

Bulletproof Agent Economics

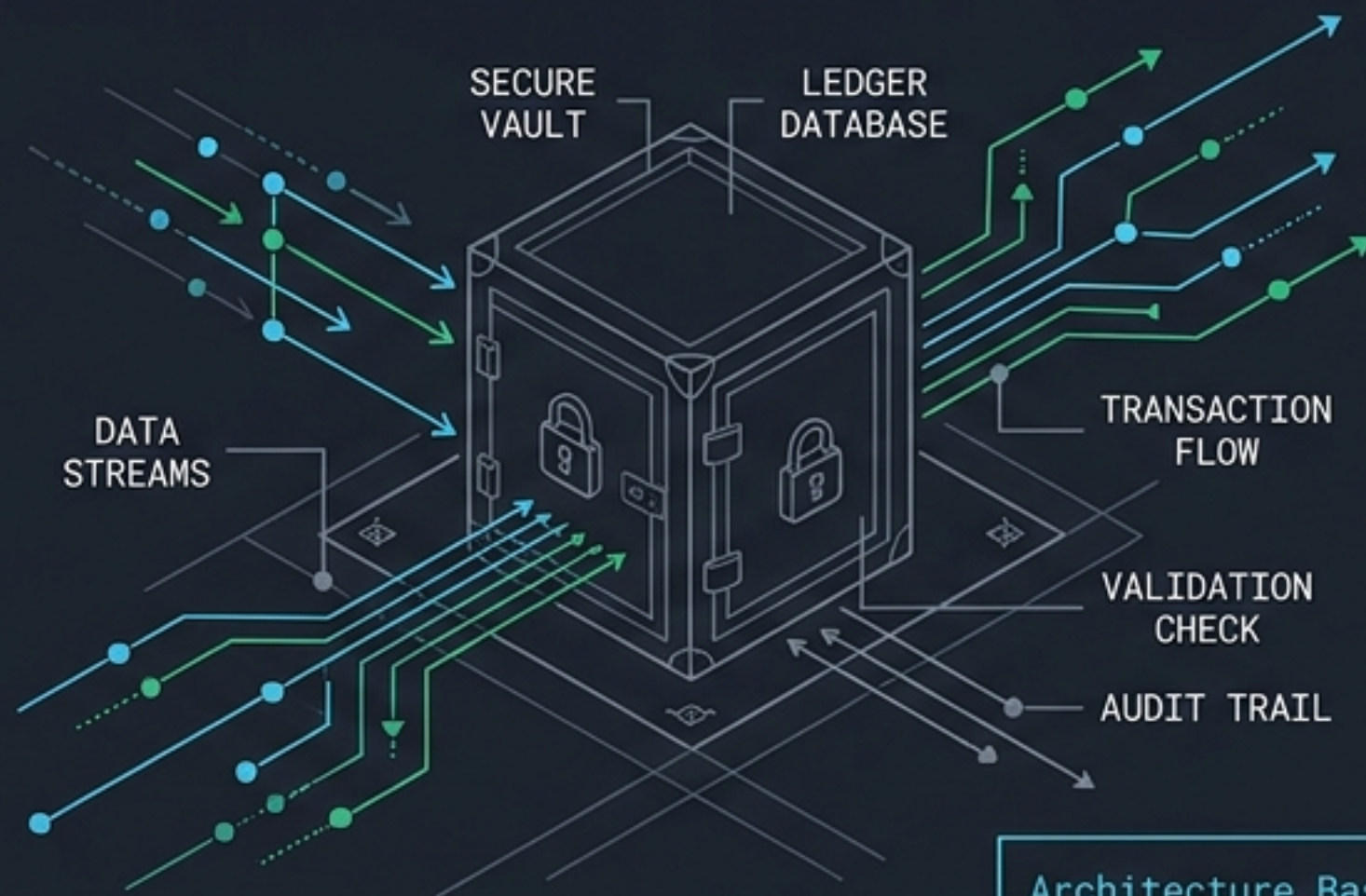
Financial Governance & Telemetry for Multi-Agent AI Systems

Cost Metering

Budget Enforcement

Heuristic Routing

Chargeback



Architecture Base: Node.js / TypeScript API (Port 8897)
Authoritative Ledger: PostgreSQL
Live Overlay: Redis

The Four Pillars of Agent Economics

A unified subsystem to track, optimize, and enforce financial governance across AI agents.

Pillar 1: Precision Metering

Records every action (llm_call, "tool_use", "cache_hit") in integer cents.

Instant rollups across hierarchical scopes: Agent → Session → Project → Department → Organization.

Pillar 2: Heuristic Routing

Advisory and deterministic routing across 13 models based on complexity.

Features automatic downgrades and audited manual admin overrides.

Pillar 3: Budget Enforcement

Inheritance-based (Equal, Weighted, Pool) budget caps.

Graduated enforcement: Allow → Warn → Throttle → Pause.

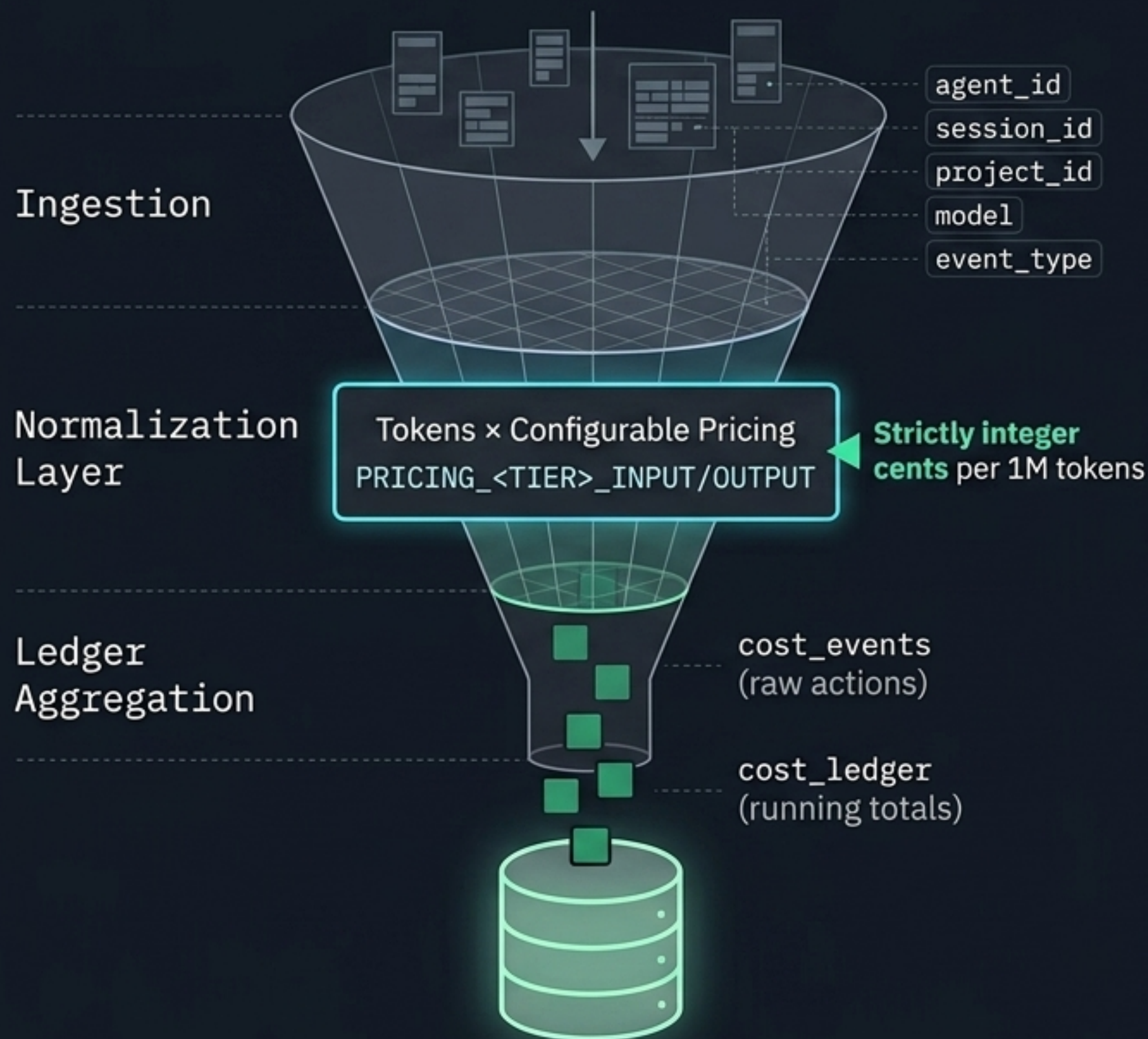
Pillar 4: Chargeback & ROI

Line-item reports generated for exact date ranges.

Calculates per-feature AI cost vs. estimated manual cost (ROI).

The Metering Funnel: From Tokens to Integer Cents

Normalizing multi-provider billing into a single, authoritative ledger.



Untrusted Correlation ID

`CLAUDE_CORRELATION_ID` is coerced to null if not a valid UUID to guarantee the cost write never aborts.

Latency Protection

Metering operations are constrained to a strict < 100ms overhead target.

Sentinel Exclusion

`claude-code-hook-presence` is recorded purely as activity. It never creates a `cost_events` row, ensuring budget and anomaly baselines remain completely clean.

Model Tier Matrix: Unifying 13 Ecosystem Tiers

Standardizing token-based and unit-based pricing models via environment overrides.

Token-Based Billing (Cents per 1M Tokens)

haiku	sonnet	opus
gemini-flash	gemini-pro	fable
ollama-local	codex	agy

Env Overrides:

```
PRICING_<TIER>_INPUT
PRICING_<TIER>_OUTPUT
PRICING_<TIER>_CACHE
```

Note: "fable" pricing is explicitly flagged as a placeholder (= "opus") pending confirmation of real API rates.

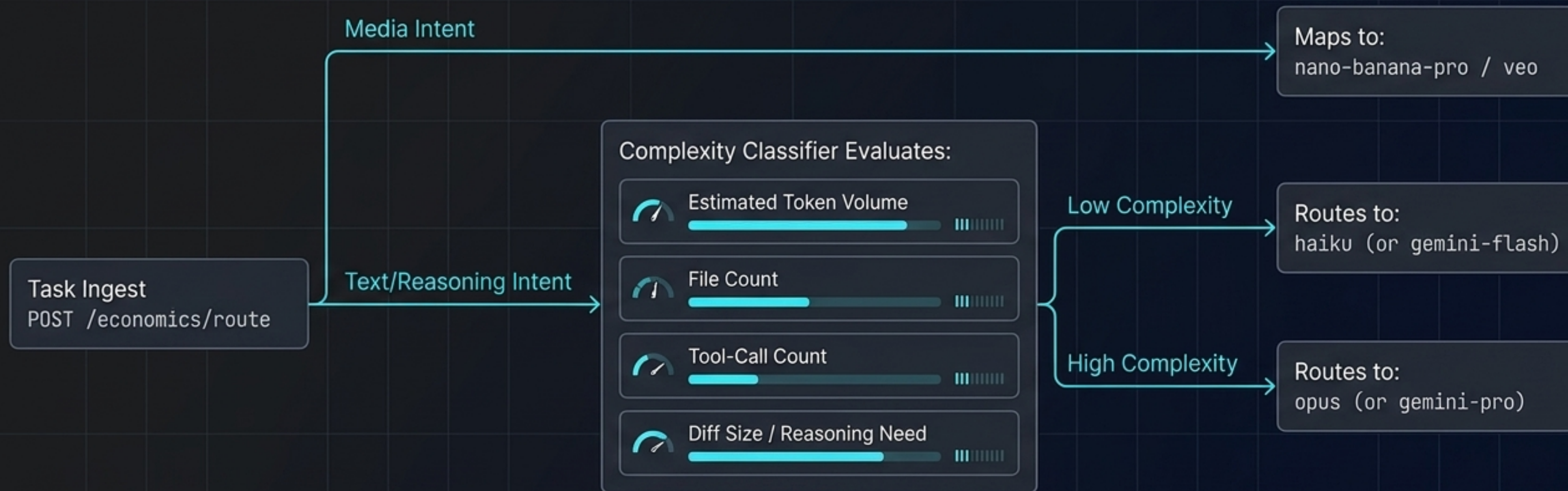
Unit-Based Billing (Mapped to Token Schema)

"nano-banana-pro"	: Per-image billing (Convention: 1 image $\approx$ 1024 tokens)
"veo"	: Per-second video billing
"elevenlabs / edge-tts"	: Per-character TTS billing

Routing Logic: Image, video, or TTS intent requests to "/economics/route" automatically return the corresponding "{ modality, tier }".

Heuristic Routing & Optimization

Mapping task complexity to the most cost-effective tier.



Admin Override Bypass Path

`POST /economics/routing/override` (Rate-limited: 10/min) forces a specific tier, permanently audited.

Budget Enforcement Action Matrix

Configurable, graduated threshold interventions per hierarchical scope.

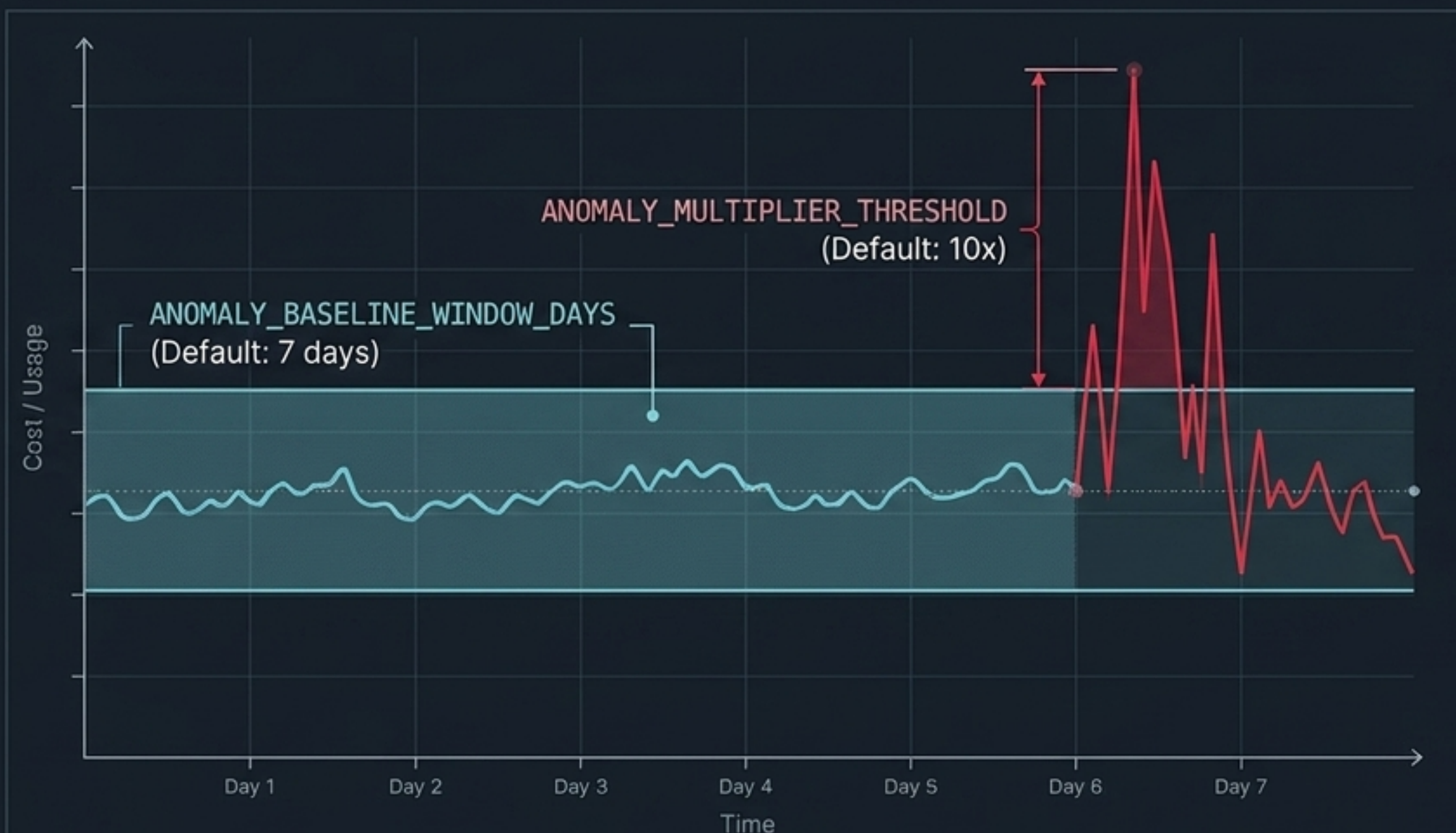
Threshold Env Var	Default	Action Triggered	System Behavior
BUDGET_THRESHOLD_MONITOR_PCT	60%	ALLOW	Silent telemetry logging.
BUDGET_THRESHOLD_WARN_PCT	80%	WARN	Alerts dispatched to Slack/Email/Webhook.
BUDGET_THRESHOLD_THROTTLE_PCT	90%	DOWNGRADE	Claude tiers auto-downgrade (opus → sonnet → haiku).
BUDGET_THRESHOLD_PAUSE_PCT	100%	BLOCK	Hard pause. Requests rejected.

Inheritance Strategy

Budgets support "EQUAL", "WEIGHTED", and "POOL" (Default) inheritance strategies across daily, weekly, monthly, or session-based periods.

The Anomaly Detection Engine

Defending against runaway costs via a 7-day rolling baseline.



System Action

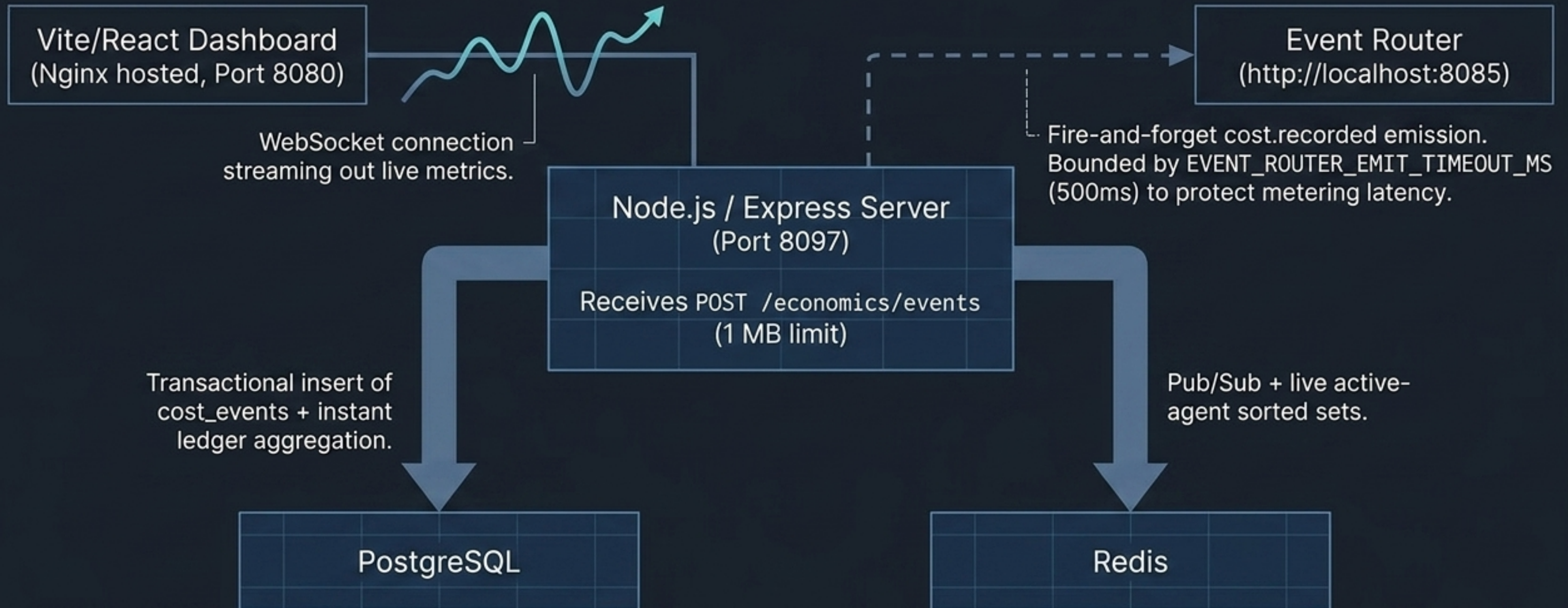
Flagged events appear in
`GET /economics/anomalies`
(last 24h).

Alert channels (
"ALERT_SLACK_WEBHOOK_URL",
"ALERT_EMAIL_SMTP_HOST") fire
immediately.

Requires manual clearance via `POST`
`/economics/anomalies/:id/resolve`
(Admin only, passing a
{`"resolution": "..."`} payload).

Sub-100ms System Architecture

Balancing transactional safety with real-time operational telemetry.



The Dual-Data Layer Diagnostic

Separation of concerns between the authoritative ledger and live overlay.

PostgreSQL (Source of Truth)

Role: Transactional, ACID-compliant historical ledger.

Key Tables:

- "cost_events" (raw data)
- "cost_ledger" (running totals)
- "budget_configs"
- "chargeback_reports"
- "roi_calculations"

Views:

"daily_cost_summary" (Materialized View, requires external refresh schedule).

Redis (Live Operations Overlay)

Role: In-memory, sub-millisecond execution and state.

Data Structures:

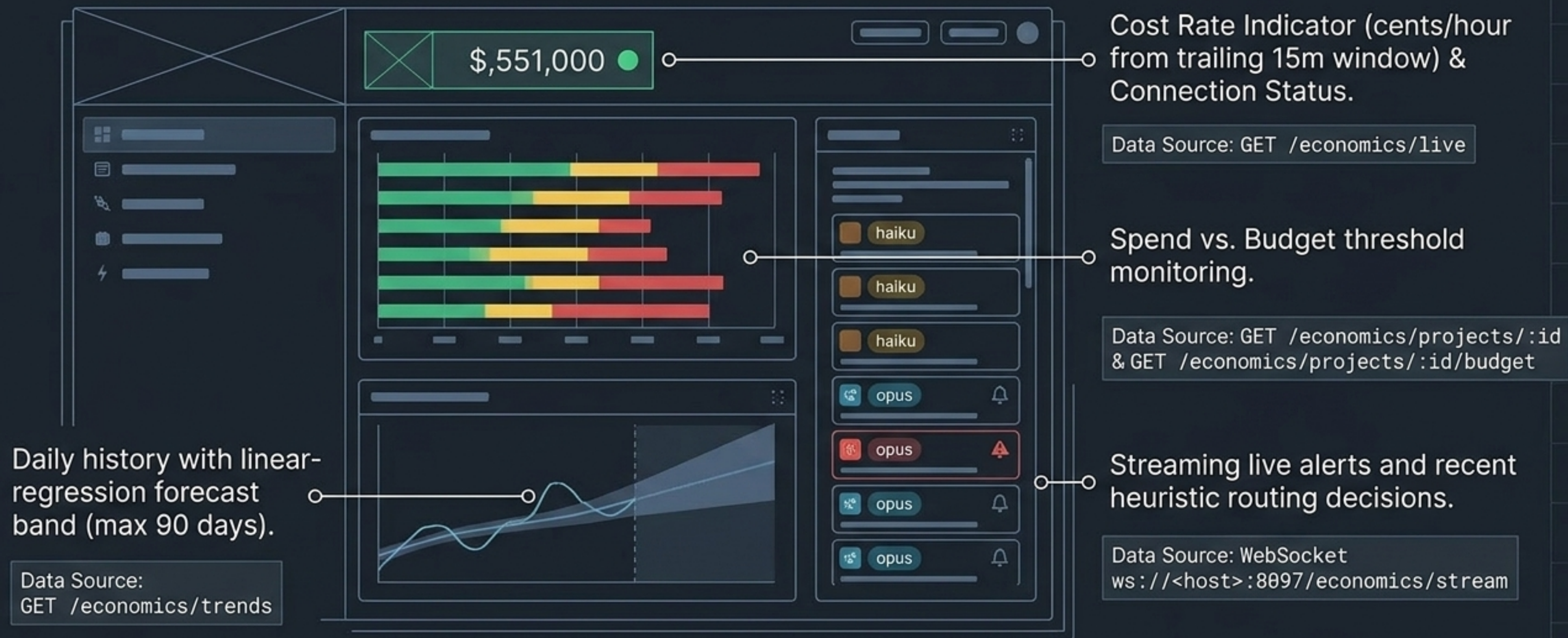
- Active agent sorted set (seen within "ACTIVE_AGENT_WINDOW_MINUTES").
- Events-per-minute counters.
- Anomaly baseline sorted set.

Engine:

Pub/Sub engine drives WebSocket streams for live budget and anomaly alerts.

The Financial Command Center Dashboard

Vite/React UI hosted via Nginx reverse-proxy on Port 8080.



Security Posture & Authentication

Hardened defaults, non-root execution, and strict JWT enforcement.

Strict Auth Enforcement

HS256 JWTs only. The "none" algorithm is explicitly rejected.

Validates "ECONOMICS_JWT_ISSUER" ("agent-economics").

Missing "ECONOMICS_JWT_SECRET" in production triggers an **instant HTTP 500**. No unauthenticated fallback.

WebSocket upgrades strictly require "Authorization: Bearer <token>" in the header (no query strings permitted per CIS0 policy).

Hardened Runtime

All containers execute as **non-root**. API runs as "node", Dashboard runs as "nginx" (UID 101).

"**helmet**" security headers enabled.

CORS restricted strictly to Dashboard origin and "localhost:3000".

Audit & Compliance

Local SQLite Governance Audit Bus ("AUDIT_DB_PATH") logs all lifecycle events.

Latest Code Hardener scan: **0 Critical / 0 High**, no secrets detected.

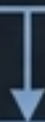
Supply Chain & Operations Profile

Lightweight, idempotent, and permissively licensed.

Docker Multi-Stage Pipeline

Stage 1: migrations target

Runs `npm run migrate` (Idempotent execution of migrations/*.sql via node:20-alpine).



Stage 2: api target

Spins up Node.js server on Port 8097.



Stage 3: dashboard image

Nginx embeds Docker DNS resolver to survive API container recreation seamlessly.

CycloneDX Certified SBOM

84

Runtime Components
(Excluding dev tooling)

100%

OSI-approved permissive
licenses. No copyleft.

MIT (75) | ISC (4) | Apache-2.0 (3) |
BSD-3-Clause (1) | MIT-0 (1)

Hardened Dependencies: ws (8.21.1) and nodemailer (9.0.3) explicitly bumped to clear previous upstream high-severity advisories.

The Bulletproof Standard

Bringing predictability, accountability, and security to multi-agent ecosystems.

	Financial Predictability Stop runaway costs before they happen with sub-100ms budget enforcement and instant "opus" to "haiku" auto-downgrades.
	Complete Accountability Trace every cent back to a specific session, agent, and project via JSON/CSV chargeback reports.
	Enterprise Grade Delivery Non-root containers, HS256 JWT auth, transactional Postgres guarantees, and an entirely permissive open-source supply chain.

Deploy the command center today via Docker.
Standardized. Secure. Bulletproof.