

Engineering the RFID Medication Kiosk Dashboard

A technical dissection of Singapore's real-time, event-driven medical collection telemetry and command center.

System Architecture & Design Specification | 2025–2026 Rollout

```
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01"  
}  
  
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01"  
}  
  
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01"  
}  
  
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01"  
}  
  
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01"  
}  
  
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01"  
}  
  
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01"  
}
```

System Scale

20 Hub Locations

9 Polyclinics | 6 Hospitals | 5 Community Hubs

18 Months Data Retention

Performance Baseline

Sub-second real-time alerts

<200ms API Response (TTFB)

Core Personas

Operations Controllers



Focus: Real-time monitoring, incident response, and predictive inventory management.

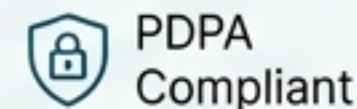
Regulatory Analysts



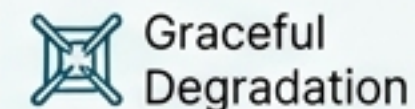
Focus: MOH compliance reporting, historical trend analysis, and audit trailing.

Core Design Tenets

Privacy-First



Resilient



Actionable

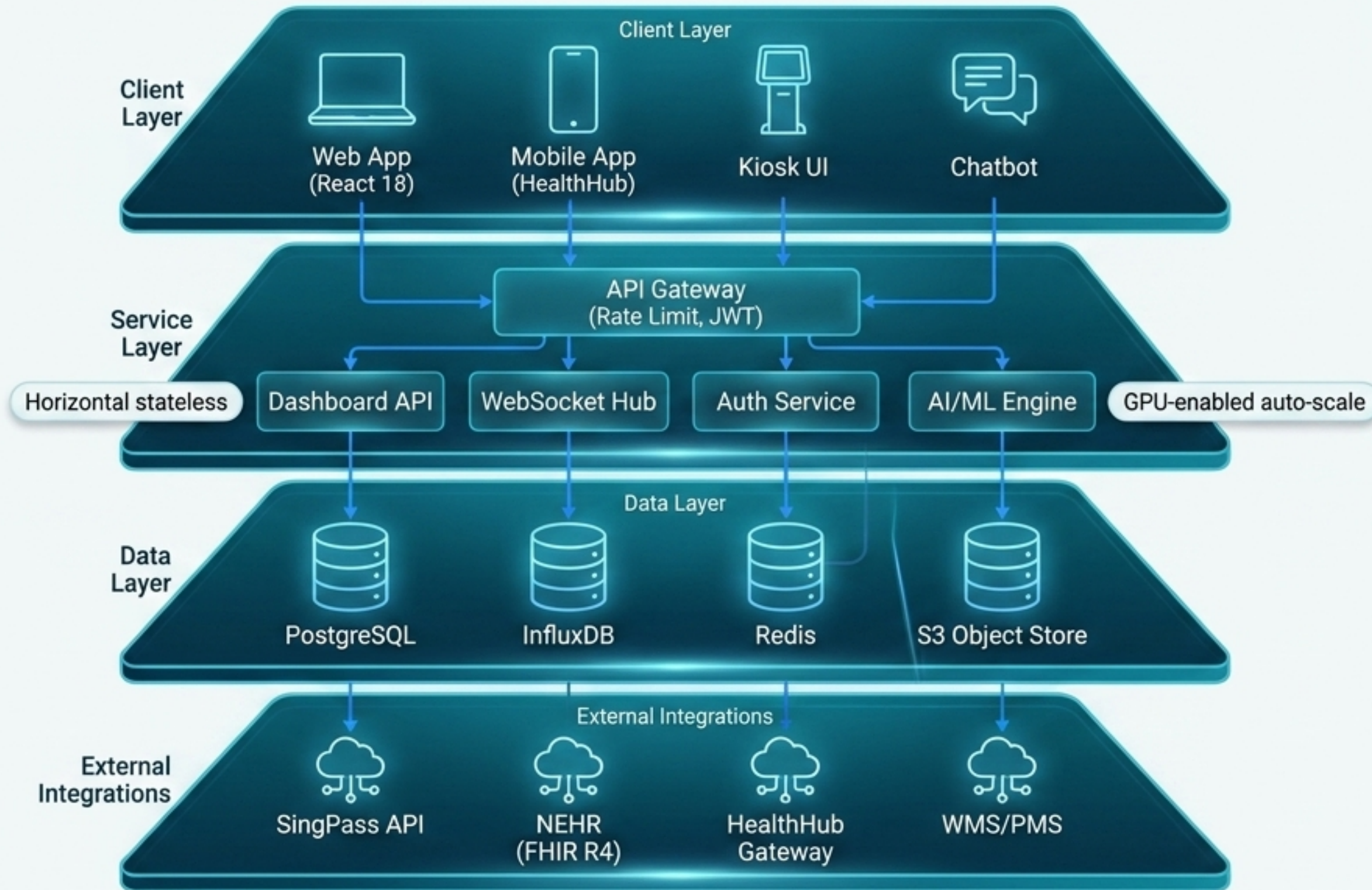


Role-Based Access Control (RBAC) Architecture

Privilege	Viewer	Operator	Supervisor	Admin	Auditor
Hub Access	Assigned Only	Assigned Zone	All Hubs	All Hubs	All Hubs
Patient Data	Aggregate Only	Masked IDs (SXXXX123D)	Masked IDs (SXXXX123D)	Full (with justification)	Masked default (Unmask via 4-Eyes)
System Config	None	None	Read-only	Full Control	Read-only

The Four-Eyes Principle
Structurally guaranteeing patient privacy. Unmasking sensitive data requires two independent authorizations and instantly generates an immutable audit log.

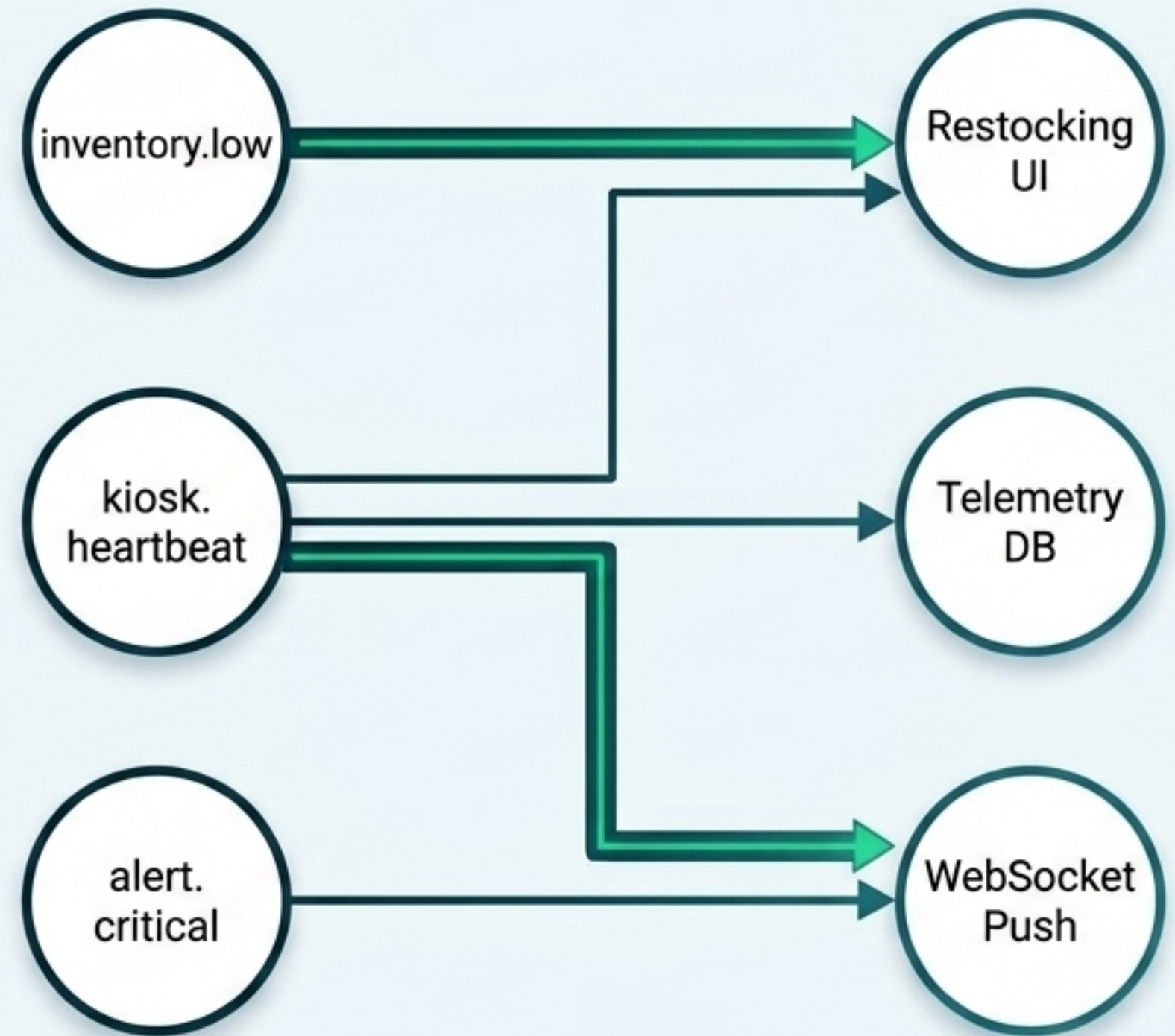
System Architecture: 4-Tier Schematic



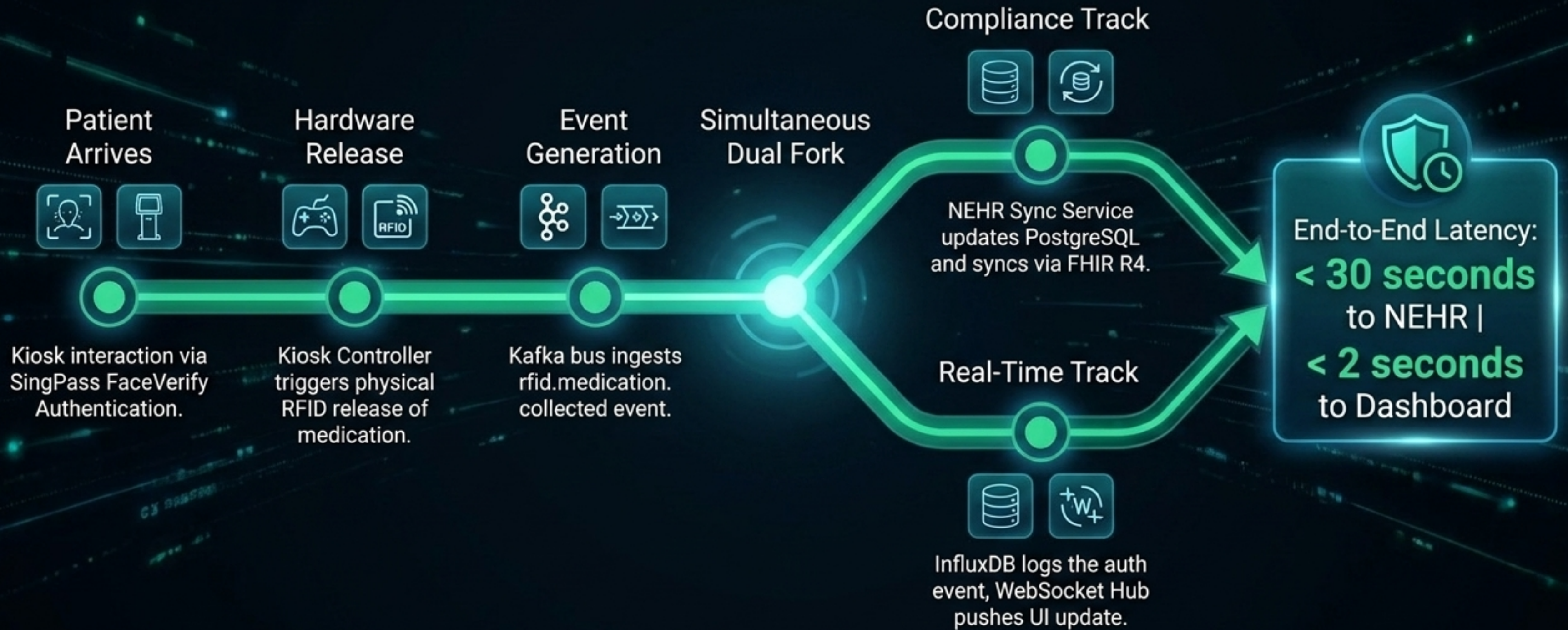
The Event Payload

```
{  
  "specversion": "1.0",  
  "type": "rfid.medication.collected",  
  "source": "kiosk-controller/AMK-01",  
  "id": "uuid-v4",  
  "data": {  
    "authMethod": "SINGPASS_FACEVERIFY",  
    "authSuccess": true  
  }  
}
```

Kafka Event Bus Routing



Event-Driven Collection Flow: Sub-Second Telemetry



Data Persistence Strategy



PostgreSQL 15

Role: Relational Core

Data Type: Prescriptions,
Inventory, Hubs

Retention: 7 Years
(Compliance)

Optimization:
Partitioned by quarter,
B-tree/GIN indexing



InfluxDB 2.x

Role: Time-Series

Data Type: IoT Telemetry,
Auth Events

Retention: 2 years hot,
5 years cold

Optimization:
Downsampled hourly,
continuous queries



Redis 7

Role: Cache & PubSub

Data Type: Active Sessions,
Dashboard Aggregations

Retention: 1 hour / 24 hour

Optimization: Cluster mode,
automated TTL expiry



Kafka + S3

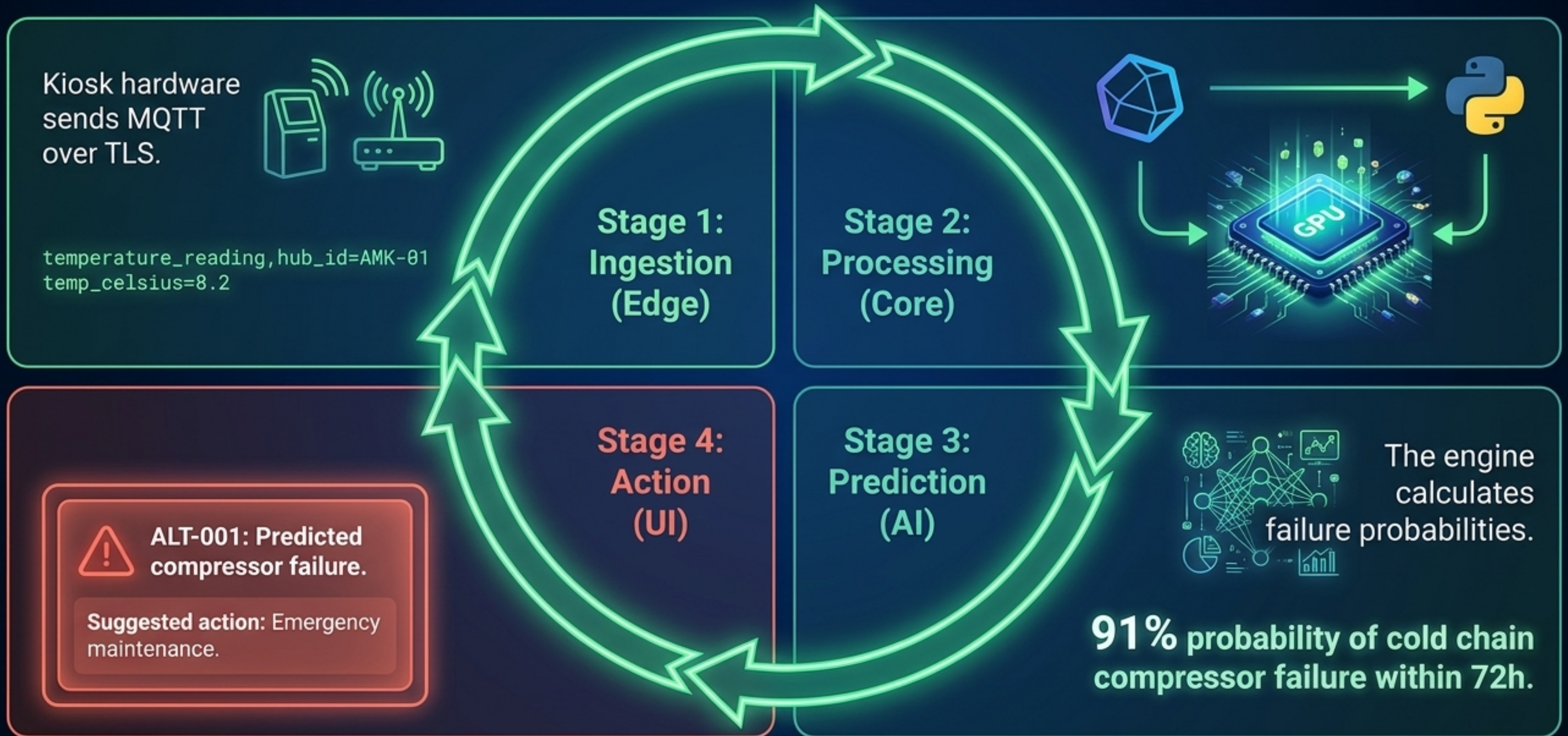
Role: Immutable Audit

Data Type: Event logs and
system trails

Retention: 10 years

Optimization:
Write-Once-Read-Many
(WORM) storage

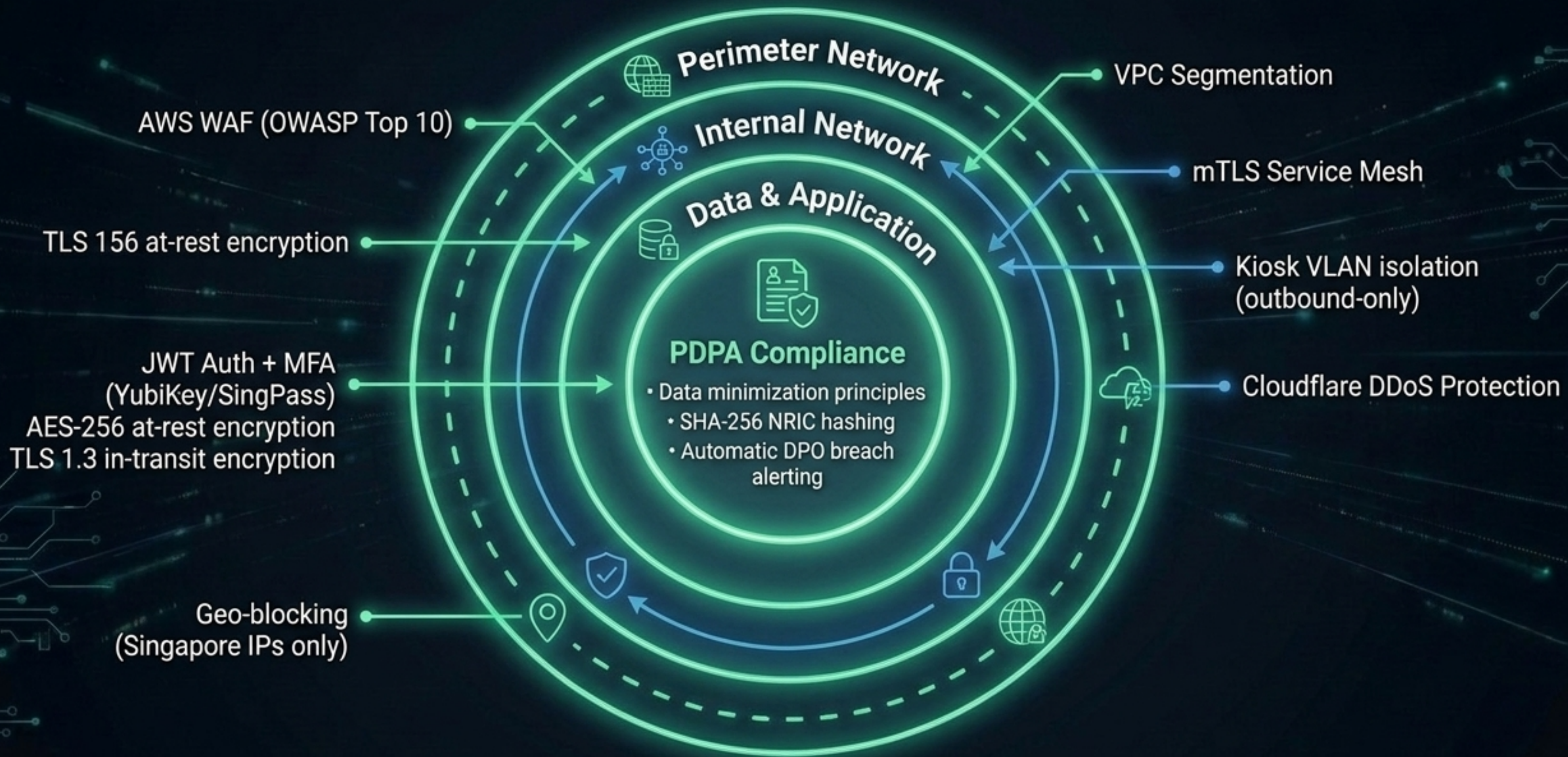
Telemetry & AI Loop: Moving from Data to Action



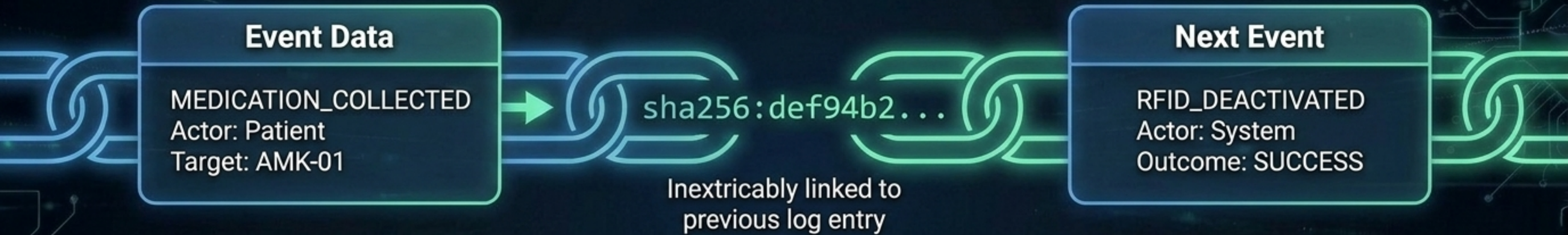
Predictive Restocking Flow: Preventing Stockouts



Defense-in-Depth: Multi-Layer Security Architecture



Regulatory Compliance: **Immutable Audit Trail**

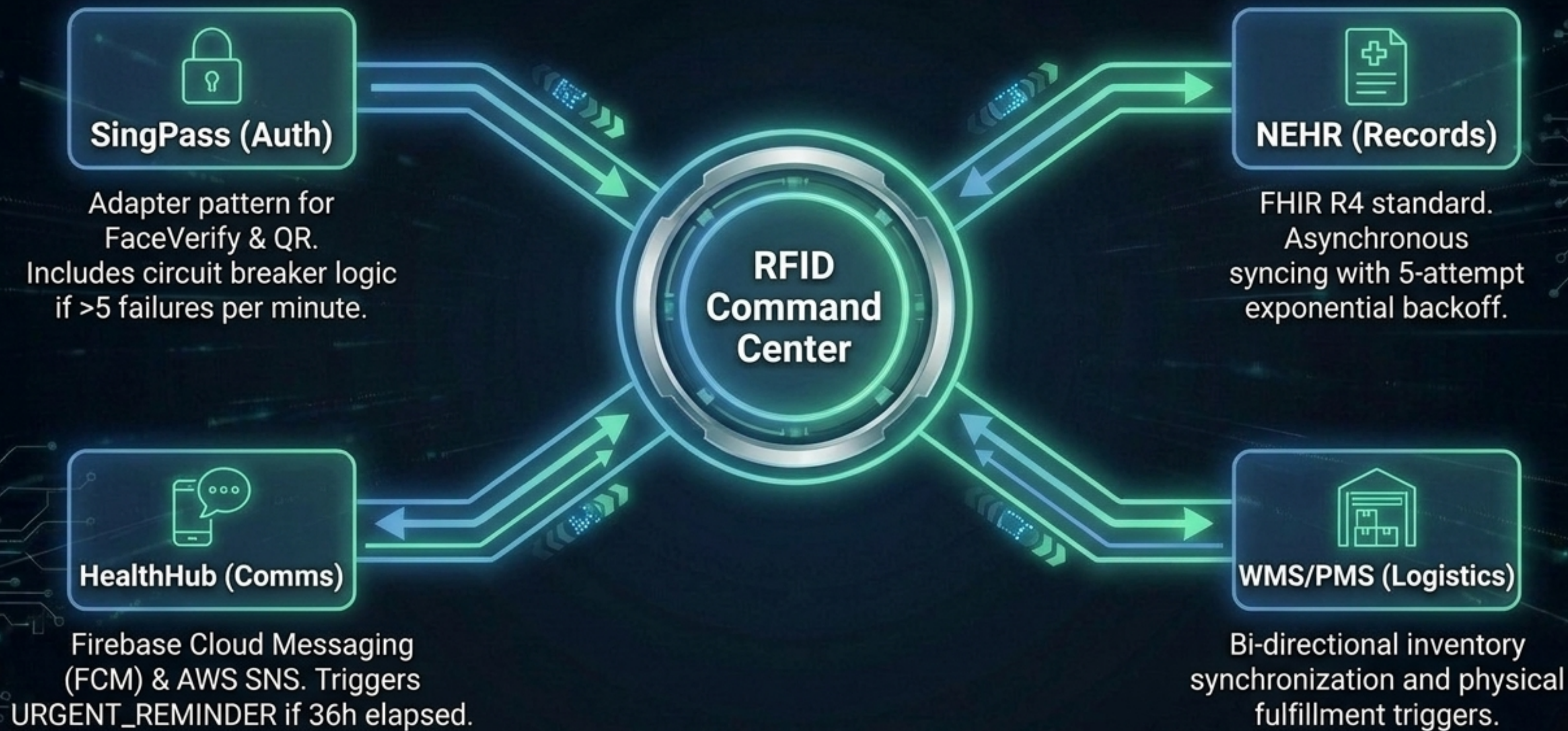


Blockchain-like Tamper Detection

Daily automated scripts verify the cryptographic hash chain integrity to detect any unauthorized database modifications.

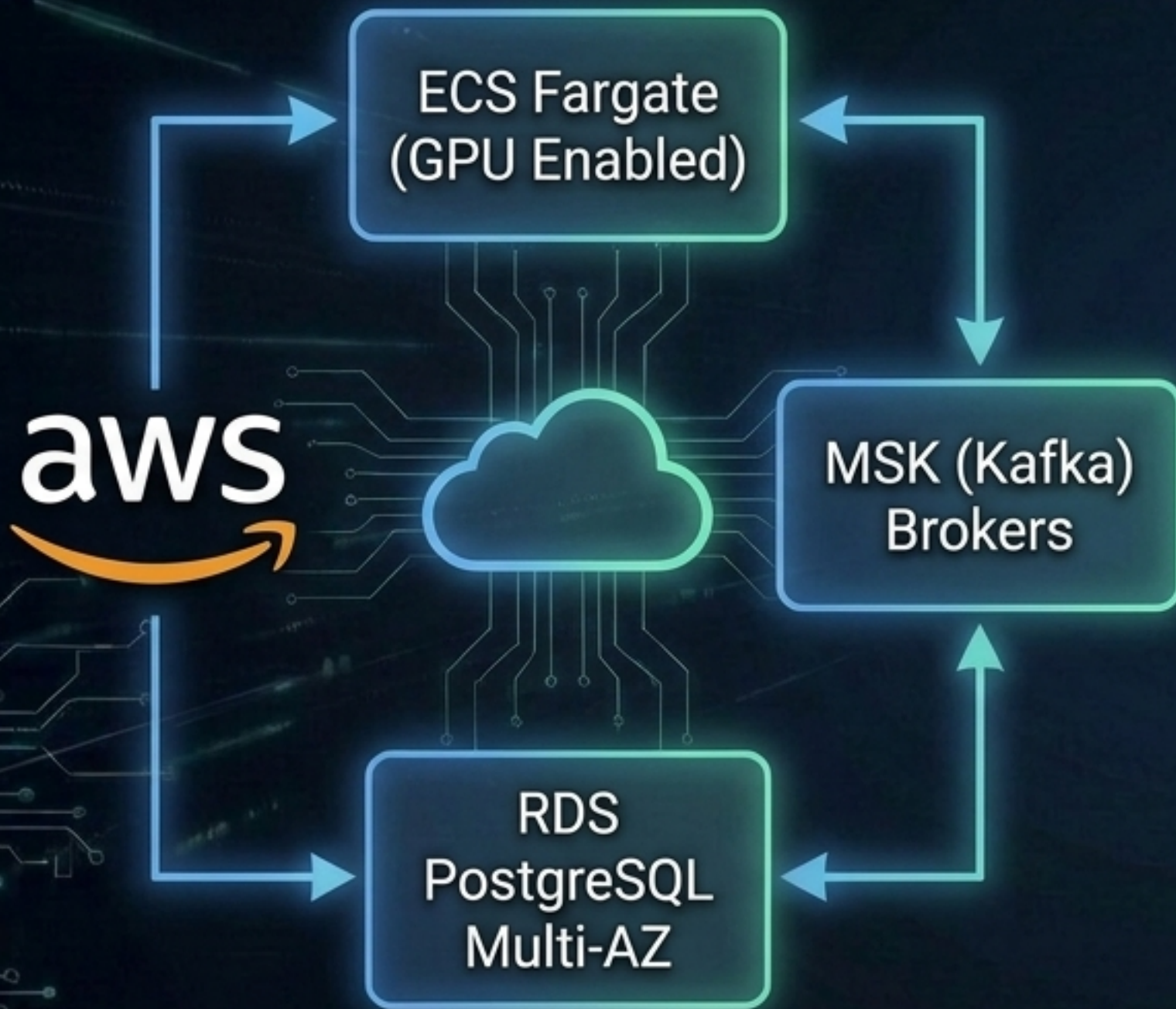
All logs are piped to AWS S3 Glacier using Write-Once-Read-Many (WORM) storage for 10-year retention.

External Ecosystem Integrations



Cloud Scalability & Infrastructure Deployment

Infrastructure Schematic



Scale Comparison & Triggers

Current Scale (20 Hubs)	Future Scale (100 Hubs)
330 Rx/day	2,000 Rx/day

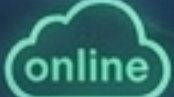
Auto-Scaling Triggers

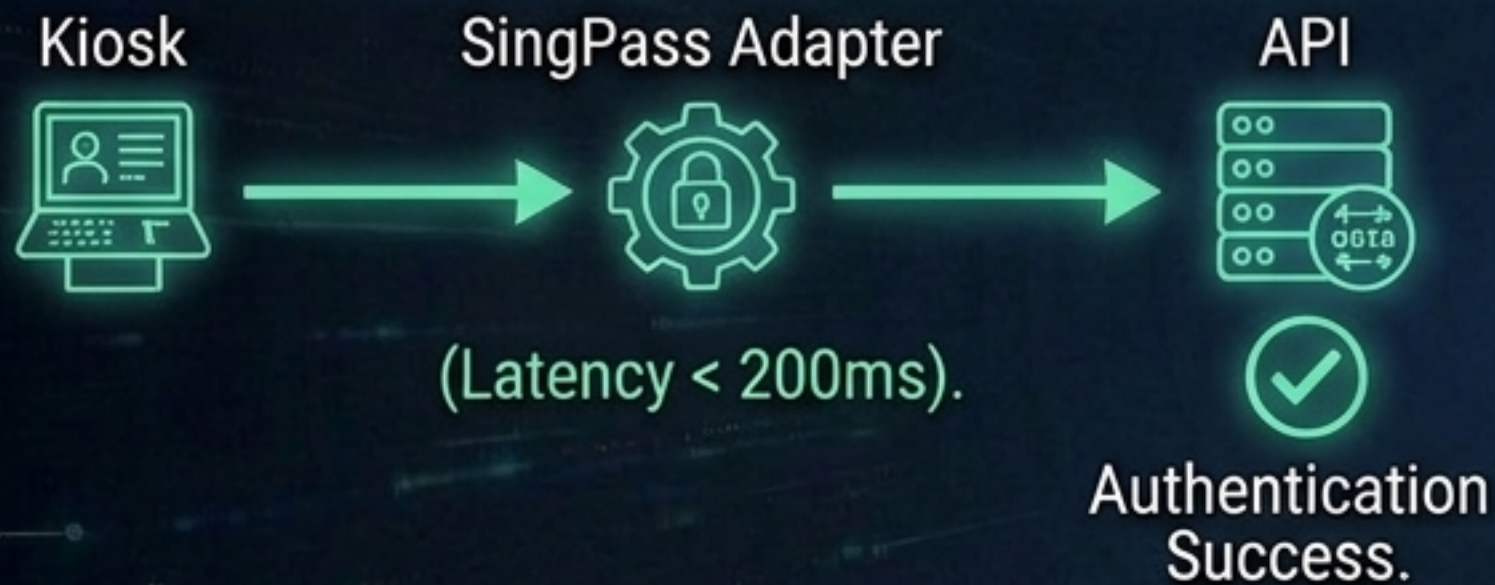
Elastic scaling thresholds without architecture rewrites:

- CPU >70% (5m) = +1 Compute Node
- API latency p95 >1s = +2 Compute Nodes
- Queue depth >1000 = +1 Kafka Consumer

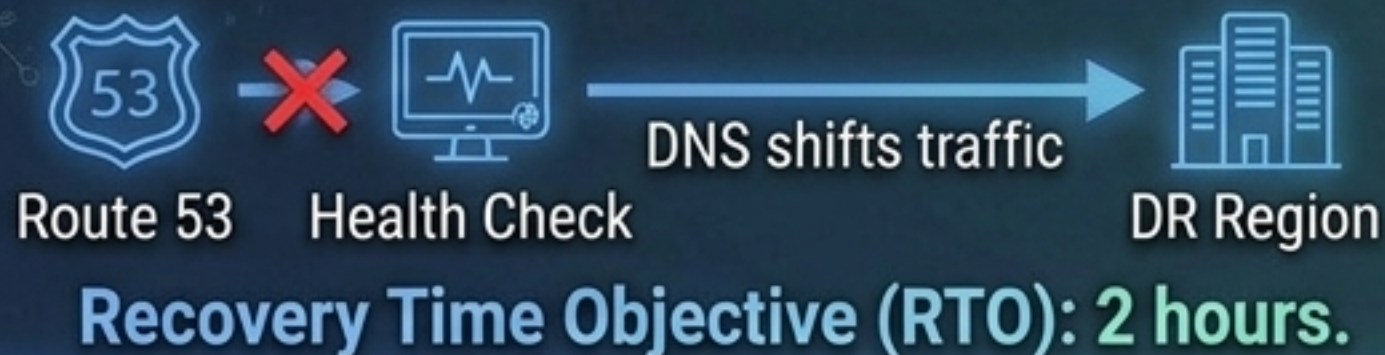
The Resilience Blueprint: Handling Component Failures

Healthy State (Optimal)

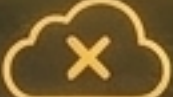
 **Scenario: SingPass API Online** 



Scenario: Regional Data Center Outage

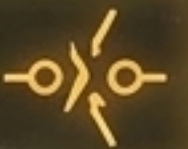


Degraded State (Fault Tolerant)

 **Scenario: SingPass API Outage** 



API fails > 5 times.
Circuit Breaker **OPENS**.



System instantly falls
back to OTP Mode.



Patient receives SMS code.
Collection continues uninterrupted.



Risk Mitigation through Graceful Degradation



Network & Hardware Disruptions

Risk: Kiosk local internet drops.

Mitigation: Automated 4G backup SIM activation. Kiosks run in isolation.



Software & API Dependencies

Risk: External integrations (NEHR/WMS) go offline.

Mitigation: Async queueing. Events are buffered in Kafka and replayed upon restoration. Dead-letter queues flag manual reconciliation.



Ultimate Physical Fallback

Risk: Total multi-region system failure.

Mitigation: Operators toggle Counter Collection Mode. Collection Mode. Lockers are bypassed, and patients redirect to the human pharmacy counter. Nobody leaves without medication.

Designed for absolute high availability: Single points of failure never compromise patient care or regulatory compliance.