DEVOPTIC ARCHITECTURE & TRUST WHITEPAPER

# The Autonomous Full-Stack Observability & Self-Healing Fabric

*Technical Specification, Data Flow Topologies, and Enterprise Security Controls*

| | |
|---|---|
| **Document Version: 2.6.4-Enterprise** | **Classification: Public / SRE Distribution** |
| **Target Audience: Staff SRE, VP Eng, InfoSec** | **Status: Pre-release · Q2 2027 · Not yet audited** |

## 1. Executive Summary

DevOptic is an autonomous full-stack observability platform engineered to eliminate on-call alert fatigue through semantic fingerprint intelligence, continuous multi-cluster Kubernetes surveillance, sub-50ms container metric time-series querying, and integrated chaos resilience testing. Rather than merely forwarding alerts, DevOptic correlates telemetry across microservices, detects silent service lockups, verifies closed-loop recovery via an autonomous 30-minute stability engine, and compiles automated Post-Incident Reviews (PIRs).

## 2. Agent Resource Economics & Footprint

Traditional APM and observability agents introduce CPU spikes, memory bloat, and garbage collection pauses. DevOptic utilizes an ultra-lightweight Go kernel binary and DaemonSet built with the following hard ceilings:

| Dimension | Design Target | Mechanism |
|---|---|---|
| Node CPU Budget | < 0.5% vCPU per host | Low-frequency delta sampling & compiled Go runtime |
| Agent Memory Cap | < 32MB RSS | gzippool sync.Pool reuse, zero runtime allocations |
| Network Egress | Compressed in-flight streaming | Batched delta payloads via TLS 1.3 mTLS |
| Data Residency | 0 secrets / credentials written | In-flight logredact scrubber eliminates PII/keys |

## 3. Cognitive Fingerprinting & The 6-Stage Stability Machine

When a Kubernetes pod reschedules or a Docker container crashes, traditional monitoring fires individual alerts for every crash loop, OOMKill, and container recreation. DevOptic utilizes a multi-tiered identity hierarchy:

- **Semantic Identity Derivation:** Evaluates compose_service → container_name → service_name → host + bare image. Ephemeral container hex IDs and transient UUIDs are strictly discarded using *isEphemeralID()*.

- **6-Stage Stability State Machine:** Tracks active issues systematically across *monitoring* → *flapping* → *recurring* → *chronic* → *stabilizing* → *recovered*.
- **30-Minute Closed-Loop Auto-Resolution:** An autonomous background promoter executes every 5 minutes. If a service demonstrates 6 consecutive healthy checks (30 consecutive minutes), DevOptic marks the incident resolved and auto-generates a Markdown Post-Incident Review.
- **7-Day Relapse Memory:** If a service fails again within 7 days, DevOptic re-opens the exact investigation lineage rather than treating it as a novel occurrence.

## 4. Enterprise Security, Governance & Zero-Trust

Observability systems require deep visibility into production infrastructure. DevOptic adheres to defense-in-depth zero-trust security principles:

- **Cascading Multi-Environment Isolation:** EnforceEnvironmentAccess middleware enforces tenant and environment boundaries. Operators scoped to Staging are cryptographically barred from querying or mutating Production clusters.
- **In-Flight Sensitive Log Redaction:** The streaming logredact engine inspects container logs in memory and sanitizes JWT secrets, private SSH keys, AWS/GCP access tokens, Bearer headers, and credit card / PII data before logs touch disk or MinIO object storage.
- **Zero-Knowledge Secrets Vault:** Integrated AES-256 GCM vault stores API keys and credentials, accessible only through scoped service bindings.
- **Audit Trails:** Every role evaluation, permission grant, and anomaly acknowledgment is logged to an immutable append-only audit log with requesting identity, IP, and timestamp.

## 5. Supported Deployment Topologies

DevOptic supports three flexible deployment models for enterprise customers:

1. **100% Air-Gapped / Private VPC:** Deployed entirely inside your private AWS/GCP/Azure VPC or on-premises datacenter. Zero telemetry leaves your secure network perimeter.
2. **Hybrid Telemetry Mesh:** Keeps high-volume container time-series metrics and logs local in your cluster VPCs, only federating anonymized incident contributor keys and alerting states to a central DevOptic command hub.
3. **Dedicated Single-Tenant SaaS:** Dedicated cloud infrastructure provisioned per customer tenant with dedicated PostgreSQL, MinIO, and WebSocket distribution instances.

---

**DevOptic Engineering & Security Architecture Group · For technical questions or security review scheduling, contact hello@devoptic.dev**