NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

PACKETOWL

Data Sheet

NEOX**PacketOwl** Security Monitoring Appliance

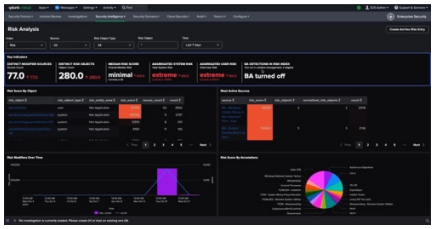
High-Performance, Precise, Suricata IDS-Based Open Network Security Monitoring, Event-Triggered 100Gbps Sustained Full-Packet Capture, Analysis, Logging, and Alerting

PacketOwl enable you to:

- Gain unparallel Suricata-on-Steroids Open IDS-based Network Security Monitoring and Visibility for SecOps
- Create a Zero-Trust defence perimeter by analyzing network traffic for up to 100Gbps sustained throughput without any loss or compromise
- Generate Security Alerts for consumption by well-known SIEM devices and NDR tools
- Generate Log Data and feed into an open eco-system of well-known log facilities
- Capture event-trigerred Packet Data for forensic analysis, evidence, and compliance
- Offload expensive security tools and reduce threats dwell time through high-accuracy signature-based threat hunting and alerting

NEOX Solution

splunk>



The NEOXPacketOwl Network Security Monitoring (NSM) appliance is an advanced, high-performance network packet-data-based security monitoring and delivery platform, designed to identify, analyze, log, and alert for cyber threats in real-time. to ensure supremacy over the adversaries. Powered by NEOX high-performance FPGA-based architecture and Suricata, a robust open-source network threat detection engine, the system leverages deep network insights, Intrusion Detection (IDS), and Network Security Monitoring (NSM) capabilities to safeguard enterprise and service provider networks against a wide array of malicious activities. With its lossless, high-throughput design, the PacketOwl can capture and analyze up to 100Gbps of sustained network traffic, making it the highest-performance Suricata-based open platform in the industry at the time.

Built for scalability and flexibility, this system offers unparalleled visibility into network traffic and provides actionable insights for both threat detection and alerting. It efficiently analyzes network flows to detect known and emerging threats, ensuring comprehensive protection against sophisticated cyberattacks.

With customizable rulesets, real-time alerting, and seamless integration into existing security infrastructure, the Suricata-based Security Threat Detection System is an essential tool for organizations seeking to enhance their cybersecurity posture, reduce response times, and proactively defend against evolving network-based threats. The solution can be a perfect first-line of defense and complementing to Network Detection and Response (NDR) tools.

SURICATA®

Unleashing Full Potential of Suricata

Businesses today face a growing number of cybersecurity challenges, primarily driven by the increasing sophistication and frequency of cyber threats. There is an evolving cyber threat Landscape as cybercriminals continuously develop new tactics, techniques, and procedures, organizations struggle to keep up with emerging threats such as Advanced Persistent Threats (APTs), Zero-Day Vulnerabilities, Ransomware, and other forms of Malware.

Modern businesses operate in increasingly complex network environments, including on-premises infrastructure, cloud, and hybrid models, which create difficulty in securing communications, identifying threats, and ensuring visibility across all traffic. On-top, the sheer volume of data transmitted across networks, combined with the speed at which traffic flows, makes it challenging for traditional security systems to analyze and detect

potential threats in real-time without causing performance bottlenecks. Many businesses lack effective tools for monitoring network traffic in real-time or for correlating events across disparate security solutions. This lack of visibility can delay the detection of intrusions and allow attacks to escalate undetected. Organizations often adopt a reactive approach to cybersecurity, responding to incidents after they occur rather than proactively identifying and mitigating threats before they cause damage. Suricata addresses these challenges by providing businesses with a high-performance, scalable security solution capable of real-time network traffic analysis and comprehensive threat detection.

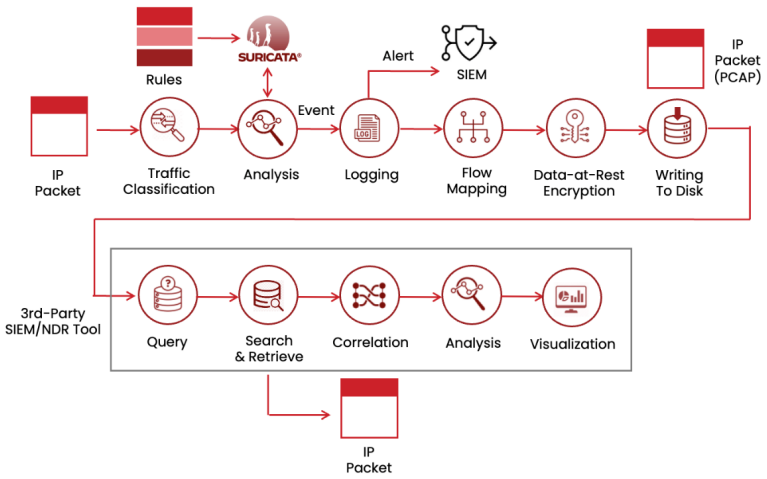


Diagram-1: Operation of PacketOwl NSM and 3rd-Party SIEM and/or NDR Tool

Enterprise-Grade Open Network Security Monitoring

Comprehensive Threat Detection based on NEOXPacketOwl NSM and Open Suricata capabilities allow businesses to detect a wide range of known and unknown threats, including advanced malware, intrusion attempts, and suspicious activity, ensuring comprehensive protection. PacketOwl can capture and analyze network traffic in real time, providing immediate detection of threats and reducing the time to respond. This helps organizations shift from a reactive to a proactive security posture. PacketOwl scales efficiently to meet the needs of businesses of all sizes and across diverse environments.

PacketOwl integrates effortlessly into existing security frameworks, whether deployed on-premises, in the cloud, or within hybrid environments. It serves as a critical element and the first line of defense, positioned after the perimeter firewall, as part of a Zero-Trust security strategy. PacketOwl effectively detects most signature-based network attacks. For new or unconventional threats, additional NDR tools can be added as an inner layer of defense, if required. Additionally, PacketOwl can forward logs to central log management systems and send security alerts to Security Information and Event Management (SIEM) platforms like Splunk.

With PacketOwl businesses gain deep visibility into network traffic and protocols, enabling them to spot anomalies and vulnerabilities across their networks with greater accuracy and confidence. It helps businesses not only detect and respond to threats faster but also build a more resilient and secure network infrastructure.

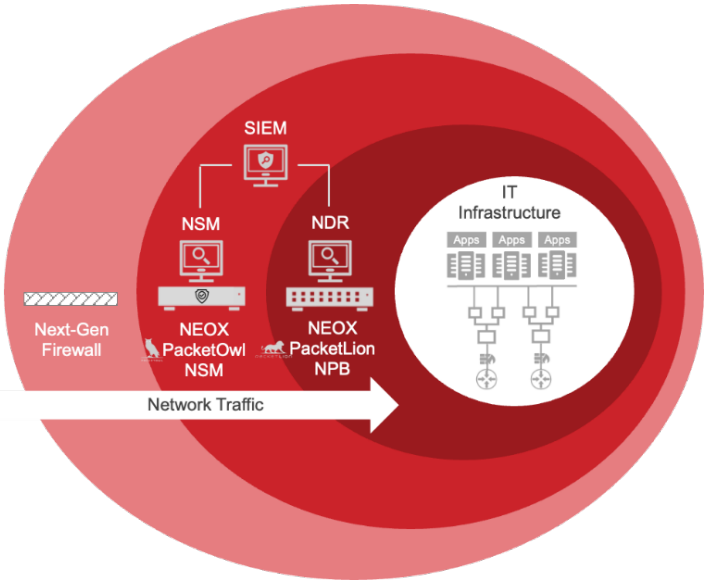


Diagram-2: PacketOwl NSM Deployment Strategy

Key Benefits

Optimized Threat Analysis for High Traffic Load

NEOXPacketOwl NSM is designed to handle high-traffic volumes where other systems may struggle or chock. With a speed of 100Gbps, PacketOwl captures and analyzes every packet using a "Suricata-on-Steroids" optimized technology. IT users can modify the signatures and the rules anytime for total control over their policies and what they consider important. Suricata signature-based rules are patterns or signatures used by Suricata, to detect and identify known network-based threats. These rules provide a structured way and predefined criteria that describe malicious activities or attack patterns, allowing Suricata to match network traffic against these signatures to flag potential threats. PacketOwl NSM filters out only the flows and transactions that that match specific events or incidents, storing the log and packet data associated with those flows for forensic analysis, historical records, and compliance. Simultaneously, it generates alerts, which can be sent to a SIEM (such as Splunk) or other monitoring platforms.

Out-of-Box Interoperability for Sharing Log Data

There is the need for log retention and preservation. Logs should be stored securely and in accordance with standards ensuring that they are available for review and analysis during cybersecurity investigations. This preservation is critical for auditing, compliance, and post-incident assessments. NEOX PacketOwl NSM fosters an open ecosystem with seamless out-of-the-box integration with standard logging facilities, such as Syslog servers and other widely used systems. These logging facilities collect, store, and manage log data, enabling security teams in a Security Operations Center (SOC) to monitor behaviors, detect anomalies, and investigate incidents. The integration plays a vital role in maintaining the health, security, and performance of IT infrastructure as centralization allows cybersecurity teams to analyze and cross-reference data from various sources to detect threats early.

Zero-Trust Forwarding of Alerts to SIEM Platforms

Logs generated by NEOXPacketOwl NSM are typically also forwarded to SIEM systems, such as Splunk or other third-party tools. These systems collect, aggregate, and analyze logs to detect patterns and anomalies. Logs can be further shared with trusted external partners and industry stakeholders to help improve the overall cybersecurity posture. The NEOX PacketOwl NSM is designed to trigger real-time alerts whenever suspicious or malicious activity is detected on the network. These alerts are then forwarded to relevant stakeholders, such as the SOC, the CISO, or Incident Response (IR) teams. For instance, a failed login attempt followed by successful access might raise an alert, or unusual outbound network traffic might trigger an alert for a possible data exfiltration attempt. In line with Zero Trust principles, every event that deviates from the normal baseline is logged and flagged for review. These alerts are integrated into a broader incident response framework that ensures that teams act swiftly to investigate, contain, and mitigate security threats.

Forensic Analysis for Incident Detection and Response

The logging mechanism is crucial for real-time monitoring and detection of cyber incidents. Logs and associated captured packet data (PCAP) by NEOXPacketOwl NSM provide key evidence needed to identify threats like malware infections, privilege escalation attempts, or unauthorized access to sensitive data. Logs and packets allow Security Operations (SecOps) teams to quickly determine the scope of a security incident. NEOXPacketOwl NSM is an all-in-one solution that offers a high-speed IDS built on open standards that generates logs and alerts, while capturing and storing selective packets in PCAP format for each interaction related to an incident. Packets Never Lie. In addition to the log data, this PCAP data provides all necessary information for forensic investigations and evidence gathering. It proves especially valuable in cases of cybercrimes targeting businesses, financial institutions, government entities, and critical infrastructure. For example, if there is a breach, the data will show which systems were accessed, by whom, and how the attack spread across the network. IR teams can use log and PCAP packet data to perform forensic investigations after an attack, identifying the entry points, methods, and affected assets. They can also use it to track the timeline of the attack and assess the overall damage.

Audit Trail for Industry and Government Compliance

The PacketOwl NSM is capable of recording every flow and transaction on the network at 100Gbps speed. This makes enterprises, service providers, and public organizations comply with Executive Order (EO) 14028 and M-21-30, which focuses on improving the US federal government's investigative and remediation capabilities related to cybersecurity incidents. Most organizations are also required to maintain an audit trail of activities, which includes not only security incidents but also the actions taken in response to them. These audit trails are used to demonstrate compliance with industry and federal cybersecurity regulations The audit trail includes logs of actions taken during a cyber incident (e.g., which users accessed which systems and when), decisions made during the incident response process, and whether security controls were followed as intended. This comprehensive record-keeping is essential for future auditing, ensuring organizations adhere to cybersecurity best practices, and enabling better decision-making in subsequent responses to incidents.

Deployment

The NEOXPacketOwl Network Security Monitoring appliance is an ideal solution for enterprises, data centers, cloud environments, service providers, and government agencies, capable of scanning and analyzing both east-west and north-south network traffic at speeds up to 100Gbps. The on-premises solution is a 2RU rack-mountable unit with front-to-back airflow and features 2 x 100Gbps QSFP28 ports along with other connectivity options such as 10, 25, or 40Gbps options, that support SR1.2 (BiDi), SR4, LR4, and ER4 optics.

While NEOXPacketOwl NSM operates as a fully autonomous appliance that can generate logs and alerts to SIEM systems (such as Splunk or any third-party SIEM), it can also work alongside an NDR tool. In such cases, a NEOXPacketLion Packet Broker or NEOX-PacketWolf Packet Processing appliance can forward real-time network traffic to the NDR tools.

A scalable data center security visibility design begins by deploying network TAPs at key points to mirror network traffic (see NEOX Network Traffic Tapping solutions for various TAP options). While TAPs can feed traffic directly to the PacketOwl NSM appliance, a more efficient approach for managing the network is to aggregate the TAPs using a Network Packet Broker (NPB). The NPB can consolidate, filter, and manipulate traffic, directing it to multiple destinations like the PacketOwl NSM appliance and NDR tools (see NEOX Network Traffic Brokering solutions for a range of NPB options).

US Government Executive Order EO 14028 encourages federal agencies to enhance their ability to detect and respond to cyber threats by implementing tools for continuous monitoring of their IT environments. The goal is to capture comprehensive logs across all endpoints, networks, and systems. This involves setting up centralized logging systems (e.g., SIEM) that aggregate logs from various security tools and network devices, such as firewalls, IDS, and endpoint detection and response (EDR) platforms. Logs captured include system events, network traffic data, application logs, security alerts, and other vital metrics.

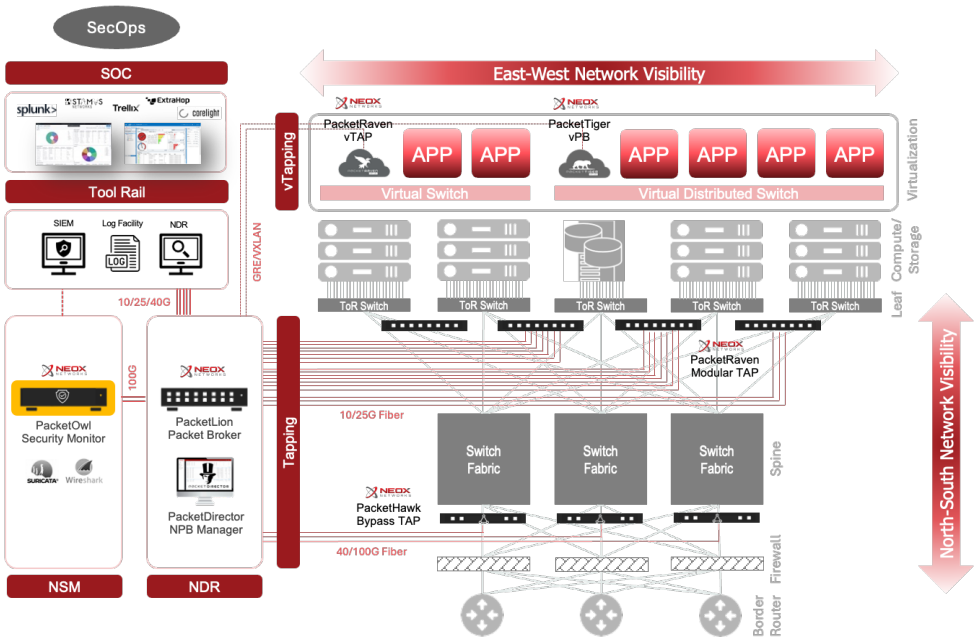


Diagram-3: NEOX PacketOwl NSM Deployment in the Data Center

The implementation of Zero Trust Architecture (ZTA), as detailed in M-21-30, adds another layer to this logging mechanism. Since Zero Trust relies on treating every access attempt as potentially untrusted, all access requests, including user authentication, device access, and network activity, are logged. Event correlation combines data from various logs to detect a coherent picture of a potential security incident. For instance, if logs from an endpoint detection system show abnormal behavior on a device and logs from a network firewall show unusual traffic patterns, these events might be correlated to indicate a breach.

For cloud deployments, the NEOXPacketOwlVirtual offers virtually unlimited performance, depending on the cloud instance provisioned. The PacketOwlVirtual can forward the alerts to a cloud-native or on-premises SIEM, while storing the log and packet data locally in the cloud within the organizations Virtual Private Cloud (VPC). NEOX solution supports all major public clouds including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

The cloud deployment begins by extracting and feeding untrusted network traffic streams that need to be analyzed. This can be easily achieved by deploying Virtual TAPs (vTAP) or using VPC traffic mirroring (see NEOX Network Traffic Tapping solutions for various TAP options).

While vTAPs can directly send traffic to the PacketOwlVirtual NSM (vNSM) appliance, a more efficient and cost-effective approach for managing the network is to aggregate the vTAPs through a Virtual Network Packet Broker (vPB). The vPB can consolidate, filter, and manipulate traffic, directing it to multiple destinations, including the PacketOwlVirtual NSM and NDR tools (see NEOX Network Traffic Brokering solutions for a range of vPB options).

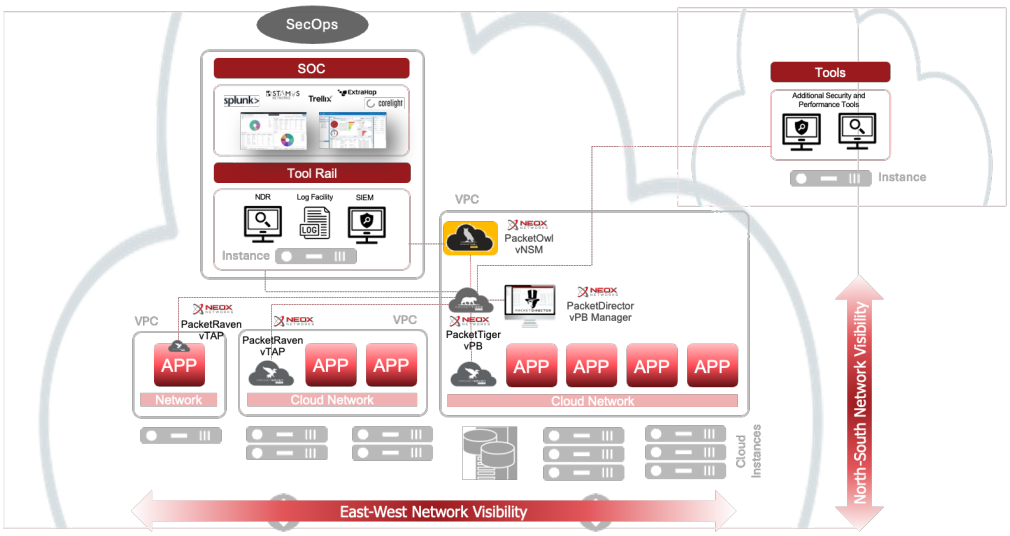


Diagram-4: NEOX PacketOwlVirtual NSM Deployment in the Cloud