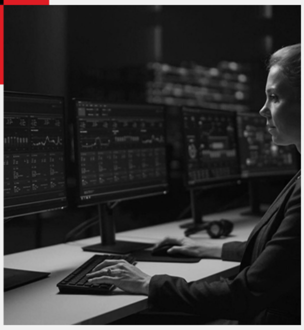
NEOX NETWORKS corelight

Solution Brief

Proactive Threat Detection and Mitigation based on **Network Detection and Response**

Driving Meaningful Network Intelligence from Next-Generation Network Visibility

Key **Benefits**



1 Strengthen cybersecurity posture through fully integrated network visibility and Intelligence for faster threat hunting, employing the latest NDR technologies and high-speed lossless network tapping and brokering

2 Secure IT and OT environments. Detect attacks, breaches, and malicious activity across physical, hybrid-cloud, and multi -cloud environments.

3 Increase SOC performance metrics and cut through the backlog with aggregated, prioritized alerts mapped to the MITRE ATT&CK® framework. Quickly access correlated evidence with PCAP data, driving faster decisions and response time

4 Respond faster to incidents through deeper network packet data capture and forensics at your fingertips with ultra-fast lookup and analysis tools.

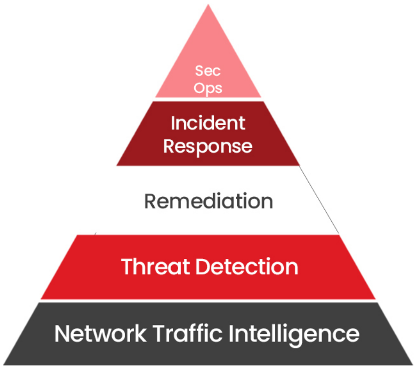
5 Fast and easy to deploy NDR solution. Field-proven interoperability with standard interfaces and open APIs makes deployment and bring-up easy and fast.

Challenge

Cyberattacks continue to increase, and with the global geopolitical landscape, more digitization, and domestic economic challenges, there is no chance of cybercrimes or cybercriminals going down any sooner. Enterprises and industrial infrastructure are the prime targets for the attackers. Enterprise data centers and clouds host highly desirable customer, financial, and other private data that can provide valuable insights and could be sold on the dark web to the highest-paying local or foreign entities. The industrial and manufacturing sites and infrastructure are the prime targets for the adversaries for causing economic and other types of harm. So, protecting IT and OT infrastructure today is the top priority for the CISO, security architects, and operations (SecOps) teams.

What is NDR

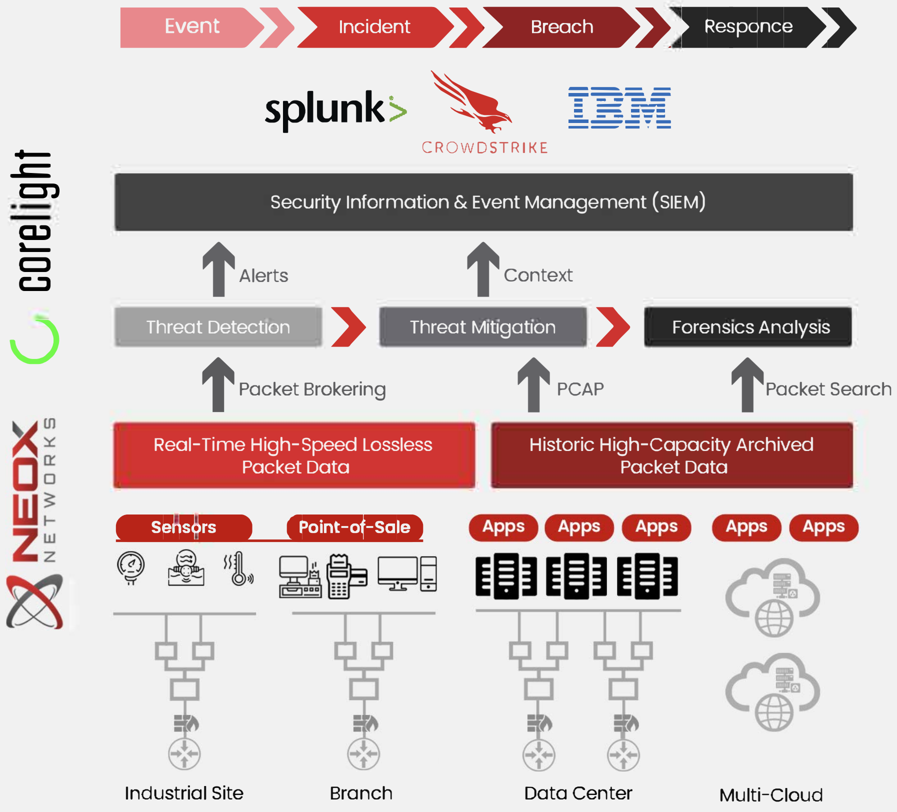
A resourceful and persistent attacker would eventually get in. The favorite infiltration point for the attackers is the network. Hence, most industrial sites and some data centers are completely cut off from outside network or Internet connectivity. In those cases, attackers find some backdoor mechanisms. But in the cloud, and in most cases where businesses run digital or SaaS services or applications for customer access, there is always network connectivity and hence the prime targets for the attacks. It is a common misconception that traditional network security mechanisms such as Firewalls or Intrusion Detection and Prevention Solutions (ID/IPS) are good enough to safeguard the network. Not at all. Traditional signature-based detection and prevention measures are only able to catch the attacks for which they are programmed.



But once an attacker can dodge those and get in undetected, the whole network and hence the attached assets, such as servers, applications, and database, are available to them. Furthermore, virtualization, such as VM and cloud environments, makes it even more convenient and vulnerable. So, how do you detect suspicious activities on the network? That is where Network Detection and Response (NDR) comes into the picture.

Solution

For NDR-based threat-detection tools to do their job effectively, they must be fed with a constant stream of real-time and precise network data to the packet level, without missing any events or blind spots. But to provide this real-time intelligence at today's high-speed multi-100Gbps networks, you need to have the right network visibility equipment and technology plugged into the network layer.

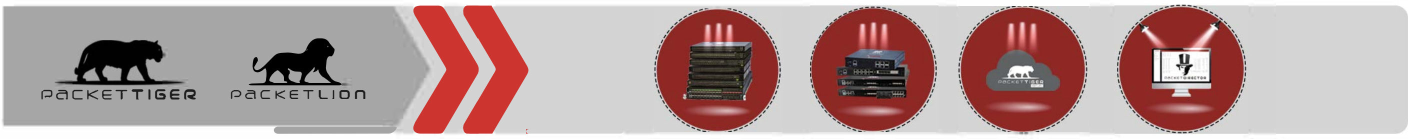


• Network Visibility

Neox Networks is the expert in tapping and brokering high-integrity network data from on-premises or multi-cloud environments and feeding it to NDR tools like Corelight in a real-time and lossless manner. A successful NDR solution foundation starts with extracting the network data by deploying NEOXPacketRaven physical TAP and NEOXPacketRavenVirtual vTAP strategically across the hybrid environment in the path of north-south and east-west network traffic. Network TAPs are decoupling elements for the secure and reliable tapping of network wire data in physical and virtual networks. These TAPs are looped into the network line to be monitored and forward the entire data traffic without interruption or packet loss.

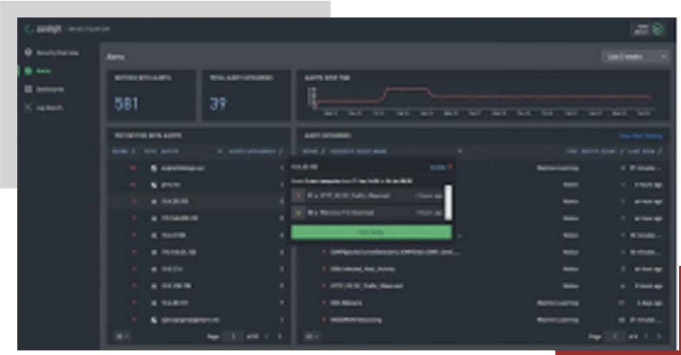
NEOXPacketRaven TAPs provide uninterrupted and permanent network traffic access up to 400G to Corelight. NEOXPackeHawk In-line Bypass TAP enables the network and security teams to maintain an uninterrupted connectivity and smooth network operations during a downtime or security tool maintenance window. NEOXPacketRavenVirtual provides Corelight, with network traffic access in hybrid-cloud/ multi-cloud environments.

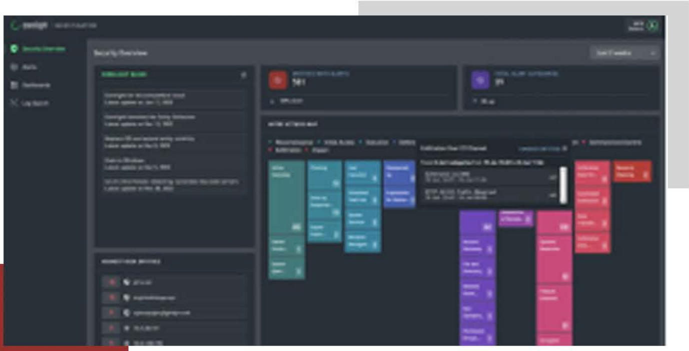
The next layer, a Network Packet Broker (NPB), aggregates all data streams from Network TAPs and processes it to filter and manipulate the data to forward it in the right format, to Corelight. NEOXPacketTiger Advanced Network Packet Brokers allow full parsing, payload processing, modifying, and optimizing the data packets. PacketTiger's advanced packet processing allows you to work more granularly and look deeper inside individual packets. NEOXPacketTigerVirtual provides a versatile solution for visibility in virtualized and public/private clouds. NEOXPacketLion Network Packet Broker acts as a high-density aggregation layer for TAPs and tools aggregation and consolidation in a two-tier scalable brokering model.

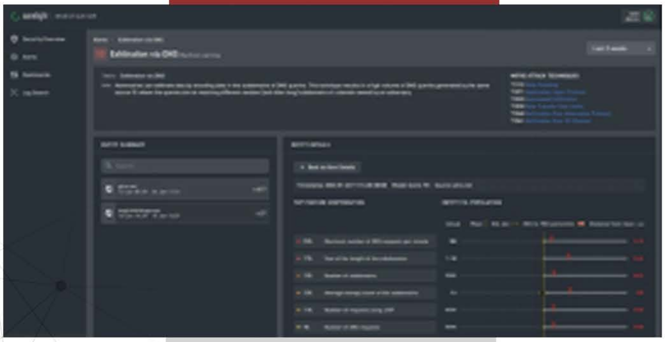


• Network Detection

Corelight Investigator Open NDR Platform is a Zeek and Suricata oriented tool that strengthens the cybersecurity posture through open standards and enhancements. Corelight Investigator combines the power of Open NDR Platform with machine learning (ML) and other analytics into an easy-to-use, quick-to-deploy SaaS solution. It simplifies Security Operations Center (SOC) workflows to give SecOps team valuable time back to triage and respond with confidence. Disrupt attacks by shifting from low-priority, reactive tasks to high-impact, proactive defense. Investigator's intuitive, out-of-the box dashboards make it easy to understand what's happening across your network—from on-prem to the cloud.
Zeek provides the evidence for anomaly detection, diagnostics, and threat hunting to narrow down the scope of the attack and locating rouge applications. Zeek maintains the log data with information consumable by security tools such as NDR, IDS, and Security Information and Event Management (SIEM). Zeek data is further complements through integration with Suricata, which is uses a binary pattern matching technology and generates the alerts, providing great context around an event. This greatly reduces the time and resulting damage, in rode rot contain and respond to the attack timely.
Investigator helps increase SOC performance metrics and cut through the backlog with aggregated, prioritized alerts mapped to the MITRE ATT&CK® framework







Corelight Investigator can deliver telemetry into existing SIEM, XDR, or SaaS-based solutions through integration with CrowdStrike XDR to enable cross-platform (EDR+NDR) analytics. This provides you with the most complete network visibility, powerful detections, and threat hunting capabilities, and accelerates investigation across your entire kill chain.

• Network Response

Although mostly NDR solutions like Corelight need real-time network data for threat hunting, it becomes more desirable to provide deeper context and evidential information in the format of PCAP in case of (a) an event is detected that require deeper investigation, and (b) if a breach has occurred and detected late when no real-time data is available and going back to that window of time is required. In such Incident Response (IR) case, time is of the essence to contain the damage, respond to the situation, and protect the financial cost and business reputation. Capturing and storing (aka recording) the network packet data become extremely useful value-add. SecOps and forensics experts can progressively drilldown the network packet data in a before, during, and after the event as alerts generated by Suricata are sent via an API call to NEOXPacketFalcon and NEOXPacketGrizzly Full Packet Capture Appliances to tag the data enabling fast data queries and analysis of specific events.

To store large amount of data at high-speeds, a packet capture appliance uses specialized high-performance hyper-converged architecture to capture network data in a lossless fashion and store it permanently on built-in storage disks or cloud storage. The stored data can be retrieved and played back at any time just like a DVR, for troubleshooting, security forensics, or evidence. NEOXPacketFalcon and NEOXPacketGrizzly Full Packet Capture Appliances are a high-performance FPGA-based s olution to record the network packet data for up to I00Gbps speeds and support Wireshark. The onboard storage capacity of up to 8 PB, depending on the use case and the length of the time the data must be stored, is ample for Incident Response and Network Forensics.

Summary

Neox Networks and Corelight Network Detection and Response solution offers one of the best choices in the industry to deal with emerging network security threats. The plug-n-play open-standards-based solution is pre-qualified and easy to deploy - which shrinks the time-to-value. Contact us for a live demo.

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 https://www.neox-networks.com/en

Corelight provides Open-Standards based Network Detection and Response solution for better security and incident response. Learn more at https://www.corelight.com