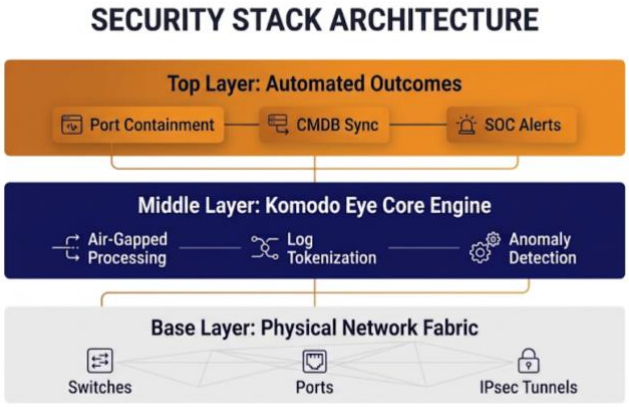
Komodo Eye: Security Architecture & Capabilities Overview

Overview

Komodo Eye strengthens enterprise security posture across critical infrastructure and enterprise networks through deep Layer 2 visibility, automated closed-loop remediation, anomaly detection, and a strictly air-gapped architecture.

By unifying real-time physical layer tracking, autonomous threat response, and advanced behavioral analytics within a strictly self-contained footprint, Komodo Eye dramatically reduces mean time to detect (MTTD) and mean time to remediate (MTTR) across complex environments.

This architecture eliminates blind spots caused by unmanaged or silent hardware, relieves operational strain on security teams through zero-touch containment and self-healing resilience, and guarantees absolute data sovereignty—allowing organizations operating critical infrastructure to maintain uninterrupted uptime, enforce zero-trust posture, and effortlessly satisfy the world's most rigorous regulatory standards.



Feature Summary

1. Device Discovery & Physical Port Tracking

- **Multi-Source Rogue Device Detection:** Discovers unknown, silent, or rogue hardware across the network fabric by correlating known MAC addresses, router IDs, forwarding and routing tables, system logs, and control-plane messages.
- **Layer 2 Physical Port Localization:** Analyzes switch forwarding tables (CAM/FDB) across the infrastructure to trace any connected endpoint—even if firewalled or non-responsive—directly to its physical site, switch, chassis, and port.
- **Continuous CMDB & Asset Reconciliation:** Continuously reconciles real-time network topology against official CMDB asset inventories, generating immediate security alerts whenever unauthorized or unmanaged assets connect.

2. Automated Remediation & Self-Healing

- **Port-Level Rogue Mitigation**: Provides policy-driven response workflows upon detecting an unapproved device:
  - **Automated Containment:** Executes targeted commands directly on the switch fabric to shut down or isolate the offending physical port within seconds.
  - **Assisted/Manual Response:** Automatically generates prioritized incident tickets in ITSM/helpdesk platforms with complete port, site, and switch telemetry for SOC review.
- **Closed-Loop IPsec Tunnel Self-Healing**: Continuously monitors bidirectional traffic across high-density IPsec deployments (tens of thousands of concurrent tunnels). If asymmetric or "hung" states are identified, Komodo Eye triggers autonomous soft bounces to restore encrypted communications without manual SOC or network intervention.

Copyright © Komodo Systems, Inc. 2026

3. Threat Intelligence & Anomaly Detection

- **Behavioral & Semantic Log Analysis:** Employs log tokenization to identify rare syntax deviations across billions of messages in real time, surfacing anomalous events such as unauthorized control writes and spoofed MAC addresses.
- **Unified Firewall & IPS Telemetry:** Ingests live threat intelligence, telemetry, and block rates directly from perimeter and internal firewalls (e.g., Palo Alto Networks, Fortinet) into a single operational pane.

4. Platform Architecture, Cryptography & Compliance

- **100% Air-Gapped & On-Premises Architecture:** Operates entirely within customer-controlled environments without external cloud dependencies or outbound internet access, adhering to stringent data sovereignty and compliance frameworks (including NERC CIP, nuclear, and defense standards).
- **Cryptographic Rigor & Data Protection:** Enforces modern encryption standards—SNMPv3 (AES-256 / SHA-512) and TLS 1.2/1.3 for data in transit—alongside automated PII and credential redaction pipelines.
- **Secure Supply Chain Governance:** Distributed exclusively as digitally signed packages, verified against rigorous CVE audit baselines and delivered with comprehensive Software Bills of Materials (SBOMs).

Conclusion

Komodo Eye delivers a robust defense-in-depth framework tailored for high-stakes environments by bridging the gap between physical network topology and proactive cyber defense.

Through its combination of deterministic Layer 2 tracking, closed-loop automated remediation, and high-fidelity anomaly detection, the platform eliminates visibility gaps and neutralizes threats at machine speed.

Delivered within a provably secure, air-gapped architecture, Komodo Eye ensures mission-critical networks maintain operational resilience, verifiable compliance, and uncompromising control over their critical data.

Copyright © Komodo Systems, Inc. 2026