NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

PACKETOWL

Datenblatt

# NEOX**PacketOwl** Security Monitoring Appliance

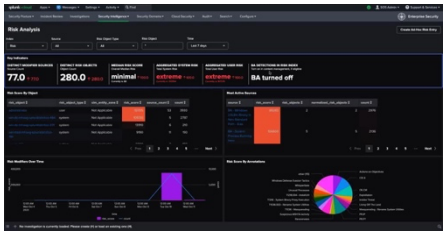
High-Performance, Precise, Suricata IDS-Based Open Network Security Monitoring, Event-Triggered 100Gbps Sustained Full-Packet Capture, Analysis, Logging, and Alerting

PacketOwl ermöglicht folgendes:

- Unübertroffenes Suricata-on-Steroids Open IDS-basiertes Network Security Monitoring und Transparenz für SecOps
- Schaffen Sie einen Zero-Trust-Verteidigungsperimeter, indem Sie den Netzwerkverkehr mit einem anhaltenden Durchsatz von bis zu 100 Gbps ohne Verluste oder Kompromisse analysieren
- Generieren Sie Sicherheitswarnungen, die von Drittanbieter SIEM-Devices und NDR-Tools verwendet werden können.
- Generierung von Protokolldaten und Einspeisung in ein offenes Ökosystem gebräuchlicher Protokollierungsfunktionen
- Erfassen von ereignisgesteuerten Paketdaten für forensische Analysen, Beweise und Compliance
- Entlastung teurer Sicherheitstools und Reduzierung der Verweildauer von Bedrohungen durch hochpräzise signaturbasierte Bedrohungssuche und Alarmierung

## NEOX Lösung

splunk>



Die NEOX PacketOwl Network Security Monitoring (NSM) Appliance ist eine fortschrittliche, hochperformante, paketdatenbasierte Sicherheitsüberwachungs- und -bereitstellungsplattform, die Cyber-Bedrohungen in Echtzeit identifiziert, analysiert, protokolliert und im Falle einer Bedrohung Alarm schlägt.

PacketOwl basiert auf der hochleistungsfähigen FPGA-basierten NEOX-Architektur und Suricata, einer robusten Open-Source-Engine zur Erkennung von Netzwerkbedrohungen.
Sie erlaubt tiefgreifende Netzwerkeinblicke, und nutzt Intrusion Detection (IDS) und Network Security Monitoring (NSM), um Unternehmens- und Service-Provider-Netzwerke vor einer Vielzahl von bösartigen Aktivitäten zu schützen.

Mit seinem verlustfreien, auf hohen Datendurchsatz optimierten, Design kann die PaketOwl bis zu 100 Gbps anhaltenden Netzwerkverkehr erfassen und analysieren und ist damit die leistungsstärkste offene Plattform auf Suricata-Basis, die es derzeit in der Branche gibt.

Dieses auf Skalierbarkeit und Flexibilität ausgelegte System bietet einen beispiellosen Einblick in den Netzwerkverkehr und liefert verwertbare Erkenntnisse für die Erkennung von Bedrohungen und die darauffolgende Alarmierung. Es analysiert Netzwerkflüsse effizient, um bekannte und neu auftretende Bedrohungen zu erkennen und einen umfassenden Schutz auch vor ausgeklügelten Cyberangriffen zu gewährleisten.

Mit anpassbaren Regelsätzen, Echtzeit-Warnungen und einer nahtlosen Integration in die bestehende Sicherheitsinfrastruktur ist das Suricata-basierte Security Threat Detection System ein unverzichtbares Werkzeug für Unternehmen, die ihre Cybersicherheit verbessern, Reaktionszeiten verkürzen und sich proaktiv gegen neue netzwerkbasierte Bedrohungen schützen wollen. Die Lösung eignet sich perfekt als erste Verteidigungslinie und als Ergänzung zu Network Detection and Response (NDR)-Tools.

SURICATA®

## Freisetzung des vollen Suricata-Potenzials

Unternehmen sehen sich heute mit einer wachsenden Zahl von Herausforderungen im Bereich der Cybersicherheit konfrontiert, die in erster Linie auf die zunehmende Raffinesse und Häufigkeit von Cyberbedrohungen zurückzuführen sind. Die Cyber-Bedrohungslandschaft entwickelt sich ständig weiter, da Cyber-Kriminelle immer neue Taktiken, Techniken und Verfahren entwickeln.

Unternehmen haben Mühe, mit neuen Bedrohungen wie Advanced Persistent Threats (APTs), Zero-Day-Schwachstellen, Ransomware und anderen Formen von Malware Schritt zu halten.

Moderne Unternehmen operieren in immer komplexeren Netzwerkumgebungen, einschließlich lokaler Infrastruktur, Cloud und hybrider Modelle, was die Sicherung der Kommunikation, die Identifizierung von Bedrohungen und die Gewährleistung der Transparenz des gesamten Datenverkehrs erschwert. Hinzu kommt, dass die schiere Menge der über Netzwerke übertragenen Daten in Kombination mit der Geschwindigkeit, mit der der Datenverkehr fließt, es für herkömmliche Sicherheitssysteme schwierig macht, potenzielle Bedrohungen in Echtzeit zu analysieren und zu erkennen, ohne Leistungsengpässe zu verursachen.

Vielen Unternehmen fehlen effektive Tools zur Überwachung des Netzwerkverkehrs in Echtzeit oder zur Korrelation von Ereignissen in verschiedenen Sicherheitslösungen. Dieser Mangel an Transparenz kann die Erkennung von Eindringlingen verzögern und Angriffe unentdeckt eskalieren lassen. Unternehmen verfolgen bei der Cybersicherheit häufig einen reaktiven Ansatz, d. h. sie reagieren auf Vorfälle, nachdem sie eingetreten sind, anstatt Bedrohungen proaktiv zu erkennen und zu entschärfen, bevor sie Schaden anrichten. Suricata begegnet diesen Herausforderungen, indem es Unternehmen eine leistungsstarke, skalierbare Sicherheitslösung zur Verfügung stellt, die den Netzwerkverkehr in Echtzeit analysiert und umfassende Bedrohungen erkennt.

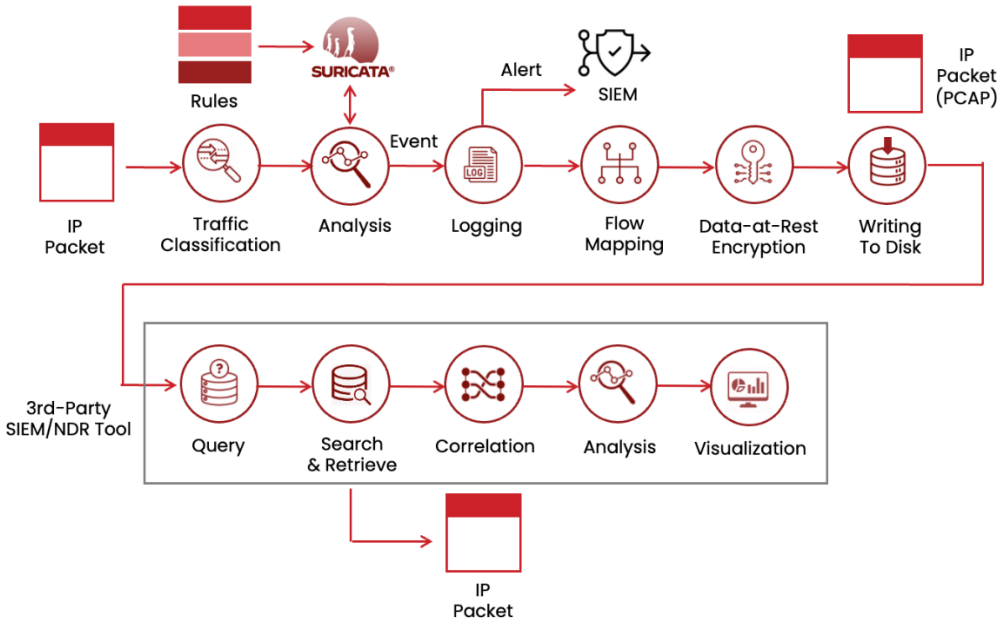



Diagramm-1: Betrieb von PacketOwl NSM und Drittanbieter-SIEM und/oder NDR-Tool

## Enterprise-Grade Open Network Security Monitoring

Umfassende Bedrohungserkennung auf der Basis von NEOXPacketOwl NSM und Open Suricata ermöglicht es Unternehmen, eine Vielzahl bekannter und unbekannter Bedrohungen zu erkennen, darunter fortschrittliche Malware, Eindringungsversuche und verdächtige Aktivitäten, um einen umfassenden Schutz zu gewährleisten. PacketOwl kann den Netzwerkverkehr in Echtzeit erfassen und analysieren, so dass Bedrohungen sofort erkannt werden und die Zeit bis zur Reaktion verkürzt wird. Dies hilft Unternehmen, von einer reaktiven zu einer proaktiven Sicherheitshaltung überzugehen. PacketOwl lässt sich effizient skalieren, um die Anforderungen von Unternehmen jeder Größe und in unterschiedlichen Umgebungen zu erfüllen.

PacketOwl lässt sich mühelos in bestehende Sicherheits-Frameworks integrieren, unabhängig davon, ob es vor Ort, in der Cloud oder in hybriden Umgebungen eingesetzt wird. Es dient als kritisches Element und erste Verteidigungslinie, die nach der Perimeter-Firewall als Teil einer Zero-Trust-Sicherheitsstrategie positioniert ist. PacketOwl erkennt effektiv die meisten signaturbasierten Netzwerkangriffe. Bei neuen oder unkonventionellen Bedrohungen können zusätzliche NDR-Tools als innere Verteidigungsschicht hinzugefügt werden, falls erforderlich. Außerdem kann PacketOwl Protokolle an zentrale Protokollverwaltungssysteme weiterleiten und Sicherheitswarnungen an SIEM-Plattformen (Security Information and Event Management) wie Splunk senden.

Mit PacketOwl erhalten Unternehmen einen tiefen Einblick in den Netzwerkverkehr und die Protokolle, so dass sie Anomalien und Schwachstellen in ihren Netzwerken mit größerer Genauigkeit und Zuverlässigkeit erkennen können. So können Unternehmen nicht nur Bedrohungen schneller erkennen und darauf reagieren, sondern auch eine widerstandsfähigere und sicherere Netzwerkinfrastruktur aufbauen.

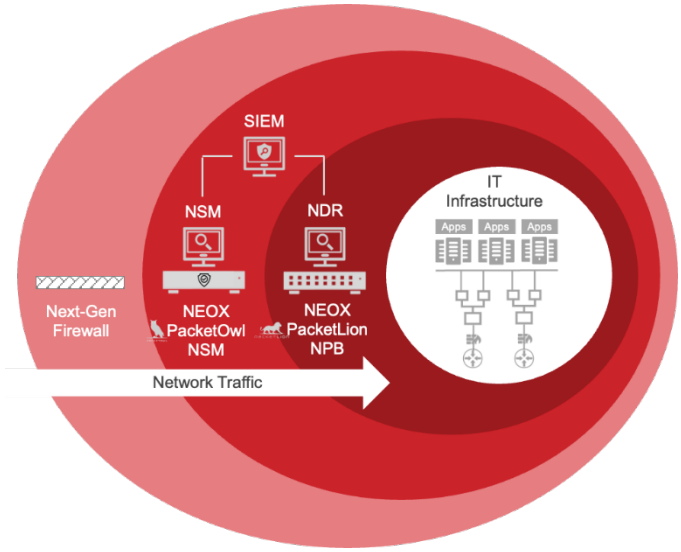



Diagramm-2: PacketOwl NSM Deployment-Strategie

## Key Benefits

### Optimierte Bedrohungsanalyse bei hoher Verkehrslast

NEOXPacketOwl NSM wurde entwickelt, um hohe Verkehrsaufkommen zu bewältigen, bei dem andere Systeme ins Stocken geraten oder ausgebremst werden. Mit einer Geschwindigkeit von 100 Gbit/s erfasst und analysiert PacketOwl jedes Paket mit einer "Suricata-on-Steroids"-optimierten Technologie. IT-Benutzer können die Signaturen und Regeln jederzeit ändern und haben so die volle Kontrolle über ihre Richtlinien und das, was sie für wichtig halten. Suricata signaturbasierte Regeln sind Muster oder Signaturen, die von Suricata verwendet werden, um bekannte netzwerkbasierte Bedrohungen zu erkennen und zu identifizieren. Diese Regeln bieten einen struktu-rierten Weg und vordefinierte Kriterien, die bösartige Aktivitäten oder Angriffsmuster beschreiben, so dass Suricata den Netzwerkverkehr mit diesen Signaturen abgleichen kann, um potenzielle Bedrohungen zu erkennen. PacketOwl NSM filtert nur die Datenflüsse und Transaktionen heraus, die bestimmten Ereignissen oder Vorfällen entsprechen, und speichert die mit diesen Datenflüssen verbundenen Protokoll- und Paketdaten für forensische Analysen, historische Aufzeichnungen und Compliance. Gleichzeitig generiert es Warnmeldungen, die an ein SIEM (wie Splunk) oder andere Überwachungsplattformen gesendet werden können.

### Out-of-Box-Interoperabilität für die gemeinsame Nutzung von Protokolldaten

Es besteht die Notwendigkeit, Protokolle aufzubewahren und zu speichern. Die Protokolle sollten sicher und in Übereinstimmung mit den Standards aufbewahrt werden, um sicherzustellen, dass sie bei Untersuchungen zur Cybersicherheit zur Überprüfung und Analyse zur Verfügung stehen. Diese Aufbewahrung ist für Audits, die Einhaltung von Compliance und Bewertungen nach einem Vorfall von entscheidender Bedeutung. NEOXPacketOwl NSM fördert ein offenes Ökosystem mit nahtloser Out-of-the-Box-Integration mit Standard-Protokollierungssystemen wie Syslog-Servern und anderen weit verbreiteten Systemen. Diese Protokollierungssysteme sammeln, speichern und verwalten Protokolldaten und ermöglichen es Sicherheitsteams in einem Security Operations Center (SOC), Verhaltensweisen zu überwachen, Anomalien zu erkennen und Vorfälle zu untersuchen. Die Integration spielt eine wichtige Rolle bei der Aufrechterhaltung des Zustands, der Sicherheit und der Leistung der IT-Infrastruktur, da die Zentralisierung es den Cybersicherheitsteams ermöglicht, Daten aus verschiedenen Quellen zu analysieren und zu vergleichen, um Bedrohungen frühzeitig zu erkennen.

### Zero-Trust-Weiterleitung von Alarmen an SIEM-Plattformen

Von NEOXPacketOwl NSM erzeugte Protokolle werden normalerweise auch an SIEM-Systeme wie Splunk oder andere Tools von Drittanbietern weitergeleitet. Diese Systeme sammeln, aggregieren und analysieren die Logs, um Muster und Anomalien zu erkennen. Die Protokolle können auch an vertrauenswürdige externe Partner und Branchenbeteiligte weitergegeben werden, um die allgemeine Cybersicherheit zu verbessern. Der NEOX PacketOwl NSM ist so konzipiert, dass er Echtzeitwarnungen auslöst, sobald verdächtige oder bösartige Aktivitäten im Netzwerk entdeckt werden. Diese Warnungen werden dann an relevante Stakeholder weitergeleitet, wie z. B. das SOC, den CISO oder Incident Response (IR) Teams. So kann beispielsweise ein fehlgeschlagener Anmeldeversuch, auf den ein erfolgreicher Zugriff folgt, einen Alarm auslösen, oder ein ungewöhnlicher ausgehender Netzwerkverkehr einen Alarm für einen möglichen Datenexfiltrationsversuch. Im Einklang mit den Zero-Trust-Prinzipien wird jedes Ereignis, das von der normalen Basislinie abweicht, protokolliert und zur Überprüfung gekennzeichnet. Diese Warnungen werden in ein breiteres Rahmenwerk für die Reaktion auf Vorfälle integriert, das sicherstellt, dass die Teams in der Lage sind schnell zu handeln, um Sicherheitsbedrohungen zu untersuchen, einzudämmen und zu entschärfen.

### Forensische Analyse zur Erkennung von und Reaktion auf Zwischenfälle

Der Logging-Mechanismus ist entscheidend für die Echtzeit-Überwachung und Erkennung von Cyber-Vorfällen. Logs und die damit verbundenen erfassten Paketdaten (PCAP) von NEOXPacketOwl NSM liefern wichtige Beweise, um Bedrohungen wie Malware-Infektionen, Versuche der Privilegienerweiterung oder den unbefugten Zugriff auf sensible Daten zu identifizieren. Logs und Pakete ermöglichen es Security Operations (SecOps) Teams, den Umfang eines Sicherheitsvorfalls schnell zu bestimmen. NEOXPacketOwl NSM ist eine All-in-One-Lösung, die ein auf offenen Standards basierendes Hochgeschwindigkeits-IDS bietet, das Protokolle und Warnungen generiert und gleichzeitig selektive Pakete im PCAP-Format für jede Interaktion im Zusammenhang mit einem Vorfall erfasst und speichert. Pakete lügen nicht. Zusätzlich zu den Protokolldaten liefern diese PCAP-Daten alle notwendigen Informationen für forensische Untersuchungen und die Beweissicherung. Sie erweisen sich als besonders wertvoll in Fällen von Cyberkriminalität, die sich gegen Unternehmen, Finanzinstitute, staatliche Einrichtungen und kritische Infrastrukturen richtet. Im Falle eines Einbruchs zeigen die Daten beispielsweise, auf welche Systeme zugegriffen wurde, von wem und wie sich der Angriff über das Netzwerk ausgebreitet hat. IR-Teams können Protokoll- und PCAP-Paketdaten verwenden, um nach einem Angriff forensische Untersuchungen durchzuführen und die Eintrittspunkte, Methoden und betroffenen Anlagen zu identifizieren. Außerdem können sie damit den zeitlichen Ablauf des Angriffs verfolgen und den Gesamtschaden abschätzen.

### Audit Trail für die Einhaltung von Industrie- und Behördenvorschriften

Die PacketOwl NSM ist in der Lage, jeden Datenfluss und jede Transaktion bei Netzwerkgeschwindigkeitigkeiten von bis zu 100 Gbit/s aufzuzeichnen. Damit erfüllen Unternehmen, Dienstanbieter und öffentliche Organisationen die Executive Order (EO) 14028 und M-21-30, die sich auf die Verbesserung der Ermittlungs- und Abhilfekapazitäten der US-Bundesregierung im Zusammenhang mit Cybersicherheitsvorfällen konzentriert. Die meisten Organisationen sind außerdem verpflichtet, einen Audit-Trail über ihre Aktivitäten zu führen, der nicht nur Sicherheitsvorfälle, sondern auch die als Reaktion darauf ergriffenen Maßnahmen enthält. Diese Prüfprotokolle werden verwendet, um die Einhaltung der branchen- und bundesweiten Cybersicherheitsvorschriften nachzuweisen. Die Prüfprotokolle enthalten Protokolle über die während eines Cybervorfalls durchgeführten Aktionen (z. B. welche Benutzer wann auf welche Systeme zugegriffen haben), über die während des Reaktionsprozesses auf den Vorfall getroffenen Entscheidungen und darüber, ob die Sicherheitskontrollen wie vorgesehen befolgt wurden. Diese umfassenden Aufzeichnungen sind für künftige Prüfungen unerlässlich, um sicherzustellen, dass Unternehmen die bewährten Verfahren für die Cybersicherheit einhalten, und um eine bessere Entscheidungsfindung bei späteren Reaktionen auf Vorfälle zu ermöglichen.

## Deployment

Die NEOXPacketOwl Network Security Monitoring Appliance ist eine ideale Lösung für Unternehmen, Rechenzentren, Cloud-Umgebungen, Service-Provider und Behörden. Sie kann sowohl den Ost-West- als auch den Nord-Süd-Netzwerkverkehr mit Geschwindigkeiten von bis zu 100 Gbps scannen und analysieren. Die On-Premise-Lösung ist eine 2HE-Rack-Einheit mit Front-to-Back Luftstrom und verfügt über 2 x 100Gbps QSFP28-Ports sowie weitere Konnektivitätsoptionen wie 10, 25 oder 40Gbps, die SR1.2 (BiDi), SR4, LR4 und ER4-Optiken unterstützen.

NEOXPacketOwl NSM arbeitet als vollständig autonome Appliance, die Protokolle und Warnungen für SIEM-Systeme (wie Splunk oder SIEMs von Drittanbietern) generieren kann. Sie kann aber auch mit einem NDR-Tool zusammenarbeiten. In solchen Fällen kann ein NEOXPacketLion Packet Broker oder eine PacketWolf Packet Processing Appliance den Echtzeit-Netzwerkverkehr an die NDR-Tools weiterleiten.

Ein skalierbares Design für die Sicherheitstransparenz im Rechenzentrum beginnt mit dem Einsatz von Netzwerk-TAPs an den wichtigsten Punkten, um den Netzwerkverkehr zu spiegeln (siehe NEOX Network Traffic Tapping-Lösungen für verschiedene TAP-Optionen). Während die TAPs den Datenverkehr direkt an die PacketOwl NSM-Appliance weiterleiten können, besteht ein effizienterer Ansatz für die Verwaltung des Netzwerks darin, die TAPs mithilfe eines Network Packet Brokers (NPB) zu aggregieren. Der NPB kann den Datenverkehr konsolidieren, filtern und manipulieren und ihn an mehrere Ziele wie die PacketOwl NSM-Appliance und NDR-Tools weiterleiten (siehe NEOX Network Traffic Brokering-Lösungen für eine Reihe von NPB-Optionen).

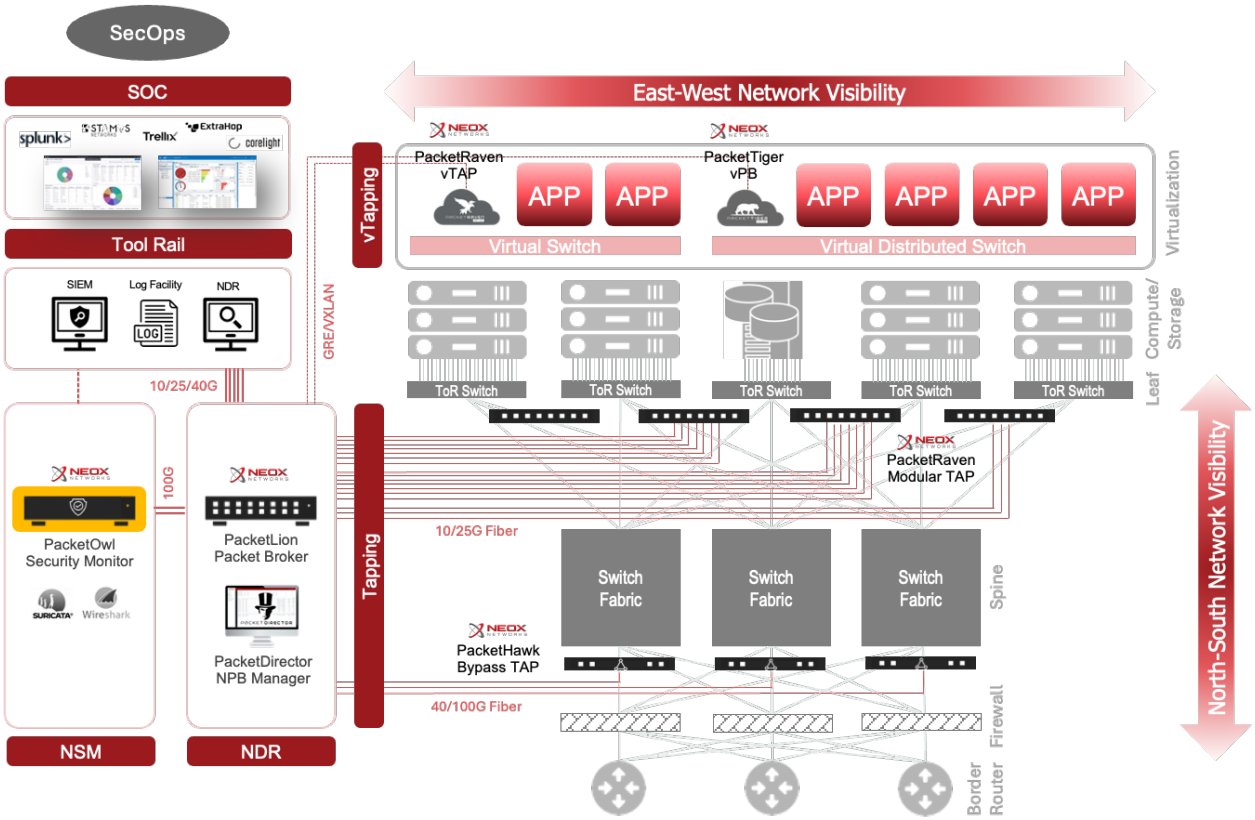



Diagramm-3: NEOXPacketOwl NSM Einsatz im Rechenzentrum

Der Erlass EO 14028 der US-Regierung fordert die Bundesbehörden auf, ihre Fähigkeit zur Erkennung von und Reaktion auf Cyber-Bedrohungen zu verbessern, indem sie Tools zur kontinuierlichen Überwachung ihrer IT-Umgebungen einsetzen. Ziel ist es, umfassende Protokolle über alle Endpunkte, Netzwerke und Systeme zu erfassen. Dazu müssen zentrale Protokollierungssysteme (z. B. SIEM) eingerichtet werden, die Protokolle von verschiedenen Sicherheitstools und Netzwerkgeräten wie Firewalls, IDS und EDR-Plattformen (Endpoint Detection and Response) zusammenfassen. Zu den erfassten Protokollen gehören Systemereignisse, Netzwerkverkehrsdaten, Anwendungsprotokolle, Sicherheitswarnungen und andere wichtige Metriken.

Die Implementierung der Zero Trust Architecture (ZTA), wie in M-21-30 beschrieben, fügt diesem Protokollierungsmechanismus eine weitere Ebene hinzu. Da Zero Trust darauf beruht, dass jeder Zugriffsversuch als potenziell nicht vertrauenswürdig behandelt wird, werden alle Zugriffsanfragen, einschließlich der Benutzerauthentifizierung, des Gerätezugriffs und der Netzwerkaktivitäten, protokolliert. Die Ereigniskorrelation kombiniert Daten aus verschiedenen Protokollen, um ein kohärentes Bild eines potenziellen Sicherheitsvorfalls zu ermitteln. Wenn beispielsweise Protokolle eines Endpunkt-Erkennungssystems ein abnormales Verhalten auf einem Gerät zeigen und Protokolle einer Netzwerk-Firewall ungewöhnliche Datenverkehrsmuster aufweisen, können diese Ereignisse miteinander korreliert werden, um auf einen Verstoß hinzuweisen. Für den Einsatz in der Cloud bietet die NEOXPacketOwlVirtual eine praktisch unbegrenzte Leistung, je nach der bereitgestellten Cloud-Instanz.

PacketOwlVirtual kann die Warnmeldungen an ein Cloud-natives oder lokales SIEM weiterleiten, während die Protokoll- und Paketdaten lokal in der Cloud innerhalb der Virtual Private Cloud (VPC) des Unternehmens gespeichert werden. Die NEOX-Lösung unterstützt alle großen öffentlichen Clouds, einschließlich Amazon Web Services (AWS), Microsoft Azure und Google Cloud.

Die Cloud-Bereitstellung beginnt mit der Extraktion und Einspeisung nicht vertrauenswürdiger Netzwerkverkehrsströme, die analysiert werden müssen. Dies lässt sich leicht durch den Einsatz von virtuellen TAPs (vTAP) oder der Verwendung von VPC-Traffic-Spiegelung erreichen (siehe NEOX Network Traffic Tapping-Lösungen für verschiedene TAP-Optionen). Während vTAPs den Datenverkehr direkt an die PacketOwlVirtual NSM (vNSM) Appliance senden können, besteht ein effizienterer und kostengünstigerer Ansatz für die Verwaltung des Netzwerks darin, die vTAPs über einen Virtual Network Packet Broker (vPB) zu aggregieren. Der vPB kann den Datenverkehr konsolidieren, filtern und manipulieren und ihn an mehrere Ziele weiterleiten, einschließlich des PacketOwlVirtual NSM und der NDR-Tools (siehe NEOX Network Traffic Brokering-Lösungen für eine Reihe von vPB-Optionen).

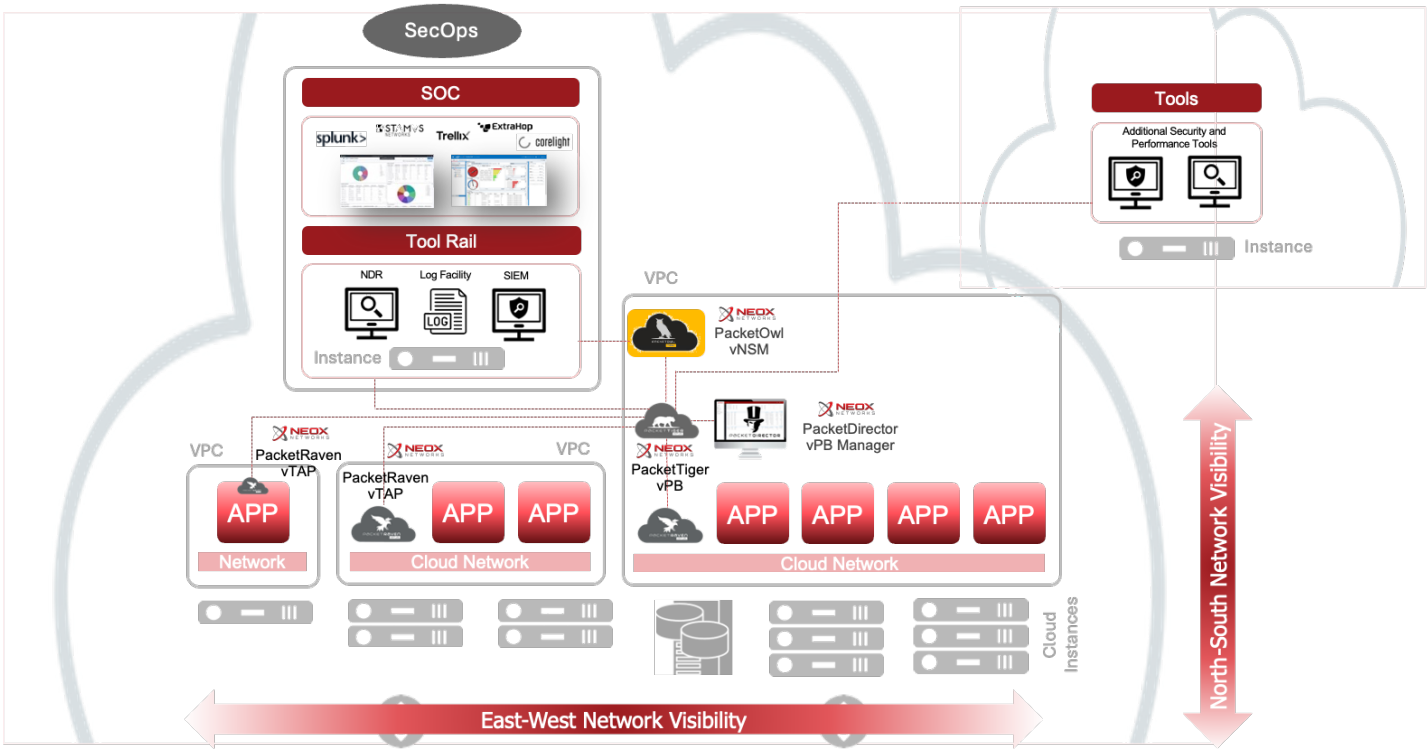



Diagramm-4: NEOX PacketOwlVirtual NSM Einsatz in der Cloud

# Technische Spezifikationen

## Key Features

| | |
|---|---|
| Suricata-basierter Threat Analysis Durchsatz (Max.) | 100Gbps |
| Paket- und Log-Daten Speicherkapazität (Max.) | 760TB |
| Event-Handling Performance (Rate) | > 10.000 Events / Sekunde |
| Event-Logging Performance (Rate) | 2GB / Minute |
| Hardware-Buffer (um Microbursts abzufangen und zu analyieren) | 8GB / 12GB |
| Kompatibilität mit Suricata Signatur-basierten Regelsätzen | Ja |
| Flexible Drittanbieter-SIEM Integration | Ja |
| Log-Rotation | Ja |
| Log-Kompression | Ja |
| Benutzerseitig konfigurierbare Regeln | Ja |
| Lua-Integration (Pattern Matching) | Ja |
| Dateiextraktion | Ja |
| Präzises Hardware-basiertes Timestamping (PTP) | Ja |
| Konditionelles Capture-to-Disk (Smart Capture) | Ja |
| PCAP-Support | Ja |
| Solid State (SSD) Speicher | Ja |
| Static Encrypted Disk (SED) Speicher (Option) | Ja |
| Hardware RAID 0, 5, 10 | Ja |
| Redundantes 10G Management-Interface (SFP+ Option) | Ja |

## Konnektivität

| Link-Geschwindigkeit (Optionen) | Anzahl Interfaces | Unterstützte Transceiver |
|---|---|---|
| 100G Ports | 2 | QSFP28 |
| 40G Ports | 2 | QSFP+ |
| 25G Ports | 4 | SFP28 |
| 10G Ports | 4 | SFP+ |
| 1G Ports | 4 | SFP |
| Management Interface | 1 | RJ45 / SFP+ |
| Timing/Synchronization | 1 | PTP |

## Abmessungen und Gewicht

| | |
|---|---|
| Höhe | 8,7 cm |
| Breite | 77,2 cm |
| Tiefe | 48,3 cm |
| Gewicht | 30 Kg |
| | |

## Platzbedarf, Strom, und Kühlung

| | |
|---|---|
| Höheneinheiten | 2 HE |
| Airflow | Front-to-Back |
| Stromversorg.redundanz | 1+1 AC/DC |
| Max. Stromverbrauch | |
| Wärmeableitung | |

## Betriebsbedingungen

| | |
|---|---|
| Betriebstemperatur | 5°C – 45°C |
| Lagertemperatur | -40°C – 65°C |

## Zertifizierungen

| | |
|---|---|
| Sicherheit | EN IEC 62368-1:2020 +A11:2020, EN IEC 62311:2020, EN 62479:2010 |
| EMC | EN 55032:2015 +A11:2020, EN 55035:2017 +A11:2020, EN 61000-3-2:2014, EN 61000-3-3:2013 |

| | |
|---|---|
| Luftfeuchtigkeit - Betrieb | 8% – 90% |
| Luftfeuchtigkeit - Lagerung | 5% – 95% |

| | |
|---|---|
| RoHS | EN IEC 63000:2018 |
| | |

## Virtuelle und Cloud-Deployments

| | |
|---|---|
| VMware ESXi | Ja |
| Open Stack | Ja |
| Docker & Kubernetes | Ja |
| Azure Cloud | Ja |
| AWS Cloud | Ja |
| Google Cloud | Ja |

| | |
|---|---|
| Min. CPU-Kerne | 1 |
| Min. Hauptspeicher | 256GB |
| Min. Datenspeicher | 1TB |
| Min. Virtuelles Interface | 1 |
| Min. Processing Speed | 1Gbps |
| Max. Processing Speed | Instanzabhängig |

# Bestellinformationen

| Artikelnummer | Beschreibung |
|---|---|
| NX-NSMPO-100G-90TB-3Y | NEOXPacketOwl Network Security Monitoring (NSM) Appliance mit 100Gbps Suricata-basiertem IDS, Logging und Full-Packet-Capture - FPGA Capture SmartNIC mit 2 x 100G QSFP28 Ports, 768GB RAM und 90TB SSD Capture Storage. Beinhaltet 3 Jahre Software-Support und -Wartung, 3 Jahre Hardware-Wartung und technischen Support. |
| NX-NSMPO-100G-180TB-3Y | NEOXPacketOwl Network Security Monitoring (NSM) Appliance mit 100Gbps Suricata-basiertem IDS, Logging und Full-Packet-Capture - FPGA Capture SmartNIC mit 2 x 100G QSFP28 Ports, 768GB RAM und 180TB SSD Capture Storage. Beinhaltet 3 Jahre Software-Support und -Wartung, 3 Jahre Hardware-Wartung und technischen Support. |
| NX-NSMPO-100G-360TB-3Y | NEOXPacketOwl Network Security Monitoring (NSM) Appliance mit 100Gbps Suricata-basiertem IDS, Logging und Full-Packet-Capture - FPGA Capture SmartNIC mit 2 x 100G QSFP28 Ports, 768GB RAM und 360TB SSD Capture Storage. Beinhaltet 3 Jahre Software-Support und -Wartung, 3 Jahre Hardware-Wartung und technischen Support. |
| NX-NSMPO-100G-760TB-3Y | NEOXPacketOwl Network Security Monitoring (NSM) Appliance mit 100Gbps Suricata-basiertem IDS, Logging und Full-Packet-Capture - FPGA Capture SmartNIC mit 2 x 100G QSFP28 Ports, 768GB RAM und 720TB SSD Capture Storage. Beinhaltet 3 Jahre Software-Support und -Wartung, 3 Jahre Hardware-Wartung und technischen Support. |

### Über NEOX NETWORKS

NEOX Networks bietet Netzwerkvisibilität der nächsten Generation für IT- und OT-Überwachung und -Sicherheit. Das Ergebnis ist eine verbesserte Cybersicherheit, Transparenz von Hybrid-Cloud-Anwendungen und Business Continuity durch die Integration von Netzwerkintelligenz und Data-in-Motion in Echtzeit. Erfahren Sie mehr unter neox-networks.com