

Komodo Eye® Technical Data Sheet

Key Capabilities & Architectural Highlights

A comprehensive network management, observability, & automation platform providing deep, full-stack data collection for mission-critical infrastructure.

Visibility & Scope

- **Unrivaled Multi-Vendor Support:** Native, agentless monitoring for over 88,000 device models across 8,000 manufacturers.
- **Full-Stack Depth (Layer 0 through Layer 7)**
 - **Layer 0:** Physical power systems, rectifiers, battery plants, generator fuel levels, and environmental sensors
 - **Layer 1/2:** Optical transport (DWDM/SONET), microwave, RF, fiber optics, and switching.
 - **Layer 3:** IP routing, IS-IS/OSPF protocol adjacencies, MPLS control planes (LSPs/SDPs), and IPsec tunnels
 - **Layer 4–7:** Transport protocols, WMI/WinRM server metrics, web services/URLs, and OT grid logic (DNP3, Modbus).
- **Atomic Telemetry Ingestion:** Captures granular sub-component details (individual sub-card faults, chassis temps, serial numbers, micro flaps) in raw form.

Intelligence and Data Retention

- **5-Year Granular Data Lake:** Retains high-resolution time-series data (latency, loss, jitter) for 5 years, enabling long-term trend analysis.
- **Utility-Grade Reliability Metrics:** Converts raw network errors directly into N-SAIDI (duration) and N-SAIFI (frequency) reporting for regulatory compliance.

Security, Resilience & Compliance

- **100% On-Premises & Air-Gapped:** Zero external dependencies or outbound internet requirements. Authorized as a NERC EACMS cyber asset and built for defense and nuclear mandates.
- **Resilient Edge Architecture:** Features disk-backed persistent queues, intelligent backpressure, and automated data replay to survive total connectivity loss during severe storms or outages.
- **Security & Change Auditing:** Includes automated rogue device detection, password management, firmware/patch auditing, and immutable JSON audit logging for configuration-as-code accountability.

Advanced Troubleshooting & Self-Healing

- **MAC-Based Physical Port Locator (Layer 2):** Scours switch forwarding tables to pinpoint the exact physical location (Site, Switch, Port) of rogue or firewalled devices in seconds
- **MPLS & IP Path Tracing (Layer 3):** Instantly traces IP endpoints through complex, nested MPLS paths to locate communication bottlenecks.
- **Closed-Loop Tunnel Remediation:** Continuously monitors bidirectional flows across thousands of IPsec tunnels, automatically bouncing/re-keying "hung" or asymmetric tunnels without operator intervention.
- **SCADA "Slow Flinger" Engine:** Monitors low-bandwidth field area networks (e.g., 900 MHz radios) from base stations using lightweight sampling to prevent SCADA channel congestion.

Data Collection & Integration Methods

- **Polling Protocols:** Customized ICMP (GPE), SNMP (v1, v2c, v3 with SHA-512/AES-256), WMI/WinRM, Modbus, TL1, HTTP/HTTPS.
- **Streaming Telemetry & APIs:** gRPC, gNMI, REST APIs, Webhooks, TR-069, TR-369 (USP), NETCONF/YANG.
- **Traffic & Event Message Logging:** Syslog, SNMP Traps, NetFlow (v5/v9), IPFIX, sFlow, J-Flow, CLI (SSH/Telnet scraping).

Fully API-Driven Ecosystem Integration

- **API-First Architecture:** Operates as a central nervous system using native, bidirectional REST APIs to ingest telemetry, push automated configs, and synchronize network state with corporate systems of record
- **Active API Orchestration:** Direct API-based active provisioning.
- **Bilateral Enterprise Integrations:** Seamlessly pushes and pulls data via REST API.
- **Ecosystem Connectors:** Examples include bilateral ServiceNow CMDB integration, Nokia NSP, Cisco Catalyst Center, Ciena, Adtran MCP, GE Smallworld GIS, Splunk, PagerDuty, and Sonar.