Security Monitoring

PacketOwl Series NIDS, NSM, and NDR

Network Intrusion Detection & Security Rule-based Threat Analysis
Log Export | North-bound Alerts | Event-Triggered PCAP

PACKETOWL

Suricata-based IDS

100Gbps Performance

NDR Probe

Threat Analysis

Event Logs Export

Selective PCAP Capture

Northbound Alerts

Key Benefits

- ✓ **Stronger Security Posture:** Full-fidelity Suricata rule-based 10-100Gbps NIDS reduces blind spots and speeds up threat detection and action as a key addition in a SoC.
- ✓ **Lower Operational Costs:** Smart NSM with conditional capture and scalable 90-720TB SSD capacity minimizes wasted storage, legal costs, and speeds up investigations.
- ✓ **Compliance & Forensic Readiness:** Accurate timestamping and long-term archiving of log and packet data support incident response, audits, investigations, and regulatory requirements.

- **Unmatched Threat Detection & Zero-Trust Security:** Built on an enhanced Suricata engine, delivering advanced NIDS, NSM, and NDR from 1 to 100Gbps without packet loss. It supports up to 10,000 log events per second, making it ideal for enterprises that demand an uncompromising security posture.
- **Forensic Precision & Long-Term Visibility:** With ultra-fast event-triggered packet capture, indexing, and historical search, PacketOwl empowers proactive threat hunting and incident response. It's scalable, 90TB to 720TB of SSD & SED storage ensures durable data retention for compliance and forensic investigations.
- **Seamless SOC & SIEM Integration & Operational Efficiency:** PacketOwl integrates natively with SIEM and SOC workflows by generating standardized logs and alerts while supporting log compression, log rotation, and custom rules. Pre-processing for threats offloads security tools, increasing their ROI.

Learn More