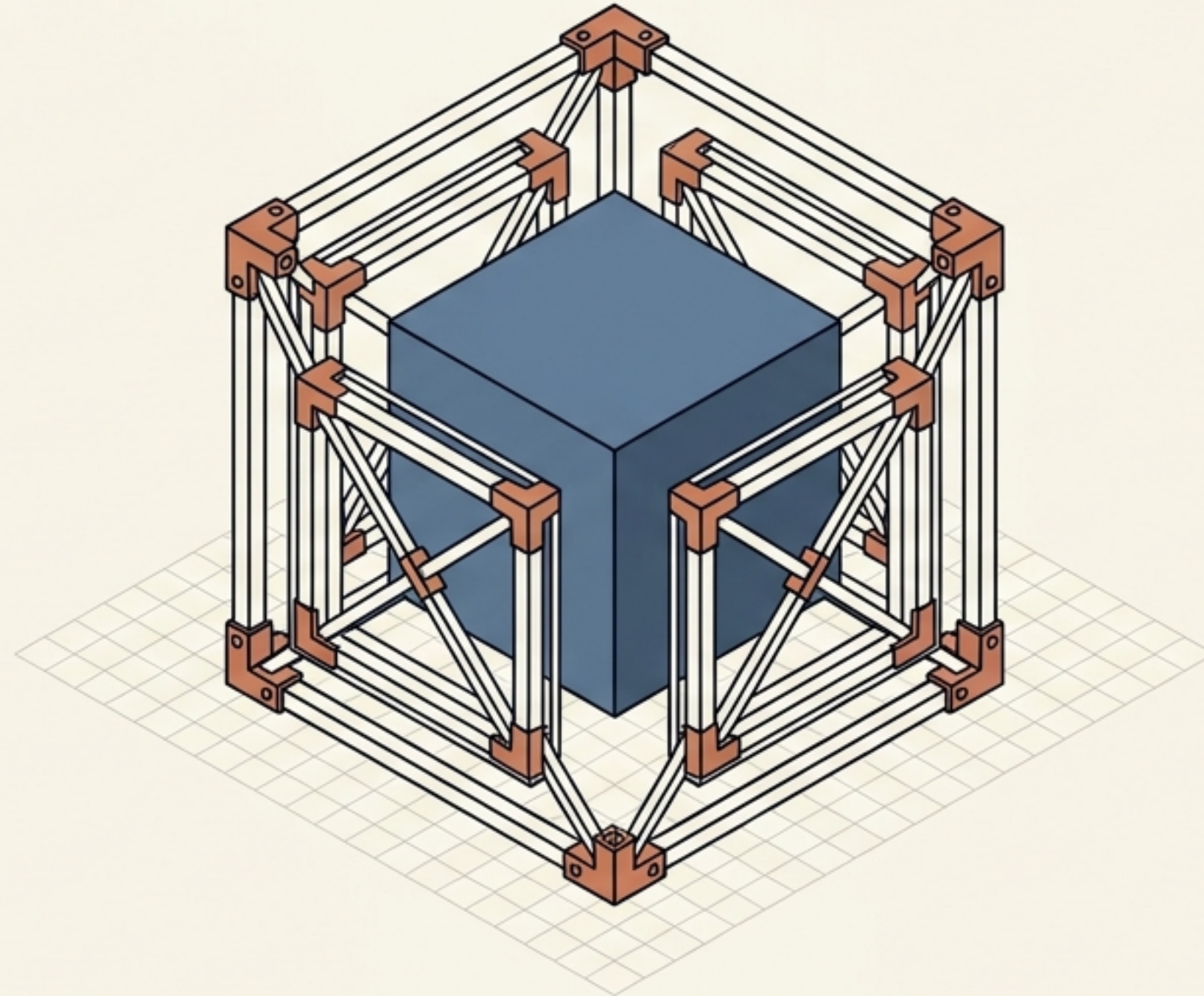


# bulletproof-agentic-data-plane

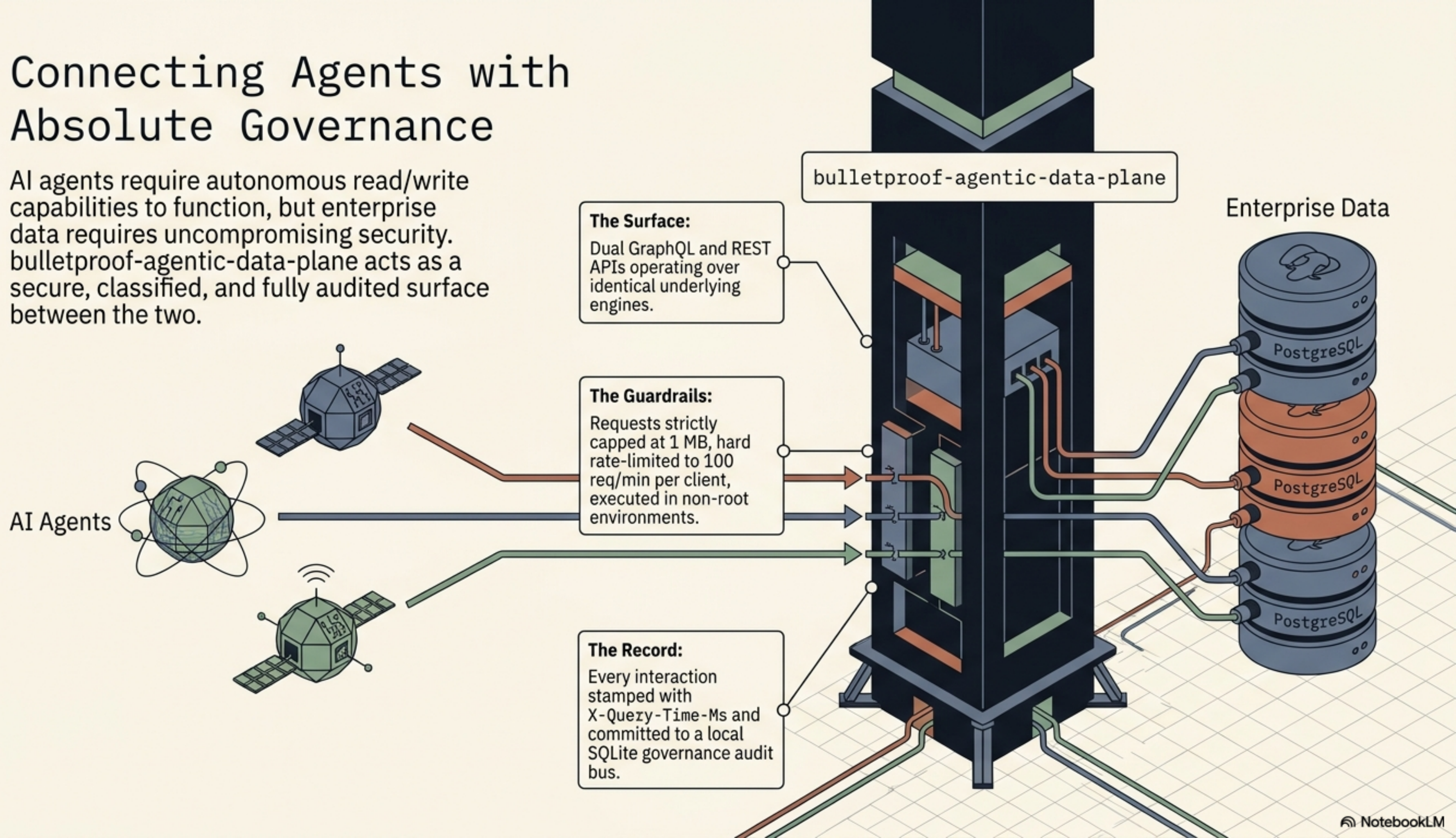
A Governed Data Plane for AI Agents.





# Connecting Agents with Absolute Governance

AI agents require autonomous read/write capabilities to function, but enterprise data requires uncompromising security. bulletproof-agentic-data-plane acts as a secure, classified, and fully audited surface between the two.





# Secure Access via Strict Identity

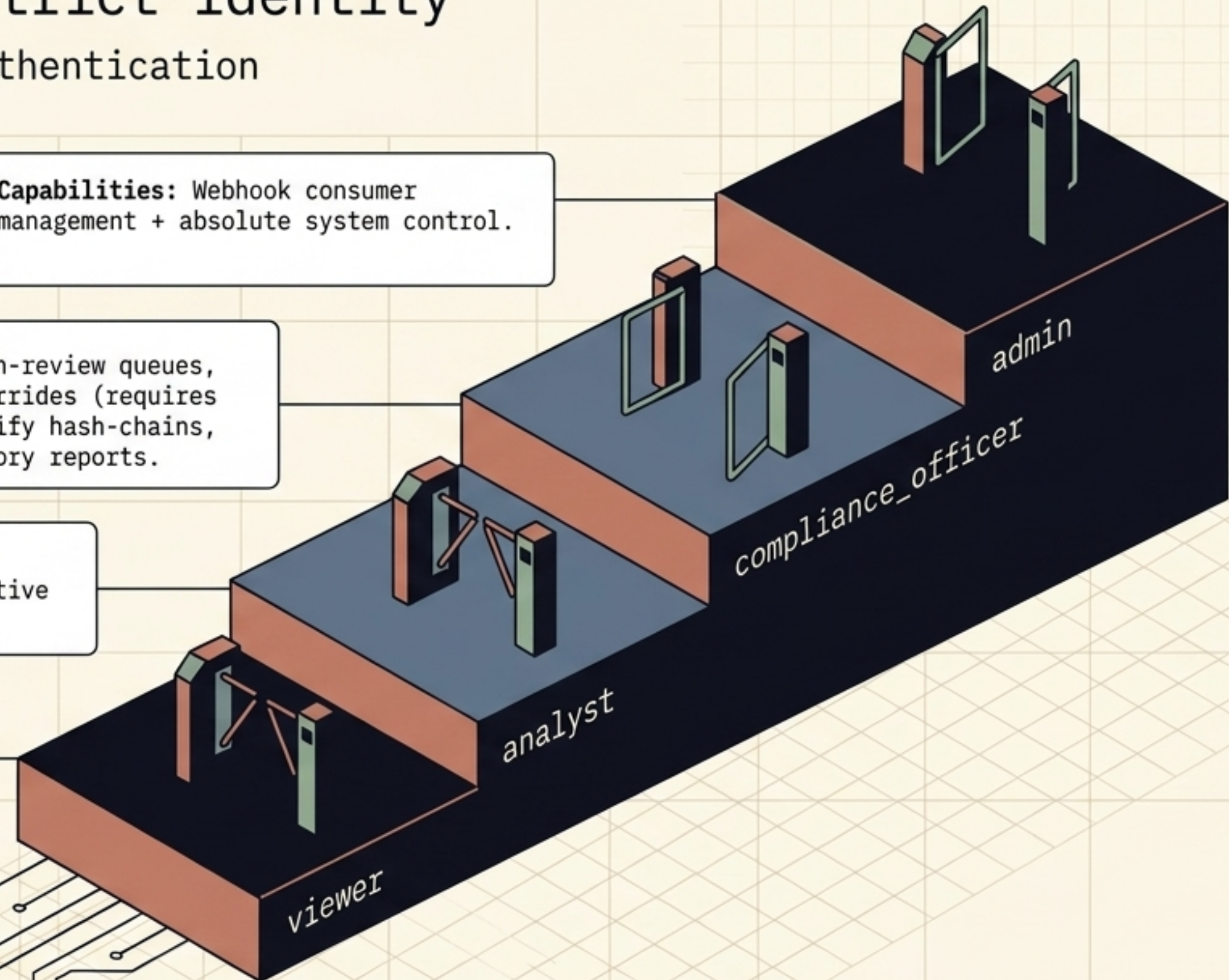
1-Hour Expiry | HS256 JWT Authentication

**Capabilities:** Webhook consumer management + absolute system control.

**Capabilities:** Process human-review queues, execute classification overrides (requires rationale  $\geq 10$  chars), verify hash-chains, generate DOI/HIPAA regulatory reports.

**Capabilities:** Query audit events, validate dataset quality, list active classifiers.

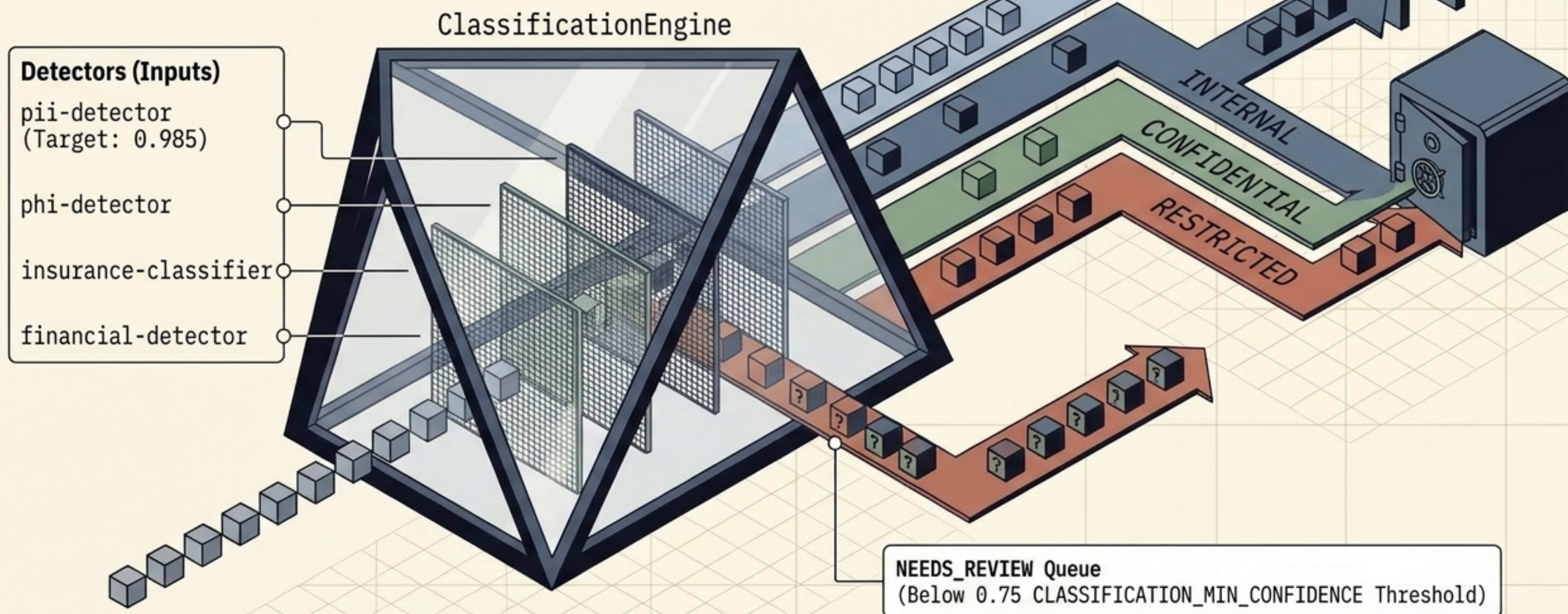
**Capabilities:** Read lineage graphs, query quality scores, and monitor pipeline health.





# Automated Sensitivity Routing

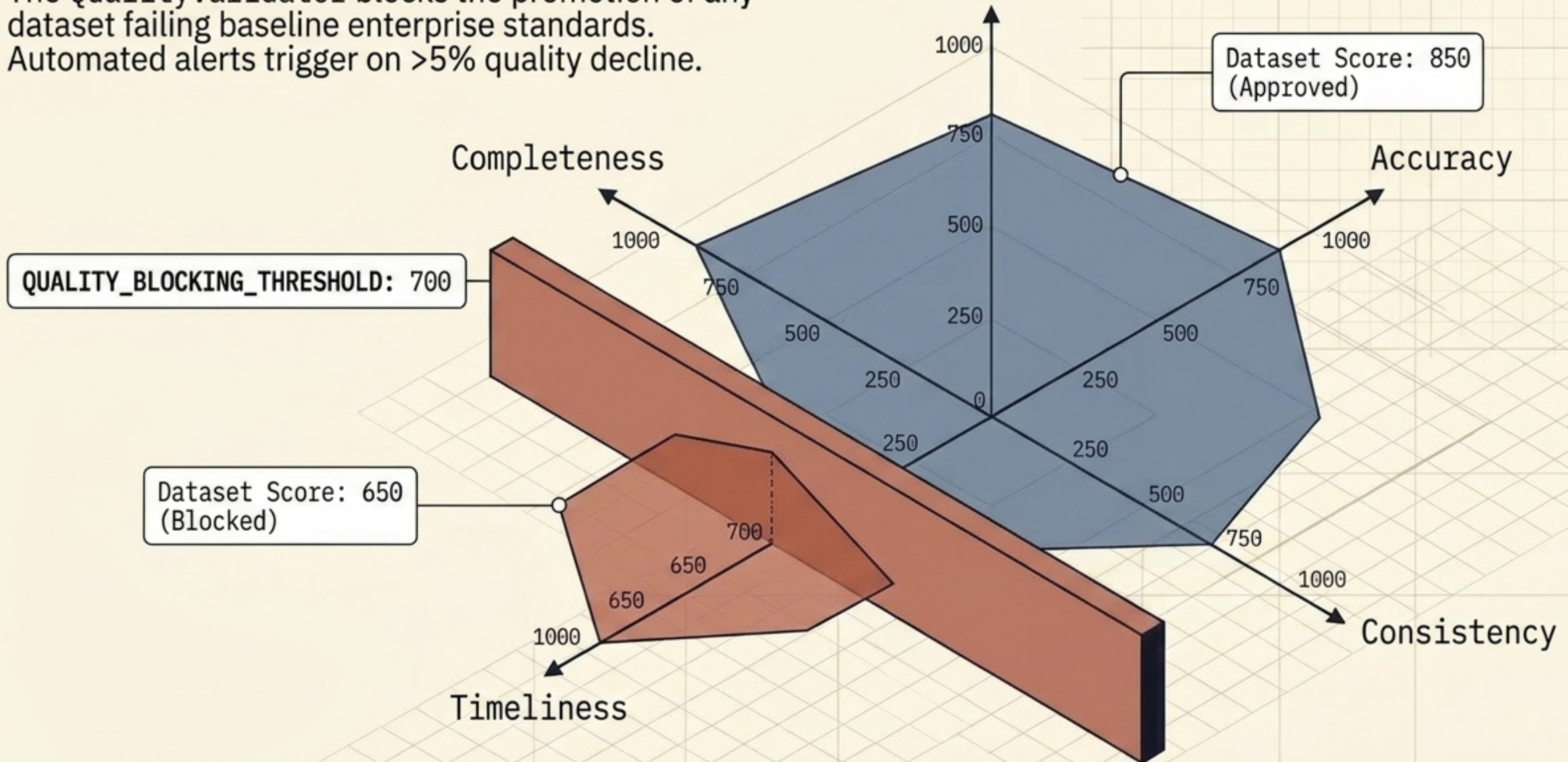
Hot-swappable classifier versions automatically evaluate payloads. Detections below the 0.75 CLASSIFICATION\_MIN\_CONFIDENCE threshold divert to a NEEDS\_REVIEW queue for human evaluation.





# 0-1000 Quality Scoring & Promotion Gates

The QualityValidator blocks the promotion of any dataset failing baseline enterprise standards. Automated alerts trigger on >5% quality decline.

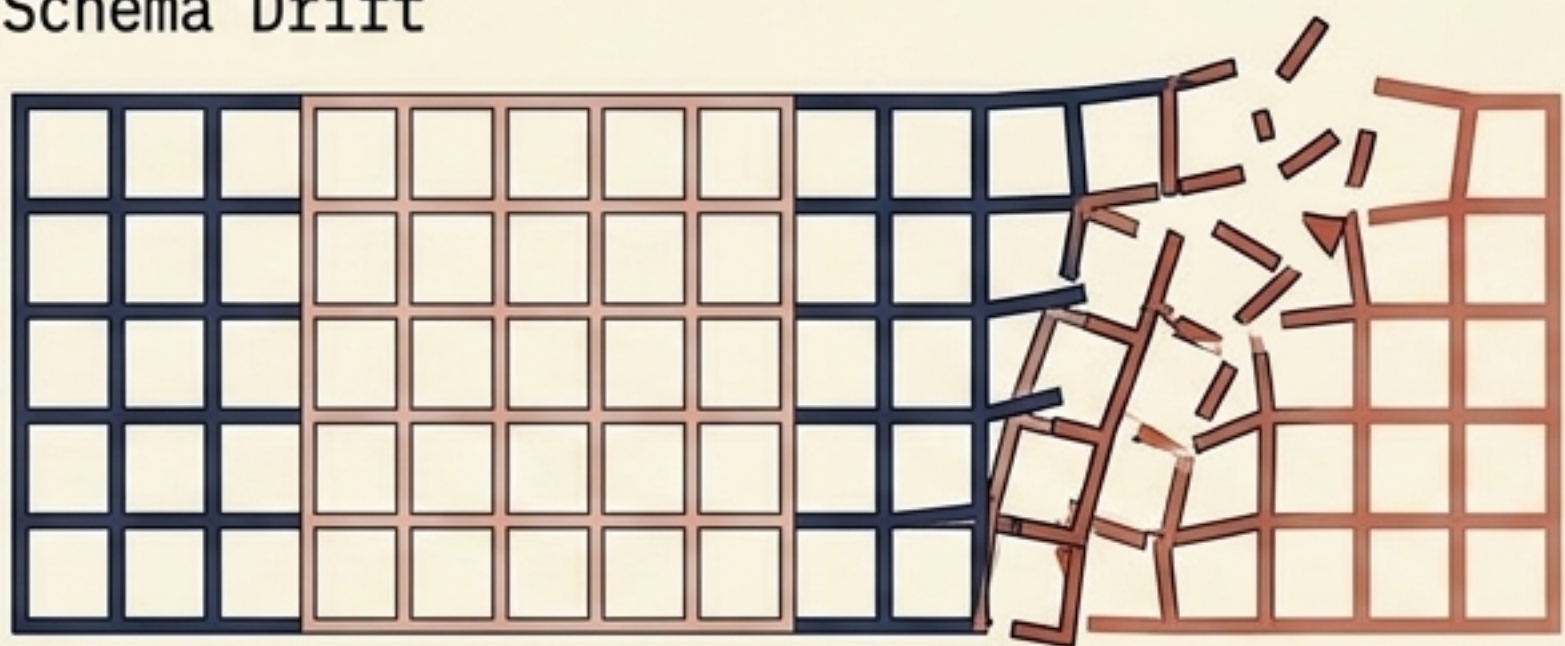




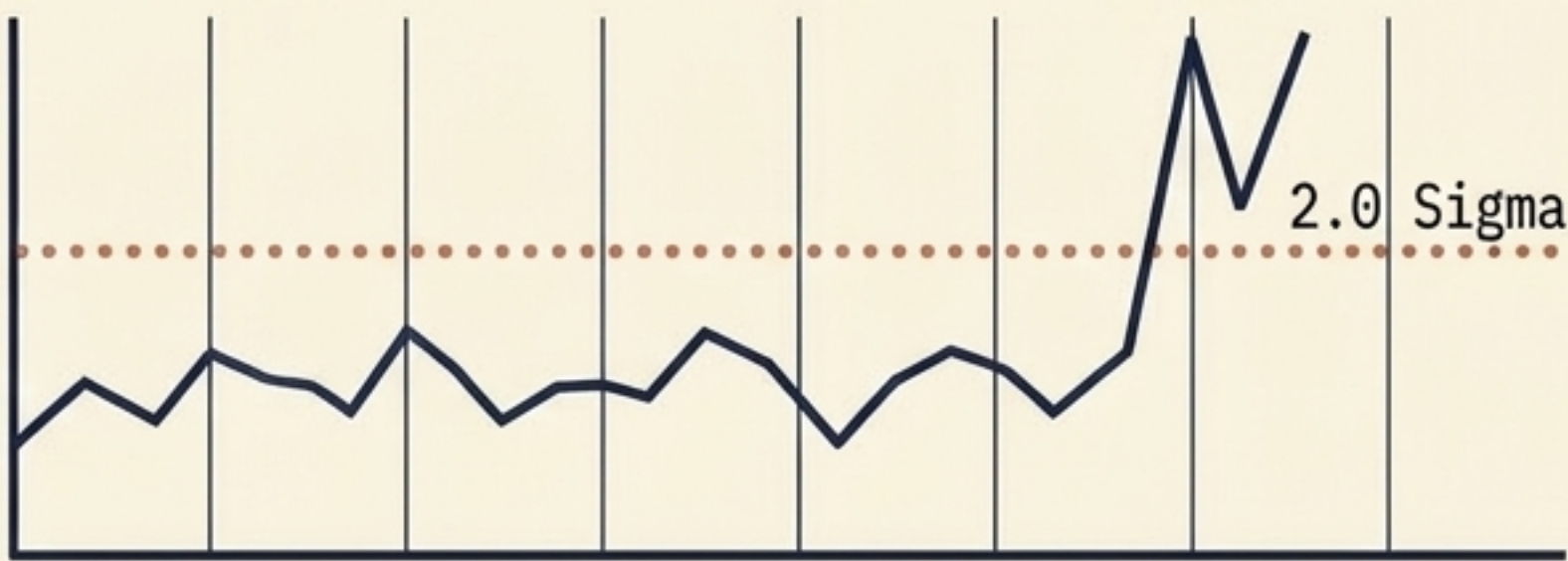
# Real-Time Observability & Alerts

The PipelineObserver continuously evaluates data streams against historical baselines, dispatching webhook notifications within a 30,000 ms SLA.

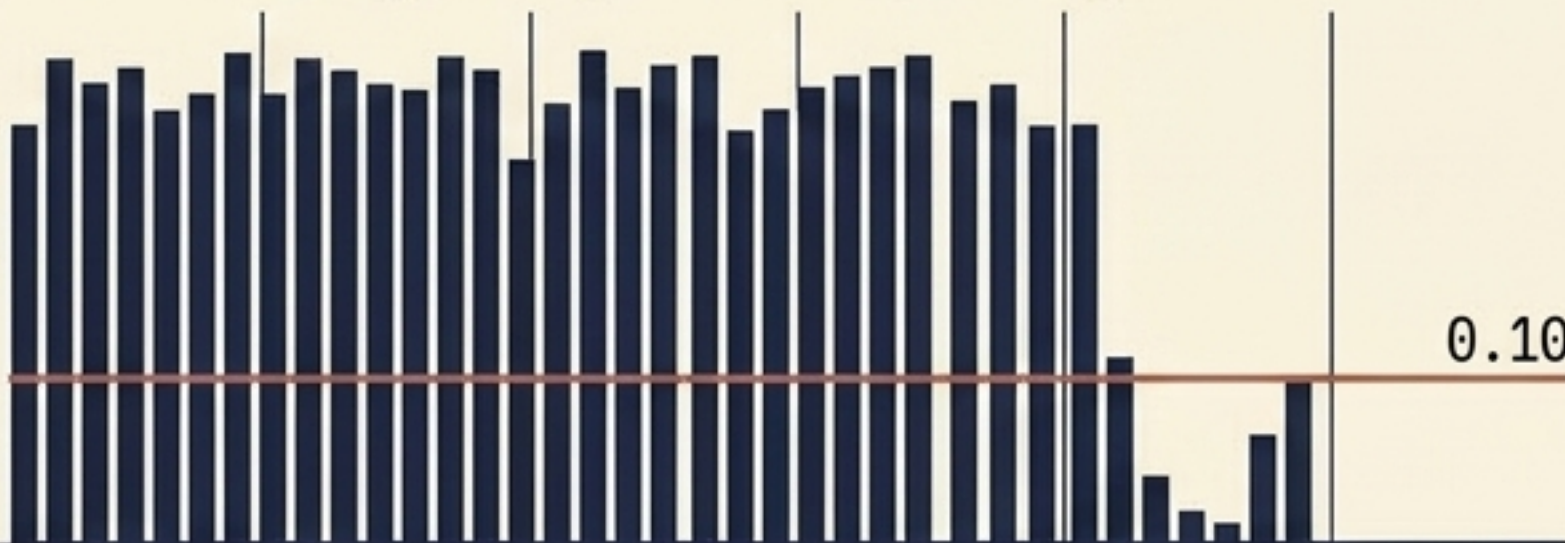
Schema Drift



Volume Anomaly (2.0 Sigma Threshold)



Null-Rate Spike (0.10 Threshold)



SLA Breach (>30,000 ms)



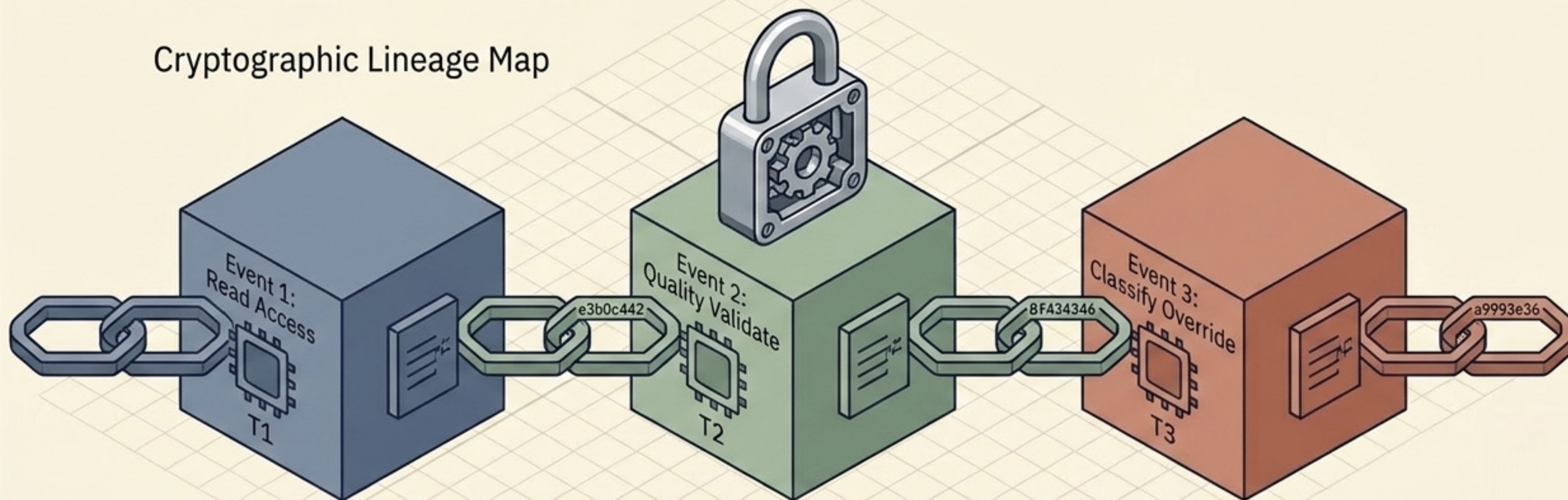


# Tamper-Evident Provenance

Every governance and access event is HMAC-SHA256 signed and strictly retained (7 years standard, 10 years restricted).

LineageEngine & EventPublisher

Cryptographic Lineage Map



Unbreakable backward traces and forward impact analysis.



# The Complete Governance Surface

bulletproof-agentic-data-plane does not just connect AI agents to your enterprise data—it fundamentally transforms how that data is protected, evaluated, and permanently audited.

