SkyDefended InfraApp: Distributed Evidence and Detection Architecture

Multi-Plane Topology, Tamper-Evident Evidence, and Zero Trust Sovereignty

Nexocyber NETWORKS

OBSERVABILITY IS NOT AN EXCEPTION TO ZERO TRUST

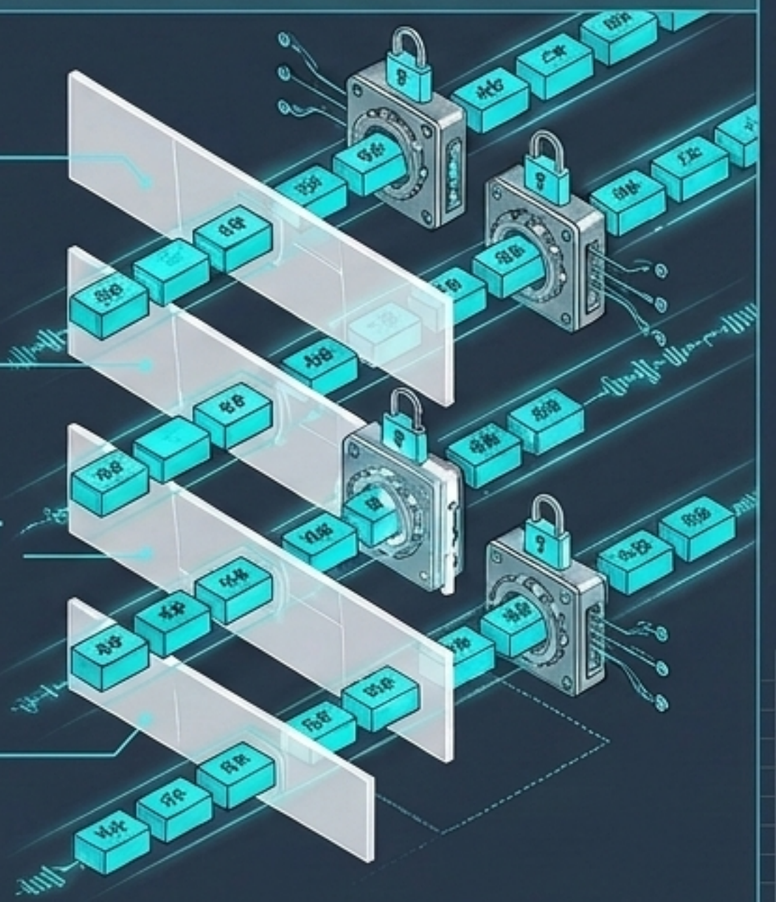
SkyDefended InfraApp abandons the anti-pattern of traditional observability (implicit centralization) to implement a distributed architecture of operational sovereignty.

TRADITIONAL OBSERVABILITY

- BLIND CENTRALIZATION
- IMPLICIT NCN VISIBILITY
- LOG MUTABILITY
- DILUTED OWNERSHIP

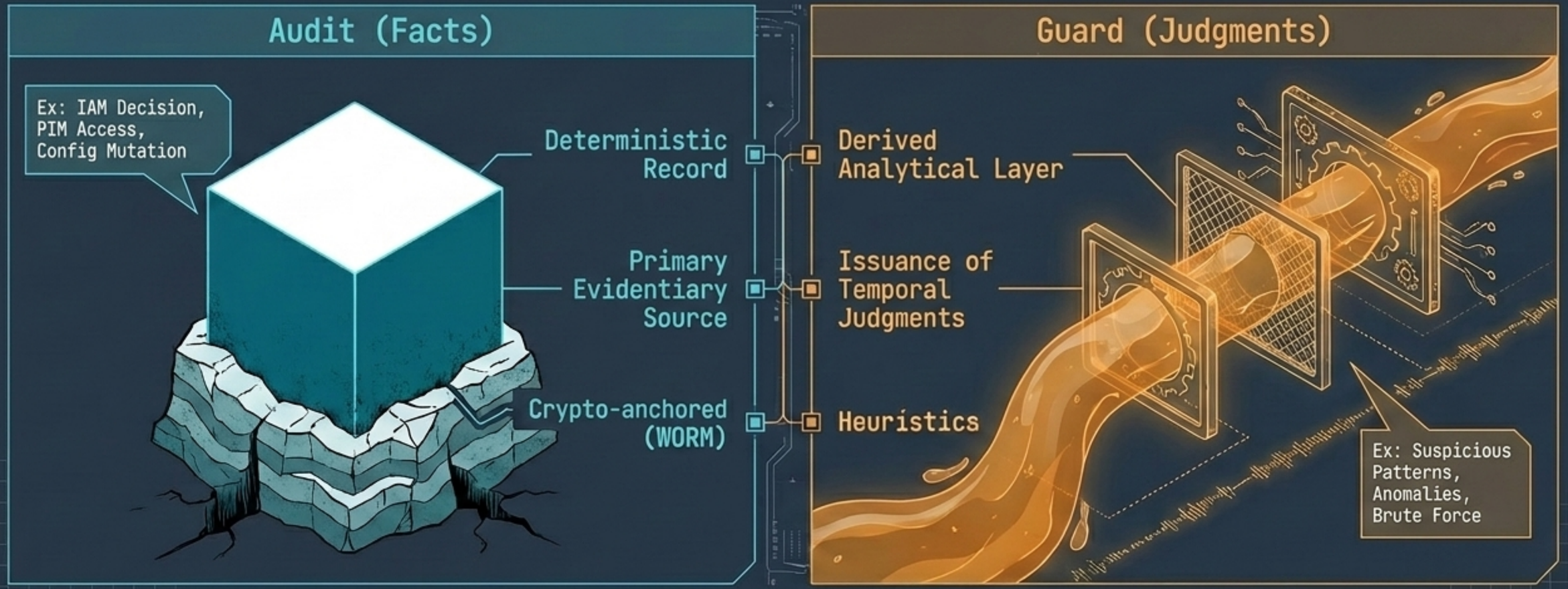
SKYDEFENDED SOVEREIGN EVIDENCE

- MULTI-PLANE TOPOLOGY
- VISIBILITY GOVERNED BY CONSENT
- TAMPER-EVIDENT WORM CHAIN
- STRICT SEPARATION OF OWNERSHIP



The Fundamental Axiom: Strict Separation of Facts and Judgments

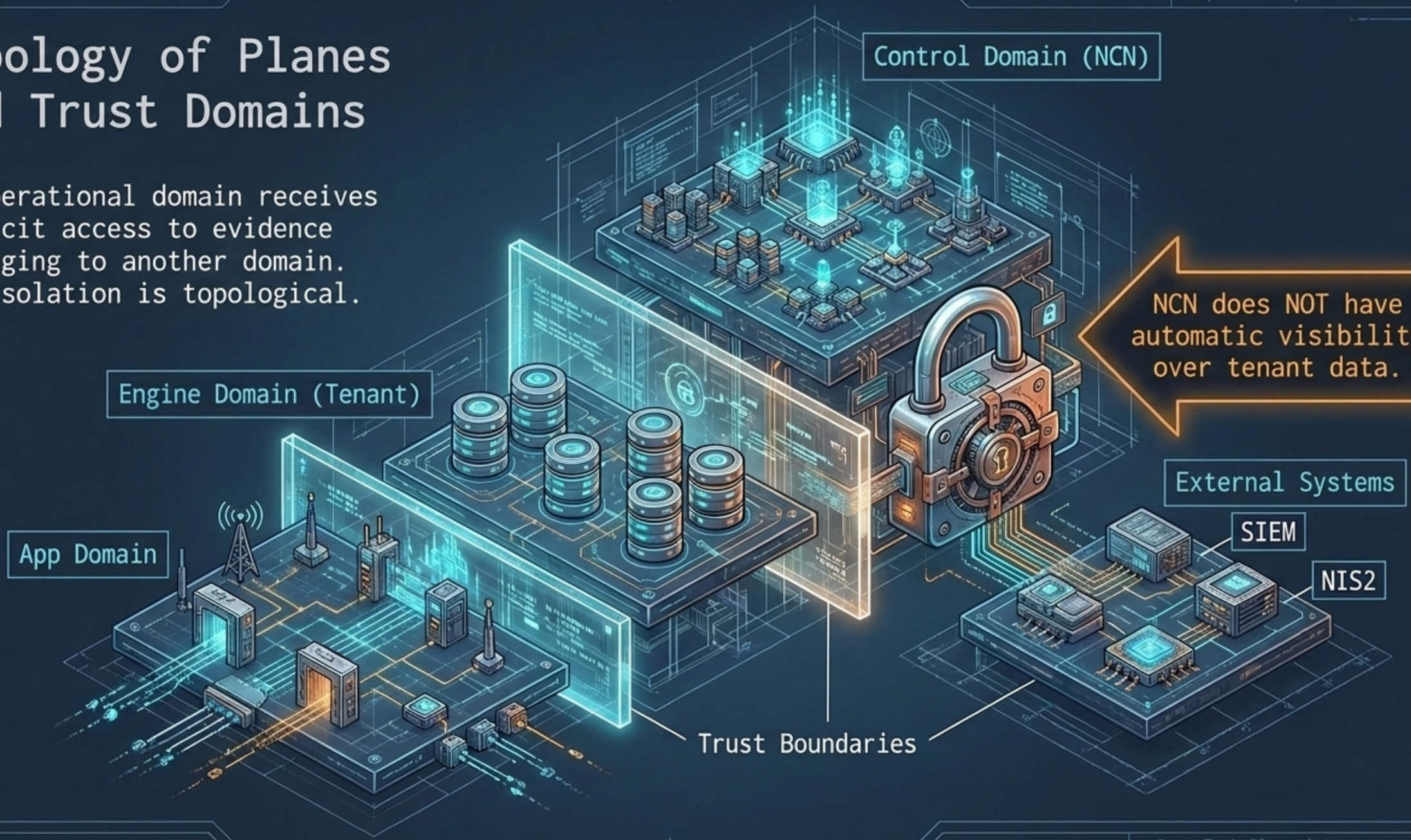
The architecture guarantees its evidentiary value by dividing the analytical domain into two immiscible layers.



Audit is the legal evidence; Guard is the operational layer.

Topology of Planes and Trust Domains

No operational domain receives implicit access to evidence belonging to another domain. The isolation is topological.



Sovereignty Matrix: Ownership Lanes (A-E)

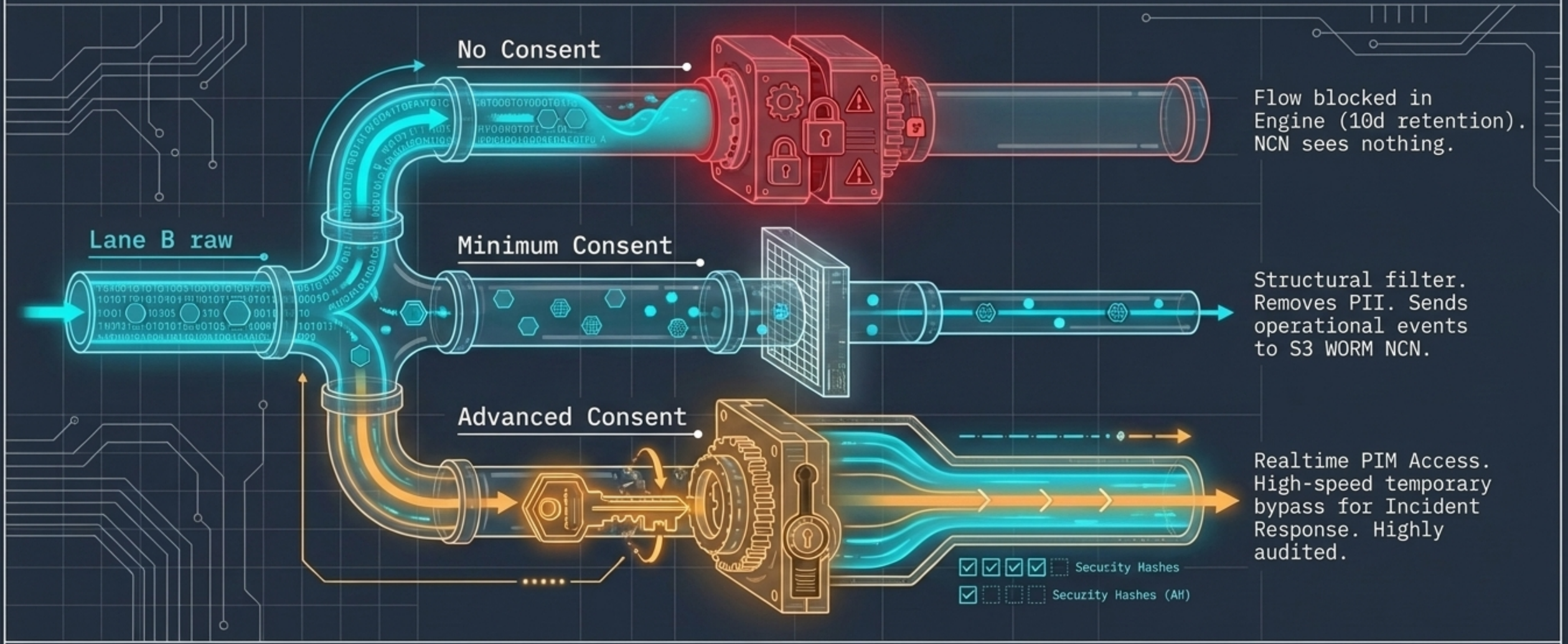
The lifecycle and visibility of evidence are deterministically dictated by its lane of origin.

Heatmap Matrix

Lane	Logical Owner	Hot Persistence	Cold WORM	Default Visibility
Lane A (Control/NCN)	NCN	60d	5y S3 NCN	NCN
Lane B (Tenant Raw)	Tenant	10d Engine	SIEM Tenant	Tenant (Isolated)
Lane C (Engine Infra)	NCN	60d	5y S3 NCN	NCN Platform
Lane D (Operator)	NCN	60d	5y S3 NCN	NCN
Lane E (App Infra)	NCN	60d	5y S3 NCN	NCN Platform

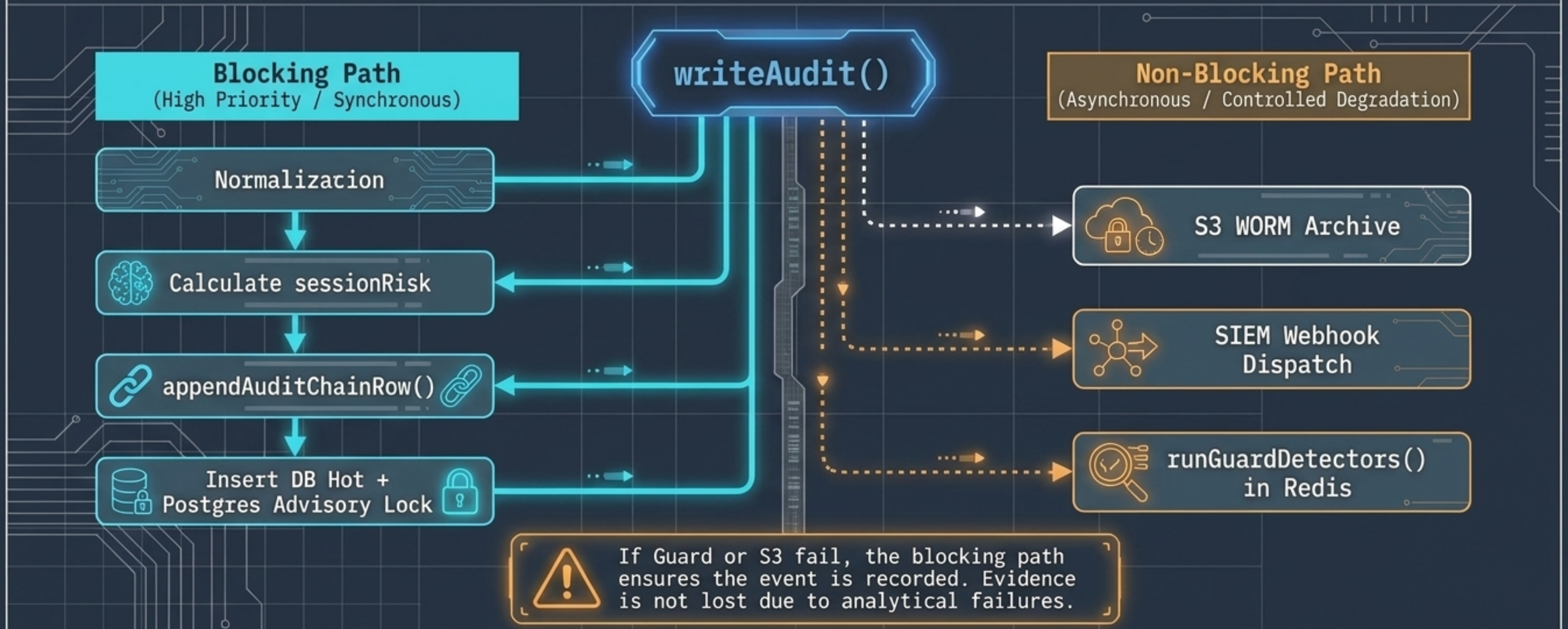
Data Governance: The Consent Mechanism (Tenant Consent)

Visibility over raw Lane B is opaque by default. The flow towards the NCN domain is physically blocked until cryptographic sluices are activated.



Resilient Ingestion: writeAudit() Runtime Pipeline

The canonical entry is designed to guarantee immediate evidentiary registration while isolating asynchronous analytics to prevent cascading failures.



Forensic Integrity: Tamper-Evident Hash Chain

Concurrent forks and retrospective alterations are mathematically impossible through iterative hash anchoring and transactional locks.

```
rowHash =
SHA256(prevHash ||
canonicalSerialize
(row_actual))
```

`pg_advisory_xact_lock`

Prevents simultaneous reads of the same prevHash

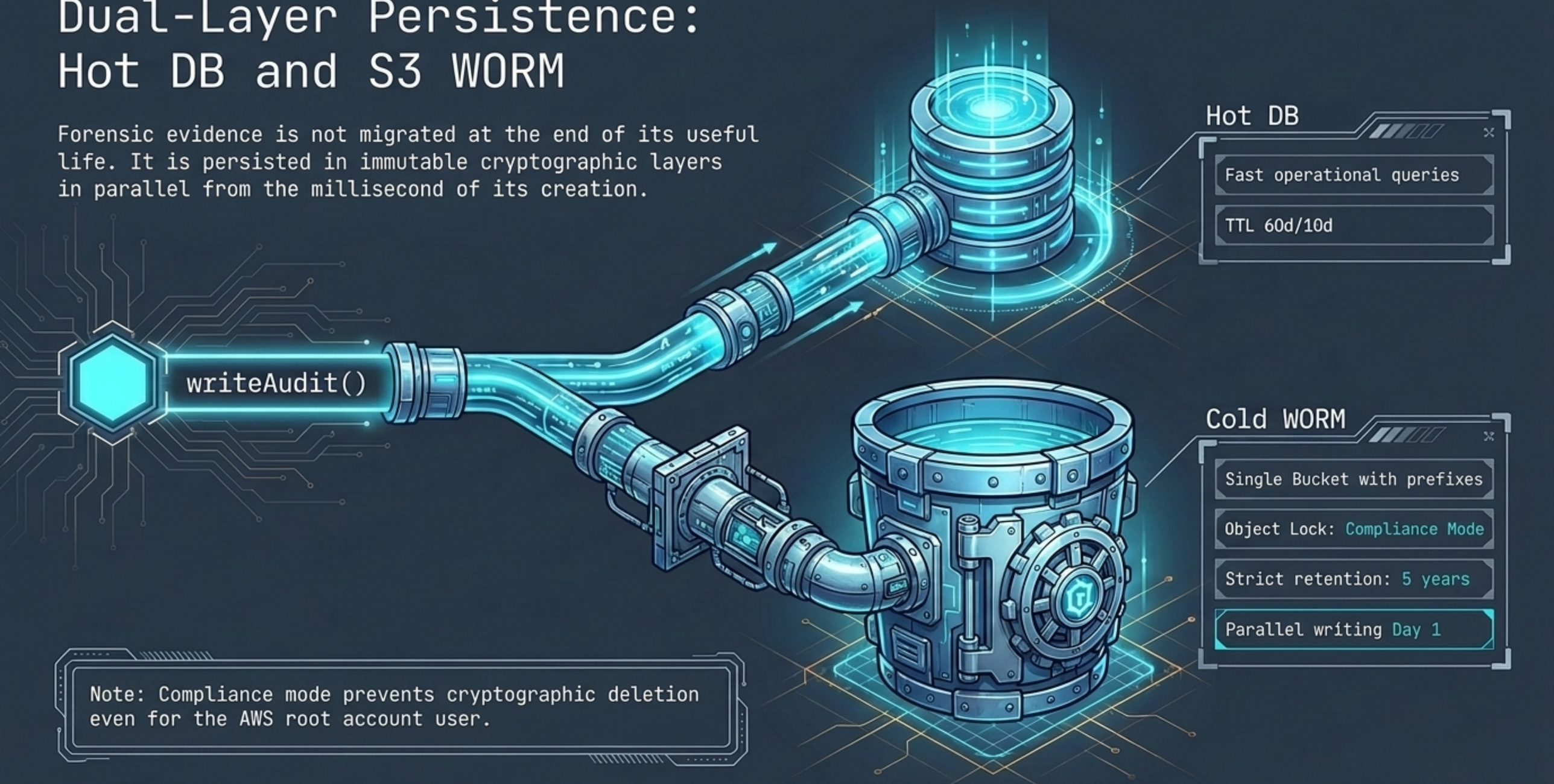
`Anchoring Endpoint: /v1/audit/chain/head`

`Anchoring Endpoint: /v1/audit/chain/head`

External projection to SIEM for time anchoring.

Dual-Layer Persistence: Hot DB and S3 WORM

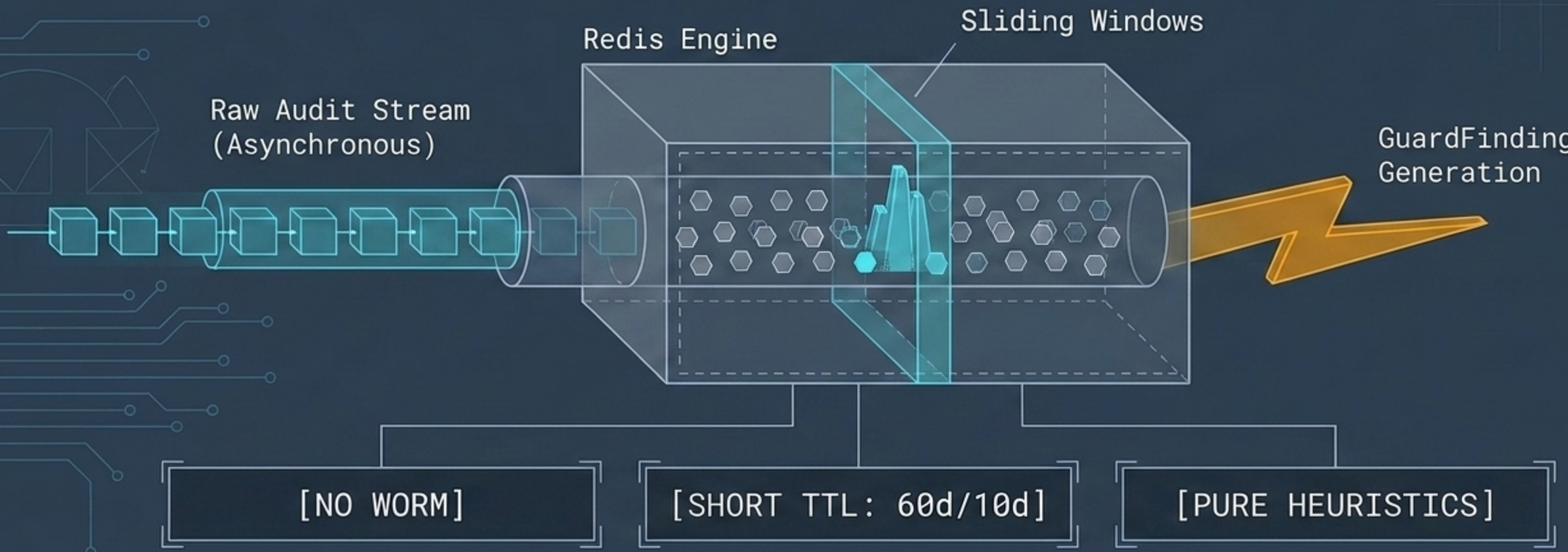
Forensic evidence is not migrated at the end of its useful life. It is persisted in immutable cryptographic layers in parallel from the millisecond of its creation.



Note: Compliance mode prevents cryptographic deletion even for the AWS root account user.

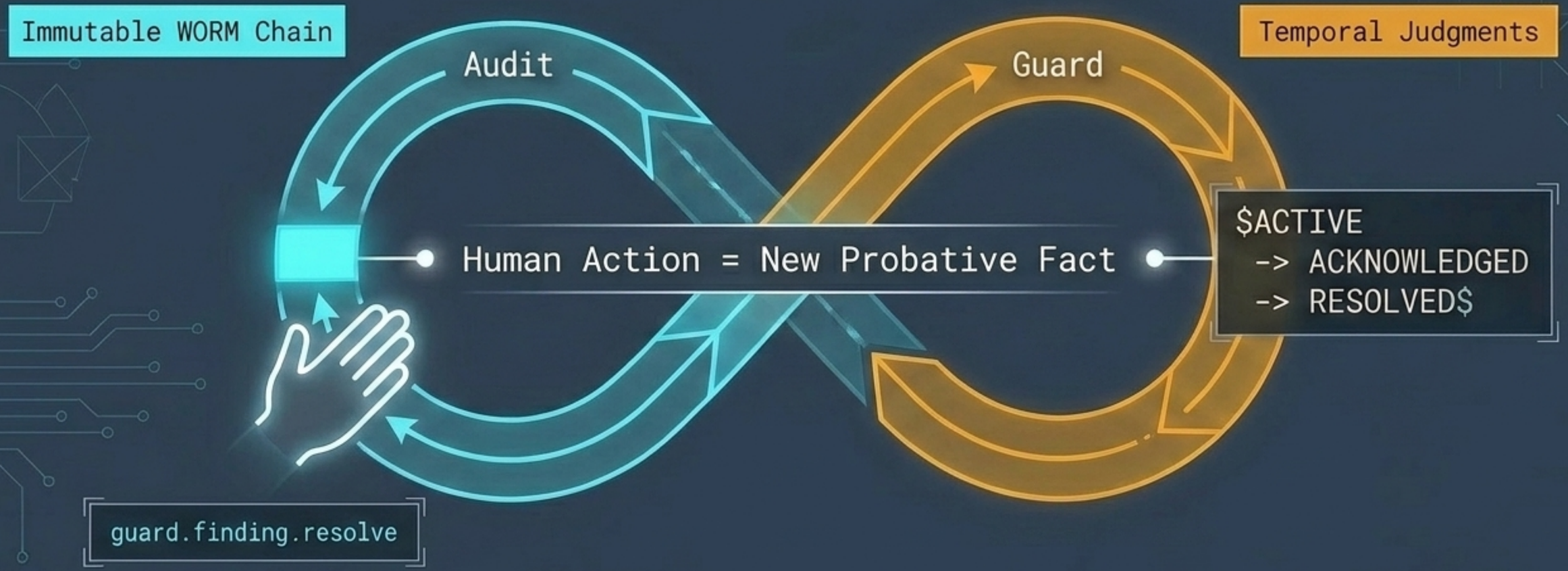
Guard: The Derived Layer and Contextual Detection

Guard asynchronously intercepts the Audit event stream to apply heuristics and temporal state memory without altering the evidentiary chain.



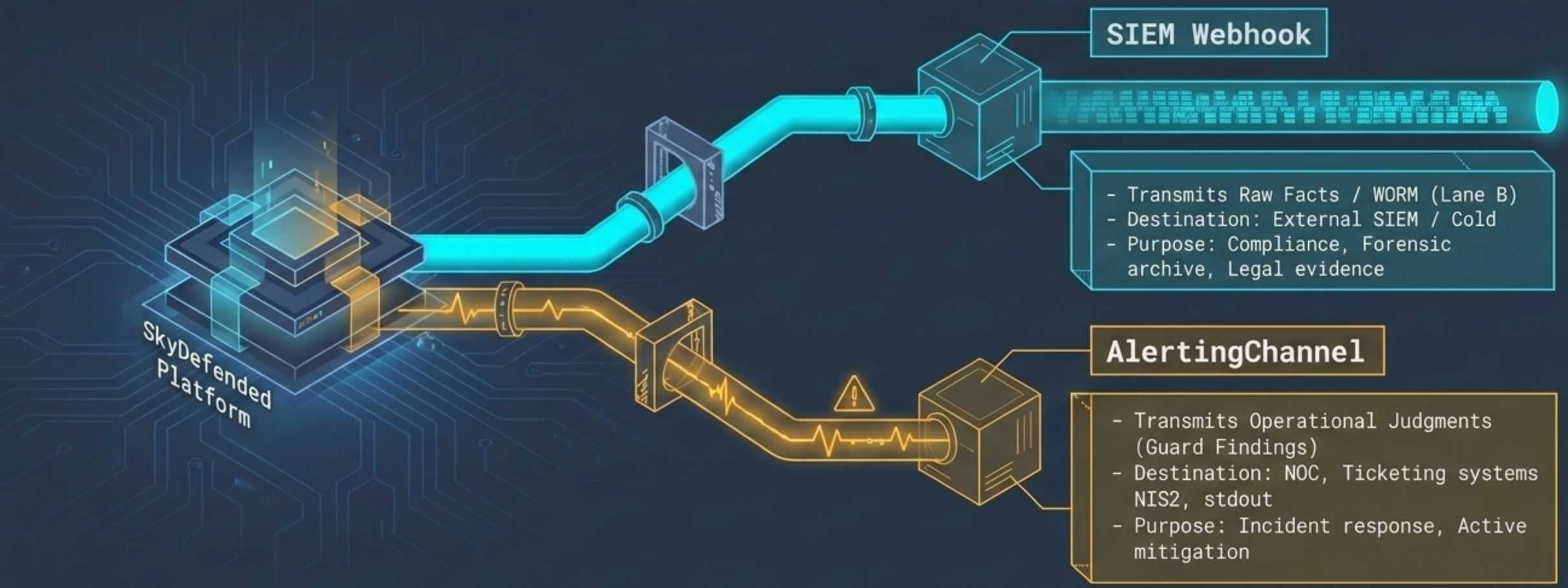
Audit-Guard Symbiosis: Lifecycle of the Finding

The asymmetry of the design is intentional: Guard generates ephemeral judgments, but human decisions on those judgments are injected back as immutable evidence.



Outbound Routing: SIEM Webhook vs AlertingChannel

The destination of data depends on its fundamental nature. Parallel output paths are maintained to avoid contaminating operating systems with massive raw data, or emptying SOCs without context.



Asymmetric Push Upward: Engine → Control

To preserve the Zero Trust sanctuary, the architecture allows centralized visibility through a strictly unidirectional flow. Control never polls; Engine always pushes.

Distributed Interrogation and Forensic Replay

Decentralized telemetry requires a query model adaptable to the incident severity and data temperature.

Hot Query

Standard UI, ultra-fast indexing. Coverage of recent incidents (10d-60d).

Advanced Realtime (PIM)

Live tailing of raw data. Requires physical unlock with PIM key. Extreme audit traceability.

Operator Console

S3 Forensic Query

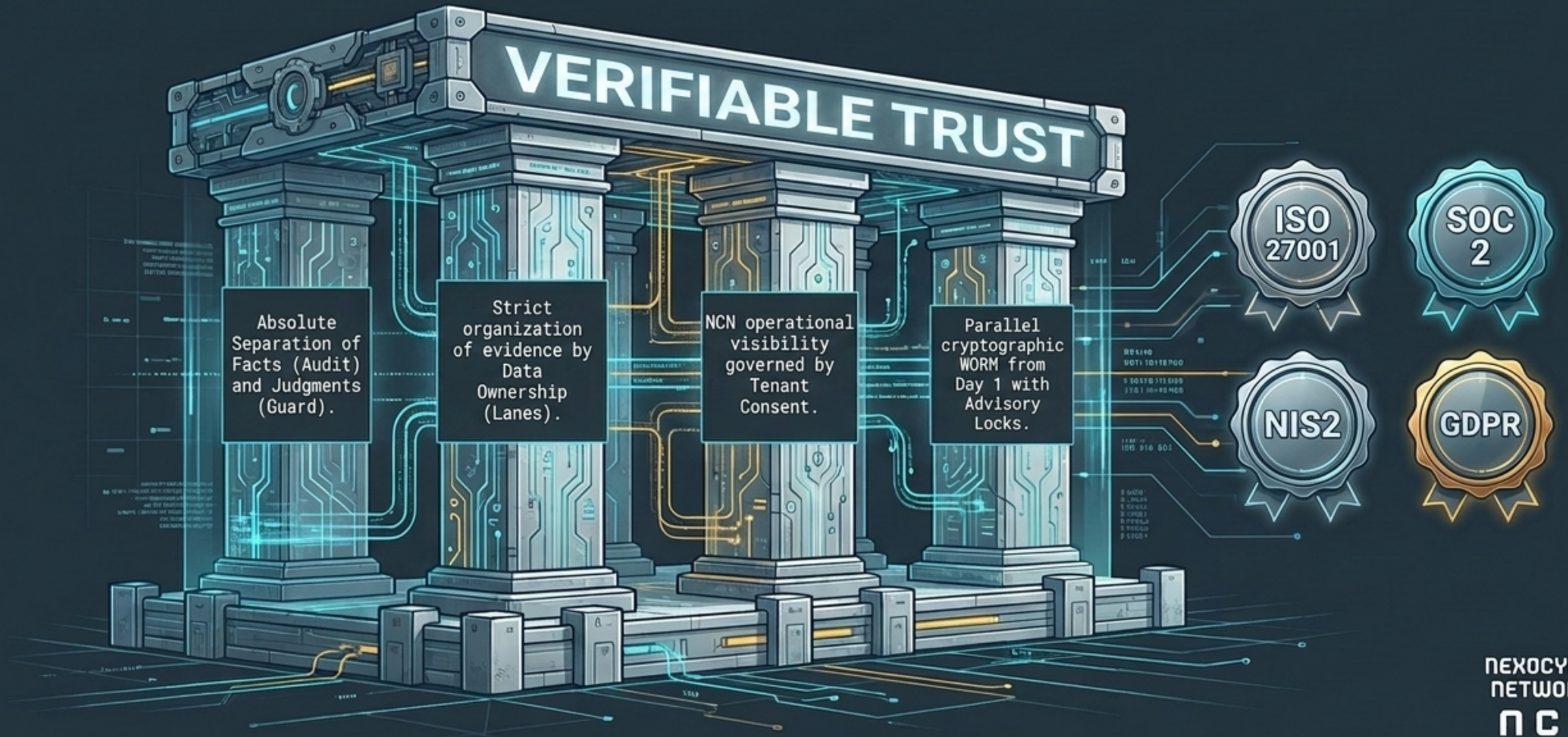
Cold query against 5-year compliance storage. Legal historical reconstruction.

Forensic Replay

Extraction of WORM cold events and retrospective reinjection into new Guard detectors to evaluate missed signatures.

Architectural Conclusion: Invariants for Verifiable Trust

SkyDefended InfraApp transforms traditional logging into a sovereign and unbreakable forensic chain. As long as the invariants are respected, the platform guarantees automatic compliance.



NEXOCYBER NETWORKS

NCN

NETWORKING, S...

NotebookLM