Solution Brief

Real-Time Guided Threat Hunting with

Clear Network Detection and Response

Challenge

Emerging cyber threats are becoming increasingly sophisticated and pose significant risks to enterprises and businesses. Ransomware attacks continue to evolve, with cybercriminals using advanced tactics like double extortion, where they not only encrypt data but also threaten to release it publicly unless a ransom is paid. Additionally, the rise of supply chain attacks targets vulnerabilities in third-party vendors, compromising the security of interconnected systems. Businesses are also facing a surge in AI-driven cyber threats, where attackers use machine learning to automate and personalize attacks, making them more effective and harder to detect. As enterprises embrace digital transformation, the expanding attack surface, especially with remote work and cloud adoption, increases the potential for data breaches, phishing, and insider threats. In this evolving landscape, organizations must remain vigilant, continuously adapt their zero-trust security strategies, and invest in cutting-edge technologies to mitigate these emerging risks.

Clear Network Detection and Response Solution

NEOX Networks' and Stamus Networks' Clear NDR™ solution delivers actionable insights with guided threat hunting and automated alert triage, including high-fidelity Declarations of Compromise™ (DoC) and Declarations of Policy Violations™ (DoPV). Clear NDR is a proactive cybersecurity defense solution designed to detect, analyze, and respond to emerging threats within an organization's network. It uses advanced analytics, machine learning, and behavioral analysis to monitor network traffic, detect threats and unauthorized activity in real-time. Unlike traditional security measures, which focus primarily on prevention, Clear NDR emphasizes detecting malicious activity that has already bypassed preventive defenses, such as IDS, firewalls and antivirus systems. The result is a comprehensive NDR solution that enables faster, more effective threat detection and response. By harnessing real-time insights based on network activity, Clear NDR reveals serious and imminent threats to your most valuable assets—empowering your security team to respond swiftly and effectively.

Business Benefits

- Increased Business Continuity due to proactive threat detection and mitigation.
- Assured Customer Experience and retention due to customer application and data protection.
- Reduced Operational and Legal Costs due to timely threat and breach containment.

Technical Benefits

- Multi-dimensional threat detection and mitigation using Clear NDR technology.
- Best of both, Log and Packet Data for high-level alerting and deeper forensics analysis.
- Integration into existing Security Eco-System such as SIEM and other SOC workflows.

Solution Construct

The 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. **Clear NDR** addresses these challenges by providing businesses with a high-performance, scalable security solution capable of real-time network traffic analysis and comprehensive threat detection and response to safeguard against a wide range of known and unknown threats, including advanced malware, intrusion attempts, and suspicious activity, ensuring comprehensive protection. The solution helps SecOps team become more efficient than ever, allowing them to focus on strategic initiatives while proactively defending against threats. With multi-layered transparent detection and response technologies – supported by extensive metadata and evidence, it delivers detection you can trust with results you can explain.

The **Clear NDR** solution is a combination of the following best-of-the-breed technologies and components that come together from the two partners to deliver a cohesive, higher value solution for IT SecOps:

A. NEOX PacketOwl Clear NDR Probe, a FPGA-based high-performance appliance along with packet capture (PCAP) capabilities, and integrated Stamus Intelligent Event-Processing algorithms with event logs – to deliver unmatched 100Gbps throughput.

B. Stamus Clear NDR Central Server, for central telemetry correlation and visualization of the key Security Analytics for actionable information for the Security Operations Center (SOC) consumption. Clear NDR offers integration with third-party tools to launch automated response via web-hooks.

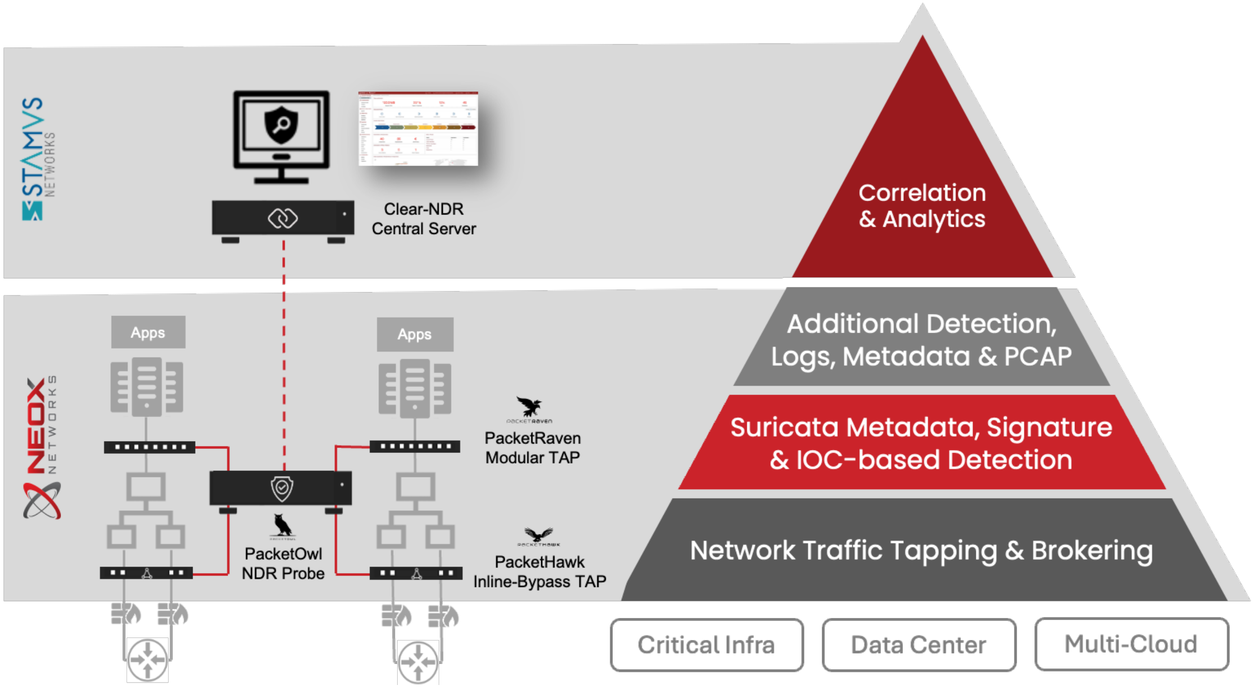
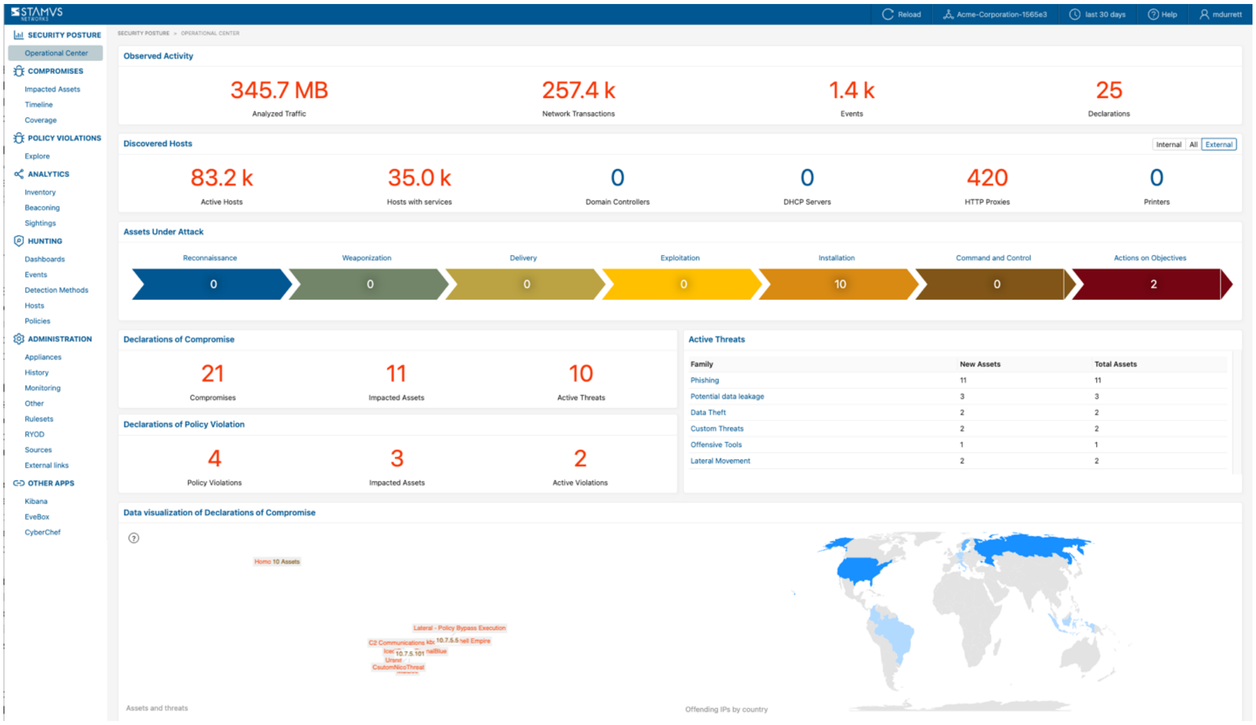


Diagram-1: NEOX and Stamus Clear NDR Solution

The **Clear NDR** solution consists of NEOX Network Visibility Platform foundation extracting the real-time packet data for real-time threat hunting. The above foundation layer may include a two or three-tier architecture comprising of Network Tapping, Network Packet Brokering (optional), and Network Security Processing. The last includes the NEOX PacketOwl Clear NDR Probe, an advanced, high-performance security processing and delivery appliance, designed to identify, analyze, log, and alert for cyberthreats in real-time to ensure supremacy over the adversaries. Powered by NEOX high-performance FPGA-based architecture, the system leverages deep network insights 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 NDR probe in the industry at the time.

The metadata generated by NEOX PacketOwl Clear NDR Probe(s) is fed into Stamus Clear NDR Central Server, which empowers defenders to build a truly autonomous Security Operations Center (SOC) – with AI/ML-powered threat detection and automated response fueled by the richest log and packet data-based network telemetry available through NEOX. Stamus Clear NDR Central Server provides the centralized management and correlation for the data received from NEOX PacketOwl probes, acting as 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 and analytics console.



Family	New Assets	Total Assets
Phishing	11	11
Potential data leakage	3	3
Data Theft	2	2
Custom Threats	2	2
Offensive Tools	1	1
Lateral Movement	2	2

Diagram-2: Clear NDR Analytics Console

Key Benefits

1. **Real-Time Threat Detection and Mitigation:** The Clear NDR solution flags all threats and unauthorized activity, classifying the most serious and imminent for automated response and/or notification. These high-fidelity DoC and DoPV events are shared with SOC analysts, security executives, and IR teams and can be used to trigger an automated response from another system such as EDR, SOAR, or firewall. In addition, they can be forwarded to external partners to enhance cybersecurity collaboration. Finally, all suspicious activity and individual threat detection methods are logged, enabling swift, informed containment and response. By combining continuous network monitoring, advanced analytics, and automated responses, Clear NDR enhances an organization's ability to detect and respond to a wide range of cyber threats—especially the sophisticated and evasive ones. This makes Clear NDR solution an essential tool for businesses aiming to address the evolving threat landscape and strengthen their overall cybersecurity posture.

2. **Seamless Event Logging and Retention:** Designed for interoperability, the solution integrates with Syslog and other logging systems, enabling SOC teams to monitor, analyze, and respond to threats and unauthorized activity across the network. Centralized logging supports incident response, auditing, compliance, and faster threat detection. And with conditional logging and conditional packet capture, all relevant evidence is preserved using less than 10% of the resources required for full-time logging. Its detailed audit trail captures user actions, host activity, security-related events, and policy violations to ensure transparency, accountability, and preparedness for future threats.

3. **Ultra-Fast Forensics and Incident Response:** In addition to logs, Clear NDR probe (PacketOwl) stores relevant packet capture data (PCAP), giving IR teams the evidence needed to investigate breaches, trace attacker behavior, and assess damage. This data is critical in identifying threat origins, lateral movement, and attack timelines. It delivers real-time, 100Gbps packet capture and analysis using an optimized network security deep packet inspection engine. It enables full control over the threat detection

algorithms, signatures, and threat intelligence, filtering only relevant traffic for data retention and forensic analysis. Alerts are generated instantly and forwarded to SIEM platforms like Splunk for further investigation.

4. **Monitor Attack Surface and Vulnerabilities:** The Clear NDR solution excels at identifying a variety of attack types, including ransomware, malware, data exfiltration, supply chain attacks, phishing attacks, and more. For example, by using multiple detection mechanisms, Clear NDR can help detect early-stage attacks where adversaries infiltrate trusted partners to access an organization's network and allows organizations to quickly contain the attack and limit the damage.

5. **AI-Driven Intelligence and Insights:** Clear NDR leverages multiple detection mechanisms, including machine learning (ML), as well as advanced heuristics, signatures, and IoC matching, e continuously examinine network traffic, refining its ability to spot threats. This is particularly useful against AI-driven cyberattacks, as the system can adapt to new tactics, techniques, and procedures (TTPs) used by attackers, identifying previously unknown or sophisticated threats. As organizations shift to cloud environments and adopt remote work, the attack surface grows, making it harder to monitor. The solution provides continuous visibility across both on-premises and cloud environments, offering real-time monitoring for unauthorized access, suspicious lateral movement, and data exfiltration attempts, which are common in cloud-based or hybrid infrastructures.

Solution Deployment Best Practices

On-premises deployments, such as those in Enterprise or Service Provider Data Centers, begin with the installation of network intelligence devices to establish a network visibility layer. This includes the NEOX Network TAPs strategically placed at key network points to monitor both north-south and east-west traffic routes. The traffic from these TAPs is typically aggregated through one of the NEOX Network Packet Brokers, which then forwards the data to t NEOX PacketOwl Clear NDR Probe. This feeds into the Stamus Clear NDR Central Server for threat correlation and analysis.

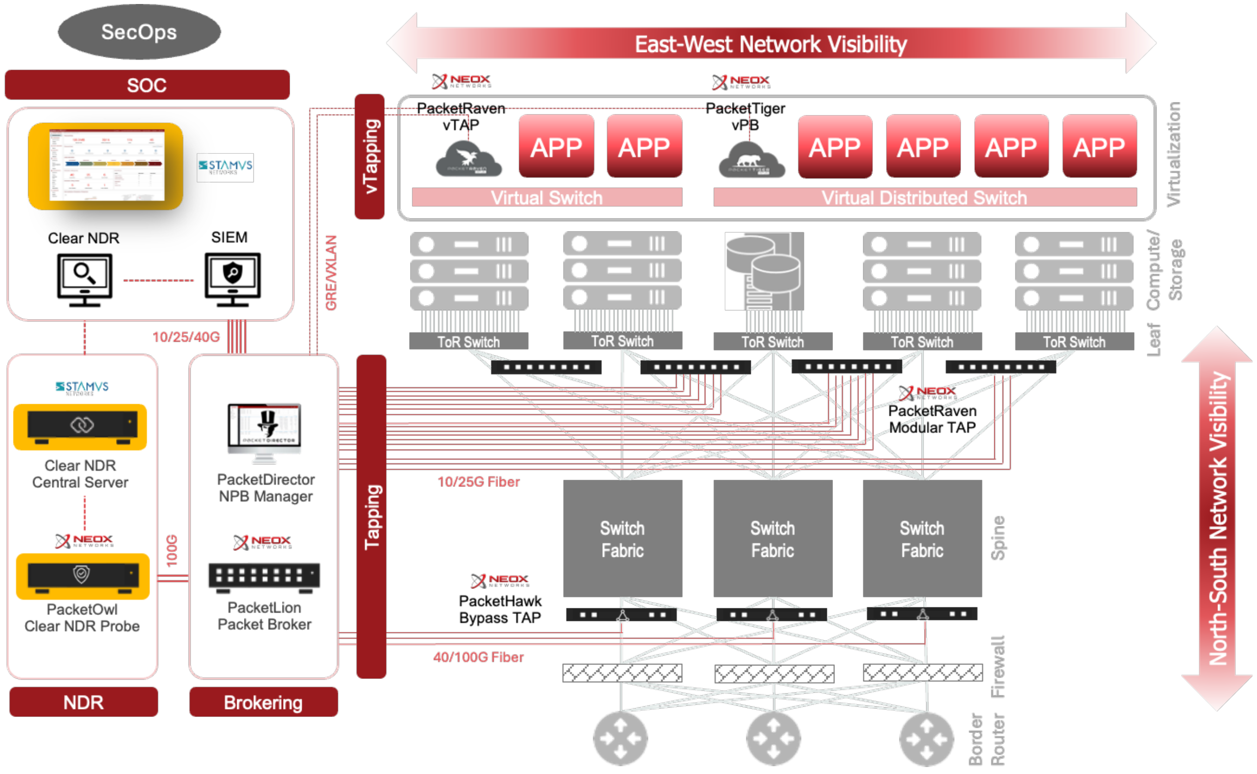


Diagram-3: Data Center Deployment of Clear NDR

Cloud deployments, whether on AWS, Azure, or Google Cloud, follow a similar approach. Network intelligence is collected from within the customer's Virtual Private Clouds (VPCs) via a cloud Traffic Mirroring service or by deploying NEOX PacketRavenVirtual TAPs (the preferred method). It is strongly recommended to use a NEOX PacketTigerVirtual Packet Broker to aggregate and process the data stream to multiple destinations, which significantly reduces costs and simplifies management—avoiding the need to pay per data stream to the cloud provider. The PacketTigerVirtual then forwards the data stream to a NEOX PacketOwlVirtual Clear NDR Probes or directly to the Stamus Clear NDR Central Server for correlation and analysis.

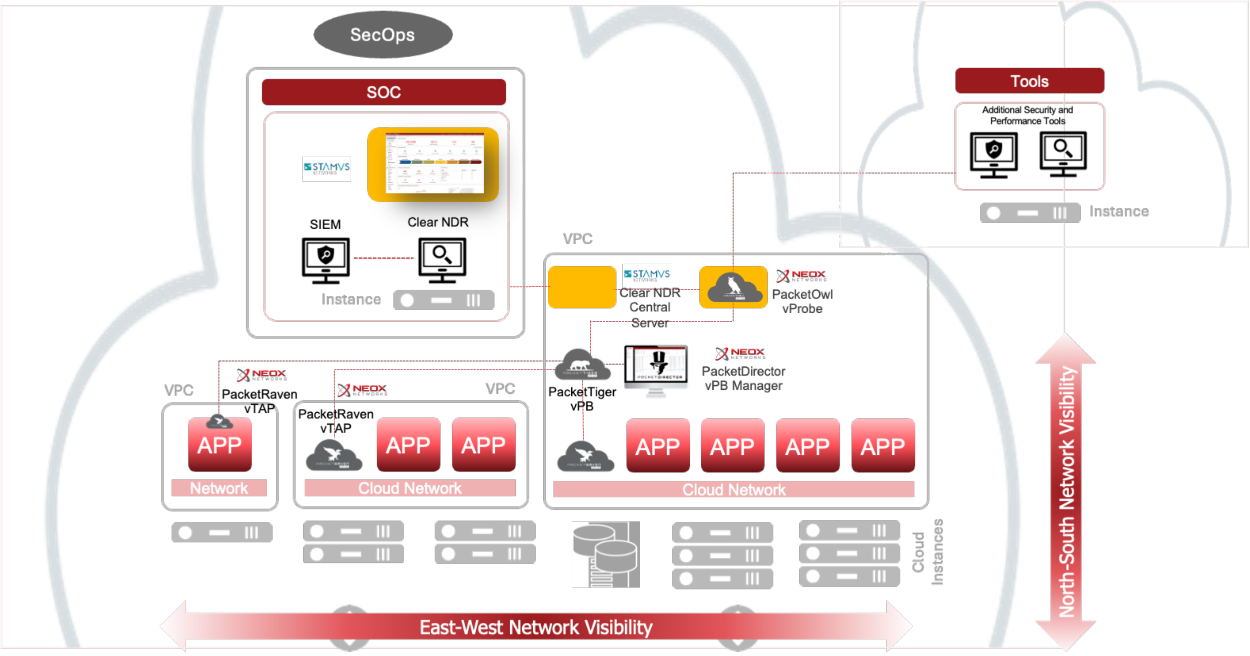


Diagram-4: Cloud Deployment of Clear NDR

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. Learn more at 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. Learn more at stamus-networks.com