# **Komodo Eye** - Comprehensive Overview

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

## Overview

Komodo Eye holds a unique position among critical infrastructure monitoring platforms by unifying IT and OT visibility into a single, high-fidelity Network Management System (NMS).

As the industry's most comprehensive on-premises observability platform, Komodo Eye delivers a true Single Pane of Glass spanning Layer 0 (physical power/environment) through Layer 5 (application/grid logic).

By natively supporting over 88,000 device models from 8,000 manufacturers, Komodo Eye delivers vendor-specific depth—detecting millisecond-level microflaps or monitoring nuclear fleet endpoints—without the limitations of vendor lock-in.

## Executive Architecture Summary

Komodo Eye is a Network Management System (NMS) designed for critical infrastructure environments where downtime, data leakage, and ambiguity are unacceptable. The platform delivers unified observability across Layer 0 (physical power and environmental systems) through Layer 5 (application and grid logic) within a single operational system.

Architecturally, Komodo Eye ingests atomic telemetry from millions of heterogeneous IT and OT assets, normalizes this data into a common data model, enriches it with geographic and relational context, and retains it in a five-year granular data lake. Edge collectors provide survivability during connectivity loss through disk-backed queues, intelligent rate limiting, and automated replay.

All monitored assets could be classified into three infrastructure classes:

1. Class 1 (Physical Infrastructure),
2. Class 2 (Network & Transport Nodes)
3. Class 3 (Client & Endpoint Devices)

This classification model underpins monitoring scope, role-based access control, alerting behavior, compliance reporting, and reliability analytics such as SAIDI and SAIFI.

Komodo Eye is fully API-driven and integrates bi-directionally with ITSM, SIEM, and automation platforms. It supports Infrastructure-as-Code workflows and is engineered for regulated sectors, including electric utilities, nuclear operations, defense, and public safety—delivering predictable behavior, forensic-grade auditability, and operational resilience at national grid scale.

### Elevator Pitch

**Komodo Eye — Field-Tested at Grid Scale. Air-Gapped by Design. Built for Operator Speed.**

**Operator Experience & Daily Workflow**

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

Key workflow advantages include:

- Instant navigation across millions of devices with no page reloads
- Real-time Normal / Warning / Critical health indicators
- Consistent workflows across sites, technologies, and vendors

This approach minimizes training overhead while maximizing situational awareness for NOC, field, and engineering teams. These workflows are optimized for three primary user personas—Operations, Engineering, and Executive leadership—each of which is described in detail later in this document.

**The Industry Challenge**
Critical-infrastructure teams typically face a trade-off:

- Vendor-specific tools (e.g., Nokia NSP or Cisco Prime) that are "deep but narrow" in data collection. They provide deep insight for one manufacturer but are blind to the rest of the work.
- Enterprise IT tools (e.g., SolarWinds, LogicMonitor, and Nagios) offer broad coverage but cannot explain root-cause behaviors in OT, MPLS, microwave or power-related failure modes.

Komodo Eye replaces fragmented stacks with -a single system of record—combining multi-vendor breadth and multi-layer depth across the full infrastructure.

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

The platform replaces a dozen disparate legacy NMS with a single "source of truth" by monitoring everything from Layer 0 (physical rectifiers, battery plants and RTUs) to Layer 5 (applications delivering data to the grid) with a unified architecture.

This holistic view enables operators to diagnose failures across power, networking, and applications — not just symptoms in isolation.

**Proven Scale & Reliability**
Komodo Eye is field-tested in some of the world's most demanding environments and is designed for "storm scenarios," cascading failures, and sustained high-volume telemetry without degradation.

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

The system is proven to sustain massive EPS volumes during storm events and cascading failures without loss of fidelity.

**Security & Compliance**
As an on-premises, air-gapped platform, the architecture meets stringent requirements, including NERC CIP, high-security nuclear mandates, defense-grade environments, and other regulated sectors. Komodo Eye servers have logged over 900 days of continuous uptime without requiring external connectivity for security updates.

**Encryption & Cryptography**

- All data in transit is protected using TLS
- Sensitive data at rest is encrypted using industry-standard cryptographic controls
- The platform integrates with local certificate authorities and customer-managed key systems

**Authentication & Role-Based Access Control**
Komodo Eye supports:

- Active Directory, TACACS, and local authentication
- Highly granular RBAC policies that can restrict access by device type, function, or action (e.g., MPLS-only modification rights)

Role-specific dashboards are supported for Tier 1/2/3 operators, engineers, and leadership.

**Immutable Audit Trails**
The system maintains immutable audit logs covering:

- Authentication and login activity
- Administrative actions
- Configuration changes
- Data access events

Audit records are tamper-resistant and designed for forensic review and regulatory audits.

**Data Protection & Redaction**
Komodo Eye includes streaming data masking, hashing, tokenization, and redaction policies to protect PII and sensitive operational data. The platform is explicitly designed to prevent the storage of credentials, passwords, or secrets within telemetry streams.

**Software Supply Chain Assurance**
Software supply chain safeguards, including SBOMs, digital signing, and CVE auditing, are detailed in the Security & Compliance section.

Komodo Systems provides:

- Digitally signed software packages
- Software Bills of Materials (SBOM) for all releases
- Regular CVE audits and documented security hardening guides

This supports formal security accreditation, change management, and third-party risk review processes.

**Designed for Air-Gapped & Segmented Environments**
Komodo Eye is specifically engineered for:

- Air-gapped OT networks
- Segmented IT/OT deployments
- DMZ-based architectures

The platform supports proxy and relay configurations, enabling secure telemetry to move across trust boundaries without violating security models.

## 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 based on the frequency and duration of interruptions. Momentary flaps are tracked alongside sustained outages, micro-outages are preserved in the data lake for up to five years and long-term trends support aging-infrastructure analysis and compliance reporting.

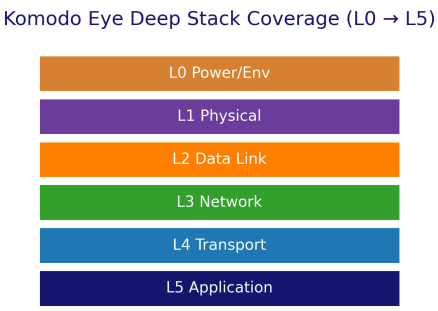
- *Frequency (SAIFI)*: Komodo Eye monitors "momentary interruptions" and instability. If a device "flaps" 35 times in 24 hours, it is flagged as a reliability risk, even if currently reachable.
- *Duration (SAIDI)*: Komodo Eye captures the exact duration of every micro-outage. For example, if a critical link is lost for 10 seconds, the data is saved, 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.** It supports the following device classes to provide consistent visibility, alerting, and role-based operations across IT and OT environments:

- **Class 1 — Physical Infrastructure**
  Physical plant and environmental systems, including battery plants, capacitor banks, circuit breakers, environmental sensors, cybrid dehydrators, rectifiers, and Quantum Key Distribution (QKD) links.
- **Class 2 — Network & Transport Nodes**
  Network and transport infrastructure such as hubs, switches, firewalls, routers, microwave and RF radios, PON hardware, LTE field area networks, and legacy SONET plants.

- **Class 3 — Client & Endpoint Devices**
  Operational and enterprise endpoints, including industrial controllers, protection relays, RTUs, industrial gateways, GPS-supported mobile devices, and enterprise endpoints.




These classes provide a consistent framework for monitoring scope, access control, alerting policies, and reliability analysis across the full Layer 0–Layer 5 stack.

**Atomic Data Collection**
Komodo Eye collects *atomic data*—the smallest meaningful telemetry units—such as 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 supports versioned pipeline management for polling and streaming ingestion (SNMP, Syslog, gRPC, NetFlow, Modbus, TL1, Kafka, REST), edge filtering and noise reduction, parsing, enrichment, calculated variables, and tiered storage and indexed querying.

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.

**Komodo Eye: Resilient Edge Data Architecture**
The Komodo Eye edge data collector serves as a hardened buffer, shielding centralized systems from the volatility of edge environments. It is engineered to maintain data integrity and visibility even during network instability or site isolation.

**Core Survivability Features**

- **Local Persistent Queuing:** Unlike standard collectors that rely on volatile RAM, Komodo Eye spools incoming telemetry directly to **disk-backed storage**. This ensures that if power or connectivity fails, your data survives the outage.
- **Graceful Degradation:** During prolonged isolation, the collector intelligently manages local resources. It prioritizes **critical health metrics** and high-priority alerts while sampling or suppressing high-volume logs, ensuring the most vital insights are preserved.

- **Backpressure & Rate-Limiting:** To prevent a "thundering herd" effect—where a sudden flood of recovered data crashes the upstream server—Komodo Eye utilizes sophisticated flow control. It throttles the replay of historical data to match the destination's ingestion capacity.
- **Automated Data Replay:** Once the uplink is restored, the collector initiates a controlled synchronization. This fills the gaps in your centralized dashboard, providing a **seamless historical record** with no manual intervention required.

**Guaranteed Delivery & Edge Buffering**
Komodo Eye's edge collectors are designed to preserve telemetry integrity during network instability by providing durable, store-and-forward buffering with guaranteed delivery semantics. Edge collectors support store-and-forward buffering with durable queues. Guaranteed delivery semantics monitor for:

- Data gaps
- Duplication
- Timestamp skew

This ensures zero telemetry loss during outages or bandwidth constraints.

**Pipeline Governance & Operations**
Komodo Eye provides enterprise-grade governance over telemetry ingestion pipelines, ensuring controlled change management, repeatability, and auditability across environments.

- **Versioned ingestion pipelines** with dev/test/prod workflows
- Controlled promotion and rollback
- Fully auditable configuration changes

**Pipeline Health & Observability**
To ensure reliable end-to-end telemetry flow, Komodo Eye continuously monitors pipeline health and performance through integrated operational dashboards. Integrated dashboards monitor:

- Collector health
- Queue depths
- Drop rates
- End-to-end latency

**Fleet Management**
Komodo Eye includes centralized fleet management capabilities to maintain configuration consistency, security posture, and operational stability across large-scale distributed deployments. Centralized Fleet Management enables:

- Remote upgrades
- Drift detection
- Automated remediation
- Policy enforcement across thousands of sites

**Analytics, Noise Reduction & Forecasting**
Komodo Eye applies analytics and noise-reduction techniques to telemetry ingestion in order to identify inefficiencies, suppress low-value data, and proactively forecast resource needs. Komodo Eye tracks ingestion metrics by:

- Source
- Protocol
- Driver

This identifies **top talkers**, noisy devices, and inefficient telemetry. Built-in forecasting tools help optimize storage and bandwidth spend proactively.

**Data Intelligence & Correlation**
Komodo Eye transforms raw telemetry into actionable intelligence by normalizing, enriching, and correlating data across vendors, protocols, and infrastructure layers.

- Schema normalization across vendors
- Regex, JSON, XML parsing
- CMDB and GIS enrichment
- Event suppression and deduplication
- Structured events with entity dependencies and symptom-vs-root-cause hints

**Storage, Query & Compliance**
Komodo Eye's data platform is architected for long-term retention, high-performance querying, and regulatory compliance across massive, time-series datasets.

- Hot / warm / cold tiering
- Configurable retention (up to 5 years+)
- Legal hold and granular deletion
- Automated index rollover and compaction
- Sub-second query performance on massive datasets

**Operational Views & Integrations**
Komodo Eye delivers purpose-built operational views and integrates seamlessly with enterprise ITSM, observability, and security tooling to fit into existing workflows.

- NOC-specific dashboards (links, circuits, reachability)
- What-changed analysis with maintenance overlays
- Bi-directional ServiceNow integration
- Outputs to BigPanda, Moogsoft
- SIEM / SOAR / data lake exports (Splunk, Sentinel, Elastic, Snowflake)

**Infrastructure as Code & Automation**
Komodo Eye is **fully API-driven** with native support for **Terraform and Ansible**, enabling repeatable, auditable deployments and operations as code.

**Compliance & Regulatory Alignment**
Komodo Eye is specifically designed for **NERC CIP** environments and has been authorized as a **NERC EACMS cyber asset**, supporting long-term auditability and regulated operations.

**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.

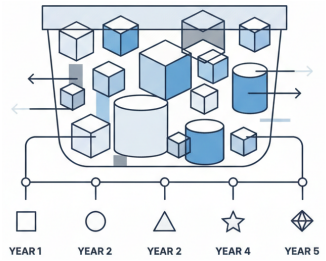
**Interface & Tunnel Monitoring at Scale**
Komodo Eye continuously tracks all interfaces on all devices, physical and logical, such as:

- 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 extended window is critical for Encroachment Analysis—such as tracking a 3-year decline in microwave signal strength caused by gradual tree growth—which would be invisible in short-term datasets.




## 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 & Grid Logic Search**
Komodo Eye can instantly locate any IP address on the network. It indicates whether the device is "online" and identifies exactly which router and physical port that 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 & Physical Topology Search**
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. Komodo Eye includes data masking, tokenization, and redaction policies to protect sensitive information such as PII, credentials, and secrets during ingestion and streaming transforms. The platform is explicitly designed to prevent the storage of passwords, private keys, or shared secrets within the telemetry stream. 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 Komodo AI™

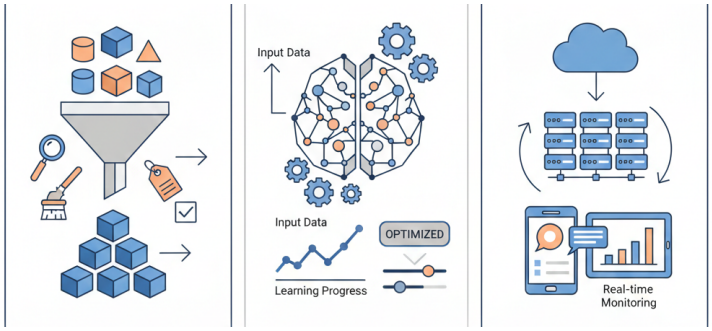
**Komodo AI capabilities are delivered in phased releases. Phase 1 reflects current generally available functionality, while Phases 2 and 3 represent planned roadmap enhancements.**

Overview
Komodo AI™ is an on-premises, air-gapped, retrieval-augmented generation (RAG) system designed to enhance decision-making without compromising security.

**AI Design Principles & Security**

- Zero External Dependencies: Operates 100% on premises with no outbound internet connectivity; updates are performed via secure on-site methods.
- Data Sovereignty: Does not train global models or transfer knowledge between customer environments. Data is strictly siloed into Documentation (Phase 1), Operational Telemetry (Phase 2), and Historical Resolutions (Phase 3).
- Human-in-the-Loop: Designed to support, not replace, human operators. All recommendations require operator review/approval before execution.

**Roadmap**
The first phase will transform how field technicians, network engineers, and operators interact with technical documentation, dramatically reducing Mean Time to Resolution (MTTR) while maintaining the strict security requirements of critical infrastructure environments.




Komodo AI is designed to support human decision-making, not replace it. All insights, analyses, and recommendations are presented for operator review and approval. As the platform matures, customers gain access to probable root-cause analysis based on historical network data to mitigate critical issues.

Komodo AI addresses operational challenges for network teams with an edge-deployed LLM that requires no internet connection. It delivers advanced capabilities while meeting the security requirements of critical infrastructure. Future updates must be done using on-site methods.

Komodo AI enables customers to use an air-gapped LLM as a core capability and a deployment toolkit to provision and configure it at each customer network site. This architecture is designed to enable a scalable, repeatable system in the future. In its initial phase, Komodo AI functions as a documentation-aware AI assistant powered by local knowledge retrieval.

**Security and Deployment Model**
Komodo AI is designed specifically for critical infrastructure environments with stringent security and compliance requirements. The system operates entirely on premises in an air-gapped configuration, with no outbound internet connectivity.

Key security characteristics include:

- No external network dependencies
- Role-based access control (RBAC) aligned to operational roles
- Full audit logging of user interactions and system activity
- Read-only access to operational systems unless explicitly configured otherwise

This model ensures customer data is always fully contained within their operational environment. All AI inference and data processing occur locally within the customer's environment.

**Architecture and Data Boundaries**
Komodo AI does not train global models or transfer learned knowledge across customer environments. It maintains strict separation between different classes of data to ensure clarity, security, and predictable behavior:

- Documentation Knowledge: Customer-provided equipment manuals, SOPs, and technical references used in Phase 1 through retrieval-augmented generation.
- Operational Data: Network telemetry, topology, state, and health data accessed via controlled APIs in Phase 2 and later.
- Historical Resolution Data: Past events, alerts, and corrective actions used in Phase 3 for pattern recognition and predictive analytics.

Data does not leave the customer environment, is not shared across deployments, and is only used within the scope explicitly configured by the customer.

**Phase 1: Local Knowledge Retrieval (RAG LLM)**
This is a document-aware assistant that allows natural-language querying of customer-uploaded equipment manuals. SOPs and technical documentation that are stored locally. Responses are grounded exclusively and traceable to customer-provided documentation.

Examples of queries could include:
- *How to set an IP on a Cybrid Dehydrator*
- *How to test an IP on a Nokia Sar-8 VPRN*
- *What are the expected light levels for Router X port 1/1/1 according to installation specs*

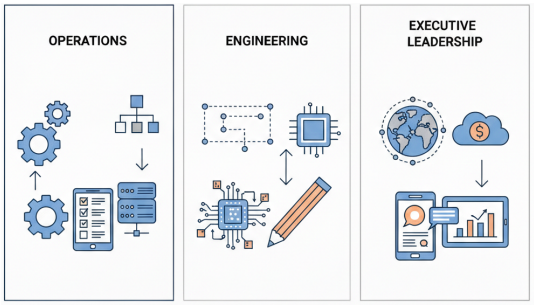
**Phase 2: Database & API Integration**
This update connects the AI layer to the Komodo Eye NMS database via the API, enabling read-only natural-language queries of operational data on network statistics, topology, and health. Responses are aggregations, summaries, and interpretations, not replacements for raw data. And, customers can create on-demand custom reports and shift handoff summaries.

Examples of queries could include:
- *Which site has the lowest availability?*
- *What sites are most vulnerable to interruptions?*
- *What sites do not have redundancy?*
- *What equipment currently in "normal" state was in "error" state in the last 24 hours?*

In this phase, Komodo AI functions as a decision-support tool. While it can aggregate and analyze operational data, all interpretations, reports, and actions remain under direct human control.

**Phase 3: Predictive Analytics**

This update adds probable root-cause analysis to network data to provide mitigation recommendations based on historical resolutions. The result is predictive failure detection—where sufficient historical data exists—enabling operators to address issues before outages occur.




Examples of queries could include:

- *Which devices are likely to fail next?*
- *Why did the "X" substation fail last week?*
- *Where is the network vulnerable?*
- *Which device failures will impact most customers?*

In this phase, predictive insights and root-cause analyses are provided as recommendations. Komodo AI does not autonomously execute network changes or corrective actions. Final decisions always remain with qualified network operators.

## 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.

**Edge-to-Core Scalability**

The system's granularity is best illustrated by its ability to monitor individual circuit breakers in an electrical panel to calculate real-time cost-per-use for a single appliance. This same architecture scales upward to monitor 10 million endpoints across a nuclear fleet, proving that Komodo Eye is effective at any resolution—from a single household breaker to a national power grid.

## 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 maintains **immutable audit trails** for all administrative actions, configuration changes, authentication events, and data access. Audit records cannot be altered and provide full accountability for regulated and forensic environments, supporting NERC CIP, internal compliance, and third-party audits.

## 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.

**Continuous Inventory Reconciliation**

- *Inventory Reconciliation*: The system identifies "uninvited" or rogue 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:

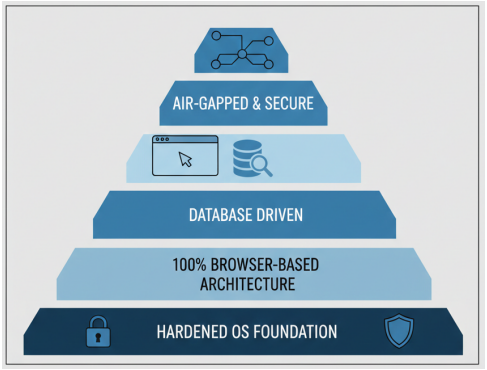
- *API Integration:* Inbound and outbound APIs enable event and alert exchange with platforms such as ServiceNow, PagerDuty, and Sonar.
- *Automation at Scale:* Scheduled and policy-driven actions can be executed across thousands of devices, including firmware updates and enforced credential changes.
- *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.

**Software Supply Chain Assurance**
Komodo Systems provides **digitally signed software packages** and a **Software Bill of Materials (SBOM)** for all releases. Each version is regularly audited for known CVEs, and formal **security hardening guides** are provided to support secure deployment baselines in regulated environments.

## Technical Details

**Robust Software Stack**




- Operating Environment: Built on a hardened Red Hat 9 or Oracle 9 Linux foundation.
- Interface: A 100% browser-based UI powered by Node.js, requiring no local agents or desktop software.
- Data Engine: Utilizes a Postgres database enhanced with Timescale for high-velocity time-series data and PostGIS for sub-meter geographic mapping.
- Concurrency & Speed: Core middleware is engineered in Golang to handle millions of concurrent polls per minute with minimal latency
- High Availability: Supports Active-Active or Active-Passive configurations with automated failover for mission-critical uptime.

**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, all data in transit is protected using TLS, and sensitive data is encrypted at rest using industry-standard cryptographic controls. Komodo Eye integrates with local certificate authorities and on-premises key management systems, enabling customers to apply their own cryptographic policies without cloud dependencies.

**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** | A Layer 2 MAC address physical port locator 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). |