Komodo Systems | Technical Whitepaper

Architectural Resilience: Future-Proofing Komodo Eye

Why Komodo Eye remains the superior observability choice for mission-critical Industrial & Utility Networks.

Komodo Systems
e> info@komodosystems.com
w> www.komodosystems.ai

Executive Summary

Emerging technologies such as TLS 1.3, Streaming Telemetry, and eBPF are reshaping the landscape of IT observability. However, industrial and utility networks operate under distinct constraints: determinism, legacy interoperability, and strict data sovereignty.

Komodo Eye is architected specifically to navigate this "brownfield" reality, providing a critical bridge between legacy hardware and modern security standards where generalist IT tools fail.

Maintaining Visibility in an Encrypted (Dark) Network

The Technical Challenge
The deprecation of cleartext metadata (SNI) via Encrypted Client Hello (ECH) and TLS 1.3 renders traditional Deep Packet Inspection (DPI) obsolete without resource-intensive decryption proxies.

The Komodo Architecture: Heuristic Flow & Counter Analysis
Komodo Eye decouples observability from payload visibility. Instead of relying on decrypted packets, we utilize Encrypted Traffic Analysis (ETA) Principles.

By correlating Layer 3/4 flow records, IPsec tunnel counters, and traffic directionality/volume heuristics, we detect performance degradation and anomalies without breaking the encryption chain or introducing latency-heavy proxies.

Hybrid Telemetry Ingestion (SNMP vs. Streaming)

The Technical Challenge
Cloud-native infrastructure is shifting toward "push-based" streaming telemetry (gRPC, OpenTelemetry), often framing SNMP as a legacy bottleneck.

The Komodo Architecture - Multi-Protocol Data Normalization
Industrial networks are rarely homogenous; they consist of 30-year-old Remote Terminal Units (RTUs) alongside modern IoT gateways. (Note: RTUs are microprocessor-based electronic devices used in industrial environments to connect physical hardware to a control system.)

Komodo Eye utilizes a hybrid engine that supports modern push-based ingestion (gRPC, tr069, REST APIs) while maintaining a robust, optimized SNMP/TL1 polling engine. We provide a unified

data structure for both, ensuring visibility of critical legacy assets that will never support OpenTelemetry.

Data Sovereignty & On-Premises AI

The Technical Challenge
Public cloud AIOps (AWS, Azure) and hardware-embedded LLMs introduce data exfiltration risks and a dependence on internet connectivity, violating strict industrial security policies such as NERC CIP.

The Komodo Architecture: Edge-Native, Air-Gapped Intelligence
Komodo Eye's roadmap prioritizes local inference. Our predictive analysis models run on-premises, training on your specific network baselines without sending log data to a third-party cloud. This ensures compliance with air-gapped security requirements while delivering a predictive reduction in Mean Time to Repair (MTTR) tailored to utility traffic patterns rather than generic web traffic.

Verification in Zero Trust Environments

The Technical Challenge
Zero Trust Network Access (ZTNA) and ephemeral micro-segmentation obscure static IP relationships, making traditional topology maps appear fragmented.

The Komodo Architecture - Cross-Vendor "Source of Truth"
Vendor-specific Zero Trust implementations often create "black boxes" where visibility is limited to that vendor's ecosystem. Komodo Eye serves as the independent source of truth, verifying that physical infrastructure supports logical security policies.

By ingesting data across the multi-vendor stack, we verify that the physical underlay supports the logical overlay. In utility environments, reliance on a single vendor for enforcement and verification creates a dangerous single point of failure; Komodo provides the necessary independent check.

Depth of OT Context vs. Security Suites

The Technical Challenge
Security vendors (Palo Alto, Fortinet) are increasingly bundling "network visibility" into their platforms, arguing for a consolidated "single pane of glass".

The Komodo Architecture: Operational vs. Threat Context
Security tools are optimized for threat detection (malware, intrusion attempts), not for operational health (voltage sags, recloser latency, modem signal-to-noise ratios). Komodo Eye provides device-specific depth for SCADA assets—such as modems, meters, and reclosers—that security platforms treat as generic nodes. While they answer, "Is it infected?" Komodo answers, "Is it working efficiently?".

The eBPF Barrier: Observability for Legacy & Embedded Assets

The Technical Challenge
eBPF is becoming the standard for observability in Linux-based cloud/container environments, offering kernel-level visibility.

The Komodo Architecture: Non-Intrusive Determinism
eBPF requires an accessible Linux kernel. Many industrial assets (PLCs, RTUs, proprietary switches) run on embedded firmware or real-time operating systems (RTOS) where eBPF is impossible to deploy. Komodo Eye is architected for agentless, external monitoring that respects the deterministic requirements of OT loops without requiring kernel modifications or risking stability on critical control devices.

Conclusion - Filling the Operational Gap

While hardware vendors offer free basic monitoring from the bottom and security giants provide threat-focused visibility from the top, a critical gap remains in the middle: Operations.

Komodo Eye fills this gap, ensuring that despite encryption, legacy protocols, or proprietary hardware, the grid remains visible, mapped, and managed.

Summary

Layer	Provider	Primary Focus	The Outcome
Top-Down	Security Suites	Threat Detection ("Is it infected?")	Security
Middle	Komodo Eye	Operational Health ("Is it efficient?")	Resilience
Bottom-Up	Hardware Vendors	Basic Device Connectivity	Connectivity

Discover how Komodo Eye bridges the gap at www.komodosystems.com.