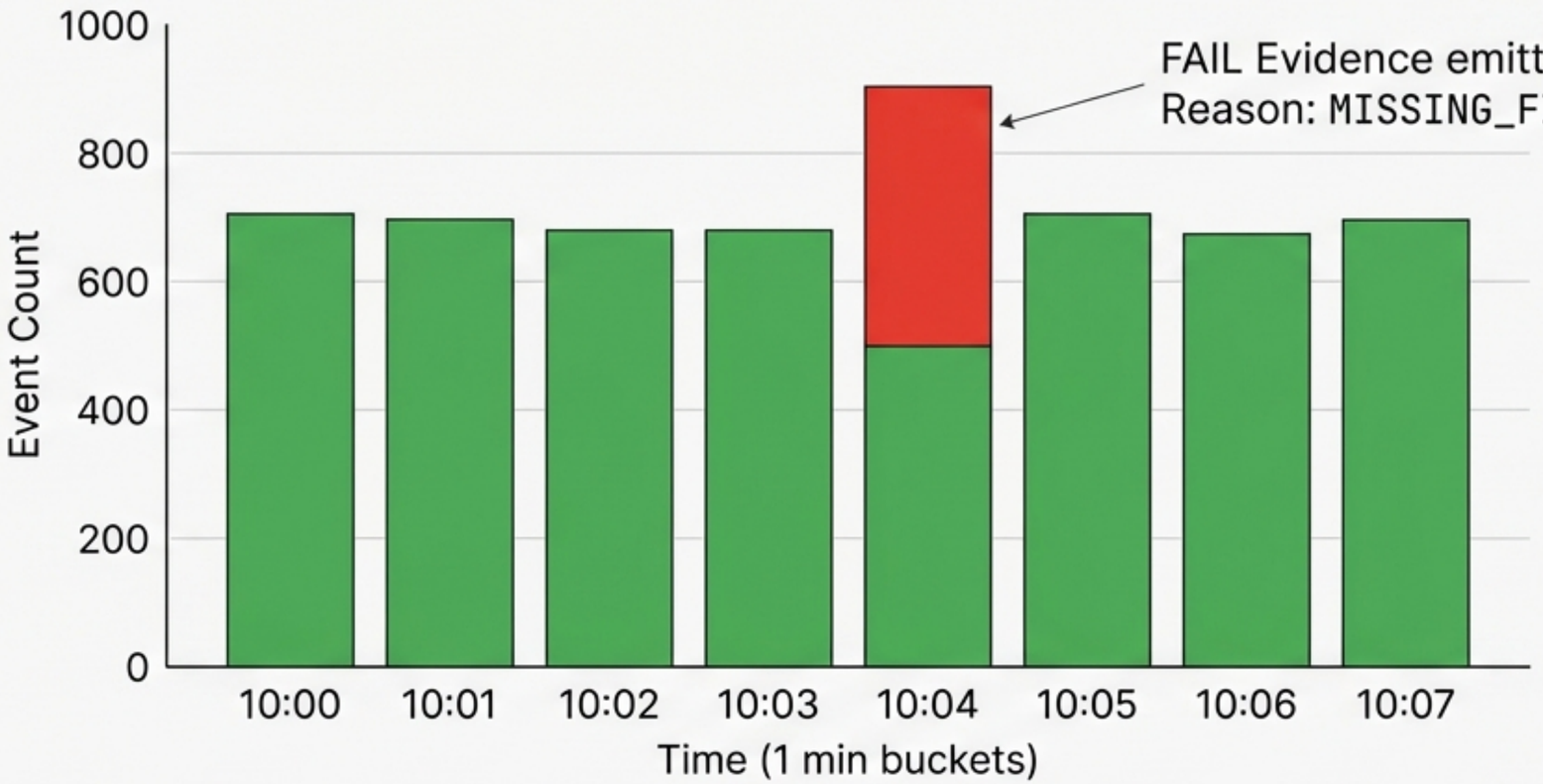
Step 3: Trigger `FRESHNESS_BREACH`

Incident Created. System knows this is 'Silence', not just 'High Failure Rate'.

NotebookLM

Scenario 3: Contract Compliance Engine

Detecting Partial Failures and Regressions



Compliance Rate = PASS / (PASS + FAIL)

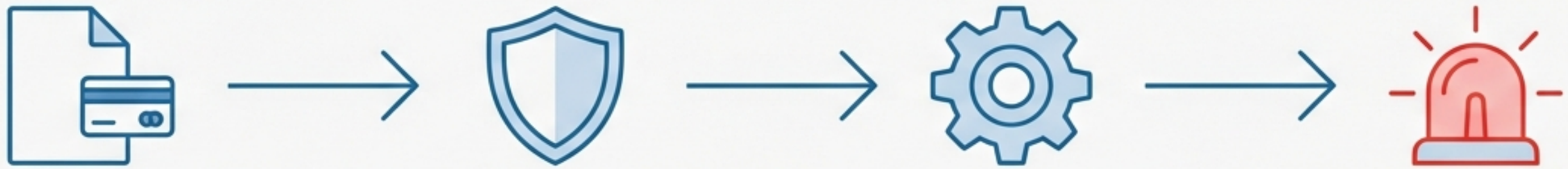
Current Rate: 82%
Policy Threshold: 99.5%

Trigger: CONTRACT_VIOLATION Incident

NotebookLM

Scenario 4: PII Security Engine

Zero-Tolerance Policy Enforcement



credit_card_number detected
JetBrains Mono

Tag: PCI_CLASSIFICATION
Quarantine

Detect 'PCI' tag in stream
JetBrains Mono

SEV-1 SECURITY INCIDENT

Single Bad Record -> Immediate Engine Trigger.

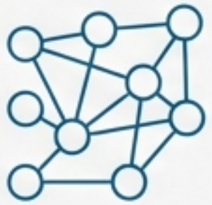
NotebookLM

Purpose-Built Data Models

DynamoDB (State)

Inter

- Purpose: “What is happening right now?”
- Usage: Operational Dashboards, Signal State, Recent Evidence.
- Characteristics: Point lookups, TTL-based.



Neptune (Causality)

Inter

- Purpose: “Why did this happen?”
- Usage: Root Cause Analysis, Blast Radius, Relationships.
- Structure: Graph (Producer -> Dataset -> Signal -> Incident).

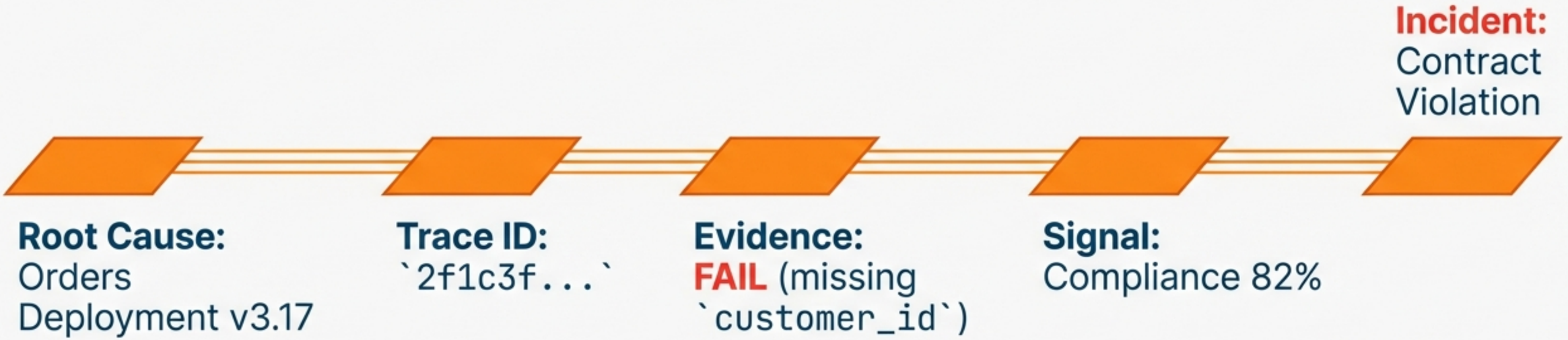
We never write raw time-series to Neptune. It stores relationships and failure signatures.

NotebookLM

Trace-Anchored RCA

Connecting the Symptom to the Source

Inter Tight



The RCA Copilot traverses the graph backwards from the Alert using the Trace ID anchor.

Industrial Precision meets Swiss Editorial

NotebookLM

Failure Modes & Resilience

Observability Failures Must Not Block Business

Enforcer Down

Evidence stops. Engines detect ‘Evidence Gap’. Triggers `OBSERVABILITY_PIPELINE_DOWN`. Business stream continues in Success Green.

Registry Unavailable

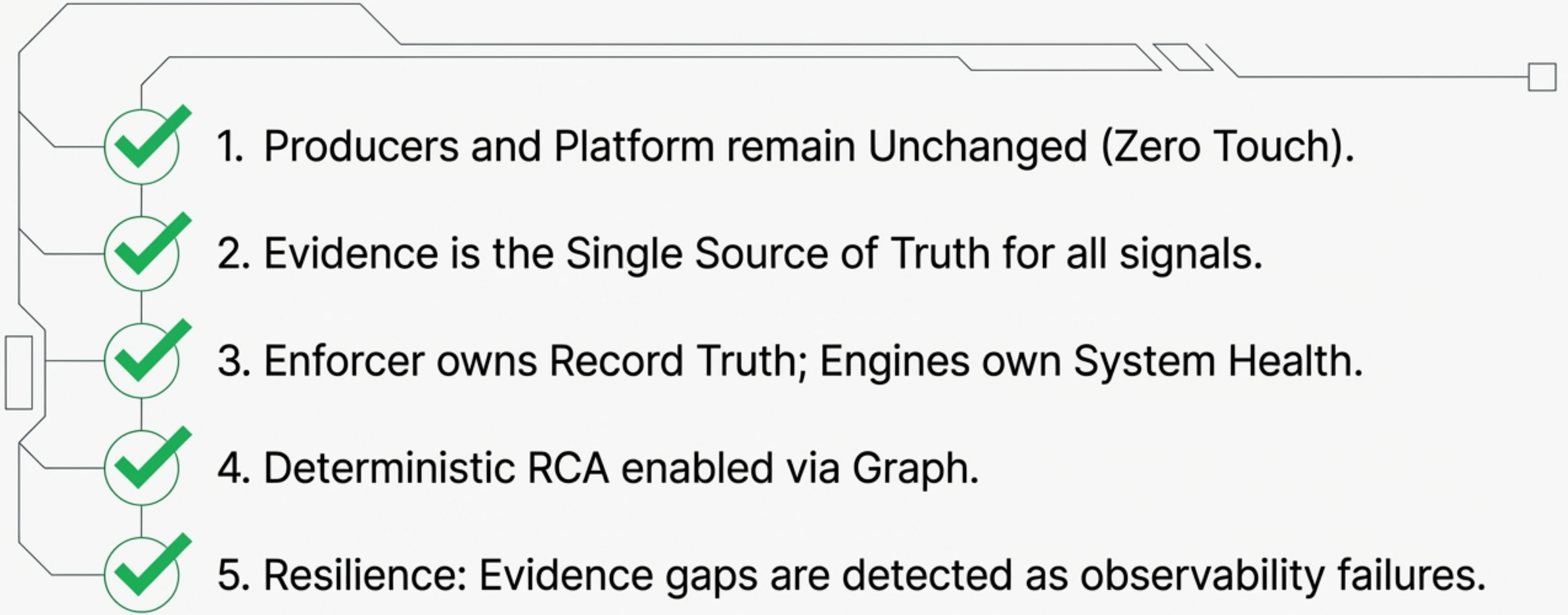
Enforcer cannot validate schema. Emits Evidence with `REGISTRY_UNAVAILABLE`. Engines flag as dependency failure, not producer failure.

Lag Spikes

Engines are ‘Lag-Aware’. Freshness alerts suppressed if consumer lag is high to prevent false positives.

NotebookLM

The Pattern 1 Definition of Done

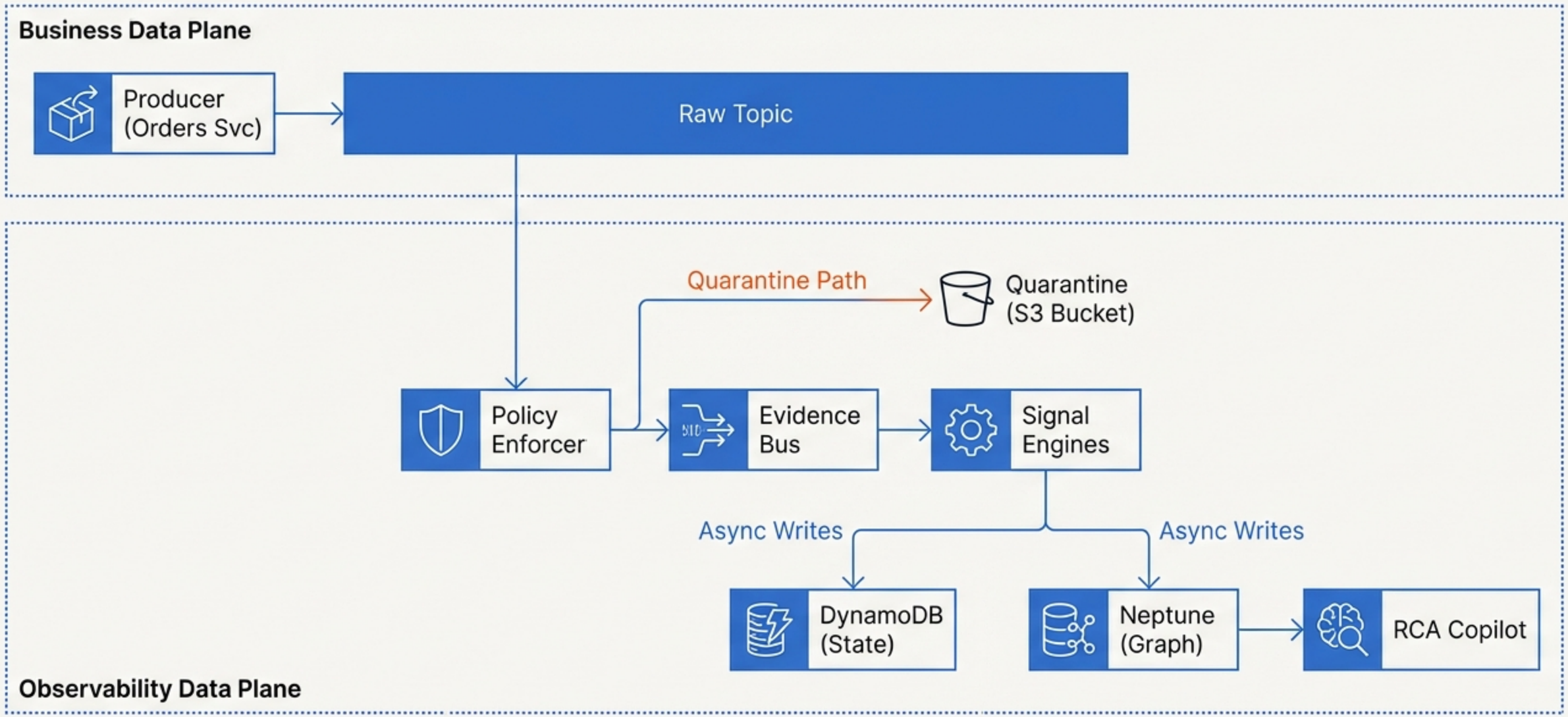


1. Producers and Platform remain Unchanged (Zero Touch).
2. Evidence is the Single Source of Truth for all signals.
3. Enforcer owns Record Truth; Engines own System Health.
4. Deterministic RCA enabled via Graph.
5. Resilience: Evidence gaps are detected as observability failures.

Industrial Precision meets Swiss Editorial

NotebookLM

Architecture Reference



NotebookLM