Komodo Eye - Comprehensive Overview

Komodo Systems
info@komodosystems.com
www.komodosystems.com

Overview

Komodo Eye holds a unique position among critical network infrastructure vendors offering network monitoring solutions (NMS). It monitors and manages IT and OT environments.

Modern utility and enterprise environments are often forced to choose between vendor-locked tools that are "deep but narrow," or IT-centric monitors that are "wide but shallow." Komodo Eye eliminates this compromise.

As the industry's only high-fidelity Network Management System (NMS), Komodo Eye provides a unified "Single Pane of Glass" that spans from Layer 0 (Power & Environment) to Layer 5 (Application Delivery).

By monitoring 88,000 device models across 8,000 manufacturers, it provides the granularity of a vendor-specific tool with the universal reach of an enterprise platform.

Whether managing 10 million endpoints across a nuclear fleet or tracking micro-flaps in a microwave backhaul, Komodo Eye ensures that critical infrastructure stays visible, secure, and resilient.

Elevator Pitch

Komodo Eye — Field-Tested Scale. Air-Gapped Security. Predictive Analytics.

Operator Experience & Daily Workflow

Komodo Eye is designed for engineers and operators who live on the platform every day. The entire system is 100% browser-based, requiring no local agents, desktop software, or client installations. Users access the system securely through a standard web browser, while all data and processing remain fully on-premises.

The interface is optimized for real-time operations:

- Instant navigation across millions of devices without page reloads
- Live status visibility using Normal / Warning / Critical indicators
- Consistent workflows across sites, devices, and device classes

This approach minimizes training overhead while maximizing situational awareness for NOC, field, and engineering teams.

Industry Challenge

Critical infrastructure organizations are typically trapped between two suboptimal choices. Komodo Eye removes this trade-off.

- Vendor-specific tools (e.g., Nokia NSP or Cisco Prime) that are "deep but narrow" in data collection. They are excellent for monitoring one brand of device but are blind to all other devices.
- Enterprise IT tools (e.g., SolarWinds, LogicMonitor, and Nagios) monitor devices in a "wide but shallow" manner. While SolarWinds can indicate if a router is online, it cannot explain the complex MPLS signaling or microwave signal-to-noise ratios that caused a "brown-out" in the first place.

Komodo Eye Solution

Komodo Eye is the only NMS platform that gathers device data "wide" (multi-vendor) and "deep" (multi-layer). In terms of "wide," it supports an industry-leading library of 88,000 device models across 8,000 manufacturers, while penetrating deeply into each manufacturer's technical stack.

It replaces a dozen disparate legacy NMS with a single "source of truth" by monitoring everything from Layer 0 (the physical rectifiers and battery plants powering the rack) to Layer 5 (the specific applications delivering data to the grid).

Proven Scale & Reliability
Komodo Eye is field-tested in some of the world's most demanding environments.

- *Large Midwest Electric Utility:* Komodo Eye monitors 4.3 million endpoints every 5 minutes, tracking every interface, IPsec tunnel, and environmental sensor across the entire power grid.
- *Large East Coast Electric Utility*: Komodo Eye manages 10 million devices ranging from nuclear, wind, and solar sites, providing unified visibility.

Absolute Security Mandate
Unlike modern "cloud-first" tools, Komodo Eye is a 100% on-premises solution and 100% air-gapped. No data is shared with the public internet. This design satisfies stringent requirements such as NERC CIP compliance and high-security nuclear environments, where Komodo Eye servers have logged over 900 days of continuous uptime without requiring external connectivity for security updates.

Global Intelligence & Geocoding

Komodo Eye provides the proverbial "Single Pane of Glass" through site-level aggregation, simplifying massive network management.

Real-Time Geocoding on Ingest
Every data point—numeric or semantic—is geocoded the moment it is measured. This enables map-enabled visualization, geographic correlation, and rapid identification of regional failure points. For example, in the Dashboard, engineers can view an intuitive, high-level status (Normal/Warning/Critical) based on geographic risk, such as identifying a cluster of failures in a single storm-hit city.

The system allows users to manually adjust device locations by moving them on the map, which automatically updates the latitude and longitude coordinates in the database.

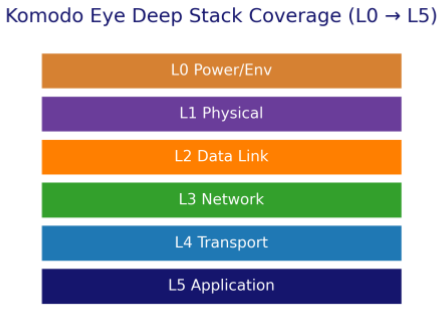
- *Live Network Summary and Drill-Down Views:* Customizable Network Summary Panes provide at-a-glance visibility by technology and status. Every metric is live and clickable, allowing you to drill directly into the devices contributing to an alert, maintain full filtering and sorting after drill-down, and automatically update as conditions change.
- *Relationship Mapping*: Geocoded data is used to build relationship maps, including OSPF and MPLS adjacency weights and point-to-multipoint wireless and LTE client relationships.
- *Edge Label Visibility:* The map view includes "edge label visibility," allowing users to see specific metrics (such as OSPF weights) directly on the connection lines between devices.
- *Mobile Tracking*: For devices with GPS support, the system can track and display a mobile device’s historical movement.
- *Site Journal & Digital Documentation:* Hierarchical journals exist at the network, site, and device levels. Sites function as digital vaults containing manuals, diagrams, photos, acceptance tests, firmware, and technician notes.
- *Contextual History*: Every substation, 911 center, or transmission tower functions as a digital vault. Site diagrams, cabinet photos, equipment manuals, and Operational Acceptance Tests (OATs) can be uploaded directly to the site record.
- *Unified Technician Logs*: When a field technician performs a microwave realignment at 3 AM, they log it in the site journal. When the next shift starts at 8 AM, the next technician does not need to guess what has changed; they instantly see the full history, notes, and photos, preventing a redundant site visit.

Reliability Metrics (SAIDI/SAIFI)
Komodo Eye measures availability by both **frequency** and **duration** of interruptions. Momentary flaps are tracked alongside sustained outages, enabling utility-grade reliability reporting and long-term trend analysis.

- *Frequency (SAIFI)*: Komodo Eye monitors "momentary interruptions" and instability. If a device "flaps" 35 times in 24 hours, it is flagged as a reliability risk, even if currently reachable.
- *Duration (SAIDI)*: Komodo Eye captures the exact duration of every micro-outage. For example, if a critical link is lost for 10 seconds, the data is preserved in a data lake for 5 years, enabling precise reliability reporting and long-term trend analysis of aging equipment.

The Deep Stack (Layer 0 to Layer 5)

Komodo Eye bridges the gap between legacy serial gear and modern software-defined networks.



Atomic Data Collection
Komodo Eye collects *atomic data*—the smallest meaningful telemetry units—such serial numbers for asset tracking, firmware versions for security audits, internal chassis temperatures, and specific sub-card failures, such as identifying a single faulty Media Dependent Adapter (MDA) card within a Nokia SAR-8 router before it causes a total reboot.

Refresh Capabilities
Users can set "Auto-Refresh" to continuous, 5-second, or 1-minute intervals to monitor critical errors in real time.

- *Data Types:* All incoming data is categorized as either numeric (counters, signal strength, jitter) or semantic (log messages, SNMP traps, words/sentences).
- *Interface Granularity:* Beyond physical ports, the system tracks all virtual interfaces, including VLANs, IP sub-interfaces, radio ports, and emulated interfaces (e.g., TDM emulation).

From Telemetry to Intelligence
Komodo Eye follows a structured pipeline:

1. Scheduled probes (typically every 300 seconds)
2. Variable collection via SNMP, tables, or inbound messaging
3. Mathematical or semantic transformations
4. Calculated variables stored alongside raw telemetry
5. Storage strategies that determine visualization and retention

Storage strategies include line graphs, rate graphs, track-changes-only storage, and table capture.

Protocol Depth & Legacy Connectivity
Legacy Assets: Komodo Eye supports legacy, non-IP assets, including Serial (1200 baud) connections, TL1 for legacy SONET plants, Modbus for the physical breakers and RTUs (Remote Terminal Units) found in every substation.

Modern Infrastructure: Komodo Eye fully supports modern standards, including TR-069/TR-386 for LTE field area networks, gRPC for high-speed telemetry, and SNMP v3 with full SHA/AES encryption.

Interface & Tunnel Monitoring at Scale
Komodo Eye continuously tracks all interfaces on all devices, physical and logical, such as:

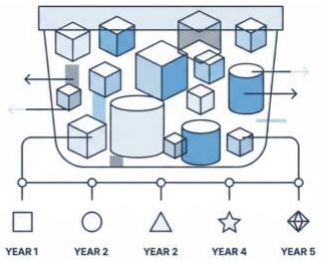
- Physical ports and fiber
- Radio and microwave interfaces

- VLANs and IP sub-interfaces
- Emulated interfaces (e.g., TDM over packet)

For each interface, Komodo Eye captures status, traffic, packet counters, error trends, and MAC associations—polled continuously and retained long-term.

At a large electric and gas utility on the East Coast, Komodo Eye monitors over 30,000 IPsec tunnels in real time. It is smart enough to detect "asymmetric traffic"—where data goes out one path but comes back another—and can trigger an automatic tunnel "bounce" to restore optimal performance without human intervention.

5-Year Granular Data Lake
Most tools only gather data for 30 days, then purge it. Komodo Eye maintains granular data (latency, loss, jitter) for 5 years. This is essential for microwave operators, for example, who track encroachment analysis (e.g., tree growth), such as when a tree gradually grows into the line-of-sight path between two towers and causes a slow, 3-year decline in signal strength.



Discovery & Troubleshooting (MAC vs. IP)

Komodo Eye performs "needle in a haystack" searches to reduce Mean Time to Repair (MTTR) from hours to minutes.

Layer 3 Search (IP Navigator)
Komodo Eye can instantly locate any IP address on the network. It will indicate if the device is "online" and identify exactly which router and physical port that specific IP is communicating through, even in complex, nested MPLS environments.

- Dual-Filtering: The platform uses both server-side (to pull data from the database) and client-side (browser-based) filtering of loaded data, which can be combined to drill down into specific equipment.
- Dynamic Columns: The browser interface allows users to dynamically add, drag, and sort columns (e.g., SNMP status, IP address) and save these custom views as default login layouts.

Layer 2 Search (Port Hunter)
Komodo Eye can search by MAC address to locate silent or firewalled devices by traversing switch forwarding tables. It combs the forwarding tables of every switch in the network to indicate exactly where that device is physically plugged in (e.g., "Summit Substation, Switch 4, Port 118"). This is a game-changer for locating rogue devices.

Dynamic Tables, Columns & Layouts
All tables are fully user-configurable to this level of detail:

- Dynamic column injection
- Drag-and-drop ordering
- Multi-column sorting
- Client-side filtering for instant response
- Saved layouts per user

Nearly all tables can be exported to CSV or Excel.

Semantic Intelligence & Message Indicators
Komodo Eye treats logs as data. Message indicators analyze millions of logs to identify rare events, correlate anomalies across devices, and surface subtle manufacturing defects or security risks. For example, if an unusual error message appears only 4 times a year across 10 million devices, Komodo Eye flags it. This allows engineers to identify manufacturing bugs in a batch of equipment or catch the subtle first signs of a sophisticated security breach before it escalates.

Intelligence: The 3 Phases of AI

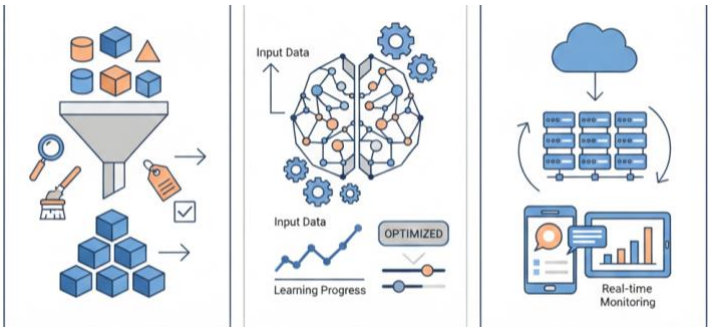
There is a 3-part product development roadmap for adding Artificial Intelligence capabilities to Komodo Eye via an on-box, air-gapped Large Language Model (LLM).

The Hardware Requirement

Komodo Eye does not share sensitive data with cloud servers. This solution runs on premises entirely. It requires dedicated hardware, typically utilizing NVIDIA GPUs (RTX 5090 for small deployments or A6000 clusters for large utilities) to process the LLM locally.

Phase 1 (Document Intelligence):

The AI product is specifically designed to access and analyze "Tags" (metadata such as cable colors) and the hierarchical journaling system to assist with troubleshooting. It "reads" every uploaded manual, OAT, and site log. It serves as a *"digital mentor."* For example, a junior technician can query the chat interface, "How do I set an IP on an Extreme Networks VLAN using the CLI?" In an instant, the correct syntax is located within a specific manufacturer's manual stored in the vault. This preserves senior experts' knowledge as they retire.



Phase 2 (Root Cause Analysis)

The AI correlates data across different technology tiers. It can explain a complex failure: "Substation X went dark not because of a network bug, but because the Nokia router lost power. The power was lost because the battery plant hit its 4-hour discharge limit following a city-wide AC outage." It connects the dots between power and networking.

Incident Anomaly Analysis: This tool performs correlation by identifying if a specific message indicator seen on one device has appeared on other devices within the same timeframe.

Phase 3 (Predictive Analysis)

This is the future of grid management. The AI identifies risks *before* they manifest. It can issue a warning that "a specific fiber link is fading at a rate that suggests an impending break," or "based on historical discharge cycles, this substation battery will fail to meet NERC requirements in 3 months."

Energy & OT Monitoring

Komodo Eye is an infrastructure tool, not just a network tool.

Industrial IoT & IoT 4.0

It monitors industrial assets such as circuit breakers, capacitor banks, and RTUs using Modbus and TL1—bridging IT and OT environments to ensure the physical delivery of power is as stable as the network that controls it.

Global Regulatory Compliance

In international markets, new regulations require organizations to report detailed energy, water, and fuel consumption to the government. Komodo Eye automates this task by pulling data directly from sensors and providing audit-ready reports.

Environmental & Social Impact

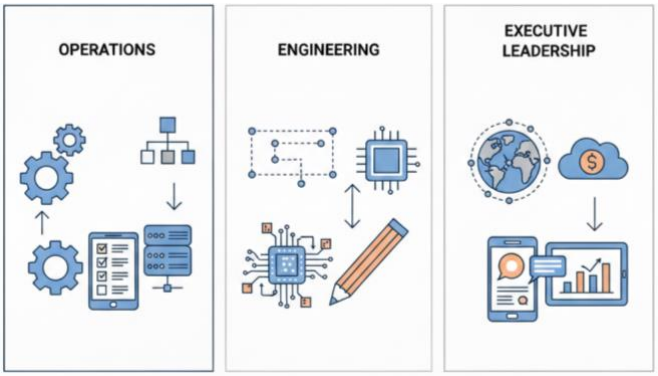
School System Case Study: Komodo Eye monitors printer usage across 25 schools. Tracking the number of pages printed helped the district calculate its environmental footprint and translated that into a "trees to replant" program for students, turning raw data into a community initiative.

Hair Dryer Anecdote: To prove the system's granularity, one of our developers uses Komodo Eye at home. He monitors every breaker in the electrical panel to see how much power each appliance uses, to calculate the cost-per-use in real-time. This demonstrates that Komodo Eye is scalable from the edge to the core.

Targeted User Personas

Komodo Eye is specifically engineered to serve three distinct organizational tiers, transforming raw network telemetry into actionable insights tailored to the specific needs of each group:

Operations — Real-time monitoring, alerts, IPAM, daily health
Focused on the "daily drive" to keep the network running, these users use tools such as IPAM, daily reports, and real-time alerts to perform day-to-day maintenance and rapid troubleshooting.



Engineering — Trend analysis, capacity planning, optimization
These users leverage deep data for long-term capacity planning and configuration optimization, analyzing message trends and core routing health to improve overall network performance.

Executives — Availability, MTTR, risk exposure, capital planning
Targeted through high-level performance metrics and risk analysis reports, this group uses the data to make informed capital allocation decisions and determine where to invest to improve the network.

Customized Actionable Reports
Network engineers do not have time to monitor millions of devices. Komodo Eye sends targeted reports to specific teams. The "Microwave Team" can receive a daily briefing on path fades, while the "Fiber Team" can receive a report on optical discards. This keeps each team focused only on what matters.

Login Tracking
The system tracks and logs all user logins to every device on the network for auditing purposes.

Security, Access & Compliance

Komodo Eye translates "big data" into "actionable knowledge" through a combination of targeted intelligence, secure access, and integrated infrastructure tools.

Role-Based Access Control
Supports Active Directory, TACACS, and local authentication. Permissions can be scoped by device type and action. All logins and actions are audited.

Alarm & Alert Engineering
Alerts are built on raw or calculated variables, support dynamic messages, severity control, and scoped suppression at the device or device-class level.

Security Watchdog & Inventory Reconciliation

- *Inventory Reconciliation*: The system identifies "uninvited" devices by continuously comparing the live network—detected via ISIS system IDs and MAC addresses—to an official inventory database. If an unauthorized device is added, the security team receives an immediate alert.
- *User Authentication:* The rights system supports Active Directory and TACACS authentication. It allows for highly granular roles, such as permitting users to see all devices on the network while restricting modification rights to specific equipment types, like MPLS routers.

- *Audit Logging*: The system tracks and logs all user logins across the network for comprehensive security auditing.

Ecosystem Integration & Deployment
Komodo Eye functions as both a centralized source of truth and a system-of-record bridge, providing:

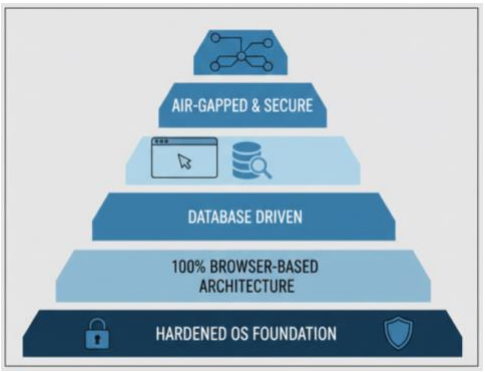
- Bidirectional CMDB and inventory synchronization
- Northbound and southbound API integration
- Native IP Address Management (IPAM)
- Bare-metal configuration, acceptance testing, and deployment automation

Designed for seamless interoperability, Komodo Eye integrates easily with existing ecosystems:

- *API Integration:* Inbound and outbound APIs enable event and alert exchange with platforms such as ServiceNow, PagerDuty, and Sonar.
- *Automation at Scale:* Scheduled and policy-driven actions can be executed across thousands of devices, including firmware updates and enforced credential changes.
- *Provisioning & Deployment:* A built-in bare-metal configuration utility generates and deploys hardware configurations directly to devices

Quantum Safety
For sensitive clients, Komodo Eye has partnered with Quantum Safe computing companies to monitor Quantum Key Distribution (QKD) links. It tracks the health of single-photon encryption keys, ensuring that the next generation of secure communications is monitored.

Technical Details



Foundation
Built on hardened Red Hat or Oracle Linux with a 100% browser-based UI powered by Node.js, the platform uses a Postgres database enhanced with Timescale for high-velocity time-series data and PostGIS for precise geographic mapping.

High-availability configurations ensure the system never blinks.

This design requires no local agents to be loaded on client machines and eliminates the need for users to manage local software or complex password rotations.

Cutting-Edge Core
To handle millions of polls per minute, Komodo Eye middleware is being ported to Golang for maximum concurrency and speed. The system includes a built-in bare-metal configuration utility to push builds directly to hardware, a fully integrated IPAM (IP Address Management) system, and automated acceptance testing.

Data Collection & Polling
Data collection is managed via customizable probes associated with specific device types. These probes are typically executed every 300 seconds (5 minutes) and can perform various functions.

- *Protocol Support*: Probes execute SNMP GET, GET NEXT, or full Table Collects.
- *CSV Walking*: The system can "walk" a specific Object Identifier (OID) and store the results as a comma-separated value.
- *Atomic Data Categories*: Information is ingested as either numeric data (counters, interface levels, signal strength) or semantic data (words, logs, SNMP traps).

- *Advanced Table Capture*: Komodo Eye can capture entire SNMP MIB tables and convert them into database tables for long-term tracking and reporting.

Data Processing & Storage Optimization
Once ingested, the system transforms raw "atomic" telemetry into readable intelligence.

- *Variable Function Chaining*: Users can perform mathematical and semantic string functions on raw data, which can be chained together to create new variables. For example, "time ticks" are converted into "hours of uptime" for improved human readability.
- *Storage Optimization*: To maintain a high-resolution 5-Year Data Lake, the system uses various storage strategies:
    - Line Graphs: Standard tracking of a variable every 5 minutes.
    - Rate Graphs: Used for tracking the rate of change, which is essential for interface traffic.
    - Track Changes: A high-efficiency method that only stores data when a value changes, such as for firmware versions.

- *Dynamic Visualization:* Users can dynamically add, drag, and sort columns in their browser, saving these custom layouts as their default view.
- *Universal Data Export:* For external analysis, almost all table views across the platform can be exported directly to CSV or Excel.

True High Availability
For mission-critical operations, Komodo Eye supports Active-Active or Active-Passive configurations with automated failover, ensuring the "eye" never blinks.

Global Flexibility
The platform is designed for channel partners. It fully supports white-labeling and rebranding, allowing systems integrators and government entities to present the tool as a native component of their service catalogs.

Summary

Komodo Eye is engineered for environments where downtime is catastrophic. It delivers unrivaled visibility, absolute security, and predictive resilience—transforming raw telemetry into actionable intelligence for the most demanding infrastructure in the world.

Unrivaled Visibility
Komodo Eye ingests "atomic data" from both legacy serial assets (Modbus/TL1) and modern high-speed telemetry (gRPC/SNMPv3), creating a 5-year granular data lake for precise trend analysis and regulatory compliance.

Absolute Security
Designed for NERC CIP and high-security mandates, Komodo Eye is a 100% on-premises, air-gapped solution. Its integrated LLM provides local, "on-box" AI intelligence without ever exposing sensitive data to the public cloud.

Predictive Resilience
Move beyond reactive troubleshooting. With built-in SAIDI/SAIFI tracking and AI-driven root cause analysis, Komodo Eye identifies impending fiber breaks, battery failures, and path fades months before they impact the grid.

Cont.

Feature Highlights

Category	Feature	Technical Capability
Visibility	**Unparalleled Multi-Vendor Support**	Native monitoring for 88,000+ models across 8,000 manufacturers (Cisco, Nokia, Schweitzer, etc.).
	Deep Stack & Interface Monitoring	Full-spectrum visibility from Layer 0 (Power/Battery) to Layer 5 (Application/Grid Logic). Tracks all physical and virtual interfaces, including VLANs, IP sub-interfaces, and emulated interfaces.
	Atomic Data Ingest	Ingests information as numeric data (counters, signal strength) or semantic data (logs, SNMP traps, and API messaging).
Intelligence	**5-Year Data Lake**	Retains high-resolution telemetry (latency/jitter) for 60 months to detect long-term degradation like "tree growth".
	Air-Gapped Gen-AI & Anomaly Analysis	Local, on-box LLM for manual synthesis and junior tech mentoring. Incident Anomaly Analysis correlates message indicators across devices within a shared timeframe.
	Calculated Metrics	Supports Variable Function Chaining to transform raw data into human-readable metrics (e.g., "time ticks" to "hours of uptime").
Resilience	**Utility Grade Metrics**	Automated SAIDI/SAIFI tracking for momentary interruptions and duration hits to ensure NERC CIP compliance.
	Needle-in-a-Haystack Search	Port Hunter (L2/L3) provides instant search by MAC or IP to locate rogue or silent devices in seconds.
	Tiered Workflow Strategy	Optimized for three distinct groups: Operations (daily uptime), Engineering (capacity planning), and C-Suite (capital allocation).
Security	**100% On-Premises**	Zero cloud dependency; designed for strictly air-gapped nuclear and defense-grade environments.
	Inventory & System Bridge	Continuous reconciliation of live network state against official asset databases. Acts as a bridge to push discovered data to external systems like ServiceNow or Sonar.
	Granular Role-Based Access	Supports Active Directory and TACACS authentication with roles that can restrict modification rights to specific equipment types (e.g., MPLS only).