Solution Brief

Intelligent Traffic Access and Aggregation for Advanced Network Threat Detection and Response

NEOX Networks and Stamus Networks Joint Solution Brief

In today's complex threat landscape, organizations need comprehensive network visibility and advanced threat detection capabilities to protect their critical assets.

This solution brief outlines how the integration of NEOX Networks' Network Visibility Platform components with Stamus Networks' Clear NDR™ creates a powerful end-to-end solution for network visibility, threat detection, and response.

Solution Highlights

Complete Network Visibility - Access to 100% of network traffic at speeds up to 400G

Optimized Traffic Processing - Intelligent packet brokering for enhanced monitoring efficiency

Advanced Threat Detection - Multi-layered detection technologies with transparent results

Actionable Intelligence - Evidence-based events with detailed context for faster response

Seamless Scalability - From small deployments to enterprise-wide implementation

THE CHALLENGES: BLIND SPOTS AND ADVANCED THREATS

Modern enterprise networks face multiple challenges, with 40% of data breaches in 2024 involving data stored across multiple environments. These challenges include expanding network perimeters due to cloud adoption and remote work, growing volumes of encrypted traffic creating security blind spots, sophisticated attackers evading traditional controls, management complexity from disconnected security tools, alert fatigue leading to missed critical threats, and limited security resources requiring more automated solutions.

Organizations need comprehensive visibility into all network traffic combined with intelligent analysis to detect and respond to threats before they cause harm.

INTEGRATED NETWORK VISIBILITY AND CLEAR NDR

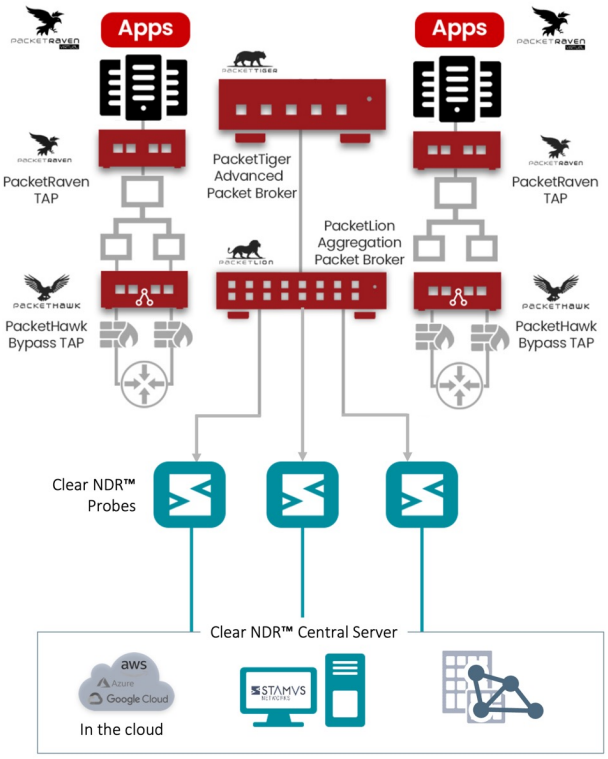

Figure 1. Solution architecture overview

The integration of NEOX Network Visibility Platform components with Stamus Networks' Clear NDR creates a powerful end-to-end network security solution. The components work together to provide complete visibility, intelligent traffic optimization, and advanced threat detection.

Network Visibility from NEOX Networks

Network TAPs

NEOX PacketRaven, PacketHawk, and PacketRoo Series Network TAPs provide secure, passive, fail-safe inline and out-of-band access to network traffic at various speeds (1G to 400G) and media types. They create exact copies of network traffic without affecting network performance or introducing points of failure.

TAPs are the foundation of network visibility, ensuring security tools have access to 100% of traffic, including the critical first packets where many attacks begin.

Network Packet Brokers

NEOX PacketWolf, PacketLion, and PacketTiger Series Network Packet Brokers aggregate, filter, and optimize traffic from multiple Network TAPs before delivering it to monitoring and security tools. Key capabilities include:

- Traffic aggregation from multiple sources
- Intelligent filtering to focus on relevant traffic
- Packet deduplication to eliminate redundant data
- Header stripping to reduce processing overhead
- Load balancing to optimize tool utilization
- Timestamping for accurate forensic analysis
- VLAN tagging to maintain traffic source information

Clear NDR™ from Stamus Networks

Clear NDR is an open and transparent Network Detection and Response that delivers:

Clear Visibility - Monitor activities across your entire attack surface

Clear Detection - Multi-layer, transparent detections you can understand

Clear Evidence - Everything you need to quickly resolve the incident

Clear Response - The confidence you need to automate your response

Clear NDR Probes

Clear NDR Probes inspect and analyze all network traffic to perform real-time threat detection, enrich the resulting events with extensive metadata, and capture network protocol transactions. The probe delivers all this data to the Clear NDR Central Server for additional analytics, processing and another layer of threat detection.

Clear NDR Central Server

Clear NDR Central Server provides the centralized management of the probes, third party threat intelligence and rulesets, consolidated event storage and a central integration point. It includes an additional layer of machine learning and algorithmic threat detection, along with automated event triage – enabled by tagging and classification. Finally, the Clear NDR Central Server provides a powerful threat hunting and incident investigation user interface.

SOLUTION BENEFITS

- **Enhanced Visibility** – with intelligent traffic optimization delivered by NEOX Network Packet Brokers, security teams can cost-effectively use Clear NDR to monitor traffic high-performance environments such as data centers for north-south and east-west traffic.
- **Reduce Costs** – with intelligent traffic aggregation provided by NEOX Network Packet Brokers, organizations can deploy fewer Clear NDR Probes for comprehensive visibility into network activity, helping identify hidden threats and vulnerabilities.
- **Improved Threat Detection** – Clear NDR's advanced threat detection capabilities, fed by optimized traffic from multiple sources through the NEOX Networks TAPs and Network Packet Brokers, ensure a high level of accuracy in identifying malicious activity, reducing false positives, and enabling faster response to genuine threats.
- **Increased Scalability** – The joint solution can handle large volumes of network traffic, making it suitable for organizations of all sizes and ensuring effective threat detection even in complex network environments.
    - Support for networks from 1G to 400G
    - Distributed deployment options for multiple locations
    - Centralized management and analysis
    - Cloud, on-premises, and hybrid deployment options
- **Operational Efficiency** – The integration between the NEOX Networks Visibility Platform components and Clear NDR streamlines security operations, reducing the complexity of managing multiple security tools and improving the efficiency of threat response. Security teams benefit from:
    - Transparent detection logic that builds trust and understanding
    - Evidence-based events that reduce investigation time
    - Seamless integration with existing security infrastructure
- **Detection Sensitivity** – Uncover even the weakest attack signals with Clear NDR, you can leverage integrated detection algorithms, third-party threat intelligence and rulesets; and easily transform a threat hunt into custom detection logic.
- **Eliminate Alert Fatigue** - with the high-fidelity Declarations of Compromise™ and Declarations of Policy Violations™, you can be confident they are investigating real security events.
- **Accelerate Incident Response** - with extensive integrations into EDR, NAC, IPAM, SOAR, and other systems, Clear NDR can automatically trigger an Incident Response.

SUMMARY

The integration of NEOX Networks' Network Visibility Platform with Stamus Networks' Clear NDR provides organizations with a comprehensive solution for network visibility and advanced threat detection. By eliminating blind spots and providing context-rich, evidence-based detections, security teams can identify and respond to threats faster and more effectively.

Organizations benefit from:

- Complete network visibility without blind spots
- Optimized traffic delivery to security tools
- Advanced multi-layered threat detection
- Faster, more accurate response to threats
- Reduced operational complexity and costs

For more information on how this integrated solution can enhance your organization's security posture, contact NEOX Networks and Stamus Networks today.

ABOUT NEOX NETWORKS

NEOX Networks provides Next-Generation Network Visibility for IT & OT Observability and Security. The result is strengthened cybersecurity, hybrid-cloud application observability, and business continuity, by integrating the network intelligence and real-time data-in-motion.

Visit the NEOX Networks website: www.neoxnetworks.com

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

 SN-JSB-NEOX-052025-1