NEOX NETWORKS

NEXT GENERATION NETWORK VISIBILITY

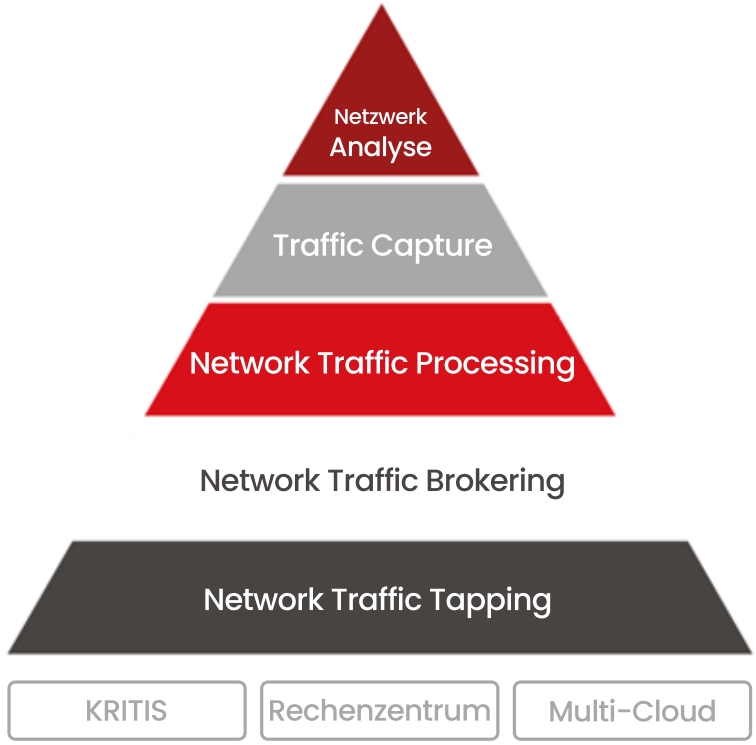
PRODUKTBROSCHÜRE

Next-Generation Network Visibility für IT & OT Observability und Security

Download

NEOX Network Visibility Plattform

Next-Generation Network Visibility für IT & OT Observability und Security



Business Benefits

- Digitale Transformation und Modernisierung durch Hybrid-Cloud Observability
- Erhöhte Business Continuity und reduzierte Downtime
- Geringere Kundenabwanderung durch bessere User Experience, erhöhte Sicherheit und Datenschutz

Technische Benefits

- Setup Once, Monitor Forever Network Visibility and Real-Time Wire-Data Access for Tools
- Skalierbares Fundament für den Aufbau von Netzwerk-überwachung, -sicherheit und Observability
- Konsistente Netzwerktransparenz für die Bereitstellung von Network-as-a-Service in der Hybrid-Cloud

Security & Datenschutz

- Stärkung der Netzwerksicherheit durch direkten Zugriff und Konsolidierung von Netzwerkpaketdaten
- Echtzeit-Netzwerkintelligenz für das Threat Hunting und Network Detection and Response (NDR)
- Historischer Netzwerkdatenzugriff für Forensik, Incident Response und Compliance

Application Observability

- Verbesserte Applikationsperformance, Reaktion und Verfügbarkeit durch Network Dependency Mapping
- Schnelleres Troubleshooting bei User Experience Problemen
- Reduzierte Mean-Time-to-Resolution (MTTR)

NEOX NETWORKS

PACKETFALCON PACKETGRIZZLY

NEOX**PacketFalcon** & NEOX**PacketGrizzly**
Packet Capture & Analyse Familien

Stärkung der Cybersicherheit und Application Observability
durch Integration historischer Netzwerkdaten und -forensik

NEOX NETWORKS

Packet Capture

NEOXPacketFalcon Mini Capture Appliance

Portabel & Kompakt | 10Gbps Capture-to-Disk | 32TB Speicher
Security-Forensik | Compliance | Out-of-Box Dashboards

- Verlustfreie Paketerfassung
- Dauerhaftes Capture-to-Disk bis zu 10Gbps
- High-Speed FPGA Capture-Karten
- Intelligentes & Kompressions-basiertes Capturing
- Bis zu 30TB Speicherkapazität
- Portabel, kompakt und robust
- Lüfterloses Design
- Flexible Konnektivität durch SFP/SFP+/SFP28
- FPGA-basiertes 10 Nanosekunden Timestamping
- FPGA-basiertes Packet Slicing & Capture Filter
- FPGA-basierte Deduplication
- PCAP & PCAPNG Support

PACKETFALCON

neoxn.de/falconm

Incident Response | Netzwerkforensik | Troubleshooting

Compliance | Zweigstelle | Remote Site

- Die NEOXPacketFalcon Mini Packet Capture Appliance ist eine leistungsstarke Lösung zur Aufzeichnung von Netzwerk-Paketdaten für Geschwindigkeiten von bis zu 10 Gbps (1Gbps oder 10Gbps).
  Die integrierte Speicherkapazität umfasst 7TB, 15TB oder 30TB, je nach Anwendungsfall und Speicherdauer der Daten.
- NEOXPacketFalcon ermöglicht es IT-NetOps- und AppOps-Teams, jederzeit auf historische Daten zuzugreifen, die Datenströme für die Fehlersuche wiederherzustellen und Analysen auf Sitzungs- oder Konversationsebene durchzuführen, wodurch die Fehlersuche und die Mean-Time-To-Resolution (MTTR) von Kundenproblemen merklich reduziert werden kann.
- NEOXPacketFalcon ist eine unverzichtbare Lösung für die Netzwerk-Forensik und die Reaktion auf Vorfälle für IT-SecOps-Teams in einer Post-Breach-Situation zur Untersuchung und gerichtlichen Beweisführung. Die vor, während und nach dem Ereignis erfassten Daten können dazu beitragen, die Sicherheitslücken, verdächtigen Aktivitäten und die IP-Adresse des Angreifers einzugrenzen.
  Durch die Indizierung der Daten und Hardware/Software-Filter (Berkeley Packet Filter) ermöglicht NEOXPacketFalcon den SecOps-Teams, Angriffe schnell zu untersuchen und zu blockieren.

NEOX NETWORKS

Packet Capture

NEOXPacketFalcon Mini X Capture Appliance

Portabel & Kompakt | 25Gbps Capture-to-Disk | 32TB Speicher
Security-Forensik | Compliance | Out-of-Box Dashboards

- Verlustfreie Packeterfassung
- Dauerhaftes Capture-to-Disk bis zu 25Gbps
- High-Speed FPGA Capture-Karten
- Intelligentes & Kompressions-basiertes Capturing
- Bis zu 30TB Speicherkapazität
- Portabel, kompakt und robust
- Lüfterloses Design
- Flexible Konnektivität durch SFP/SFP+/SFP28
- FPGA-basiertes 10 Nanosekunden Timestamping
- FPGA-basiertes Packet Slicing & Capture Filter
- FPGA-basierte Deduplication
- PCAP & PCAPNG Support

PACKETFALCON

neoxn.de/falconmx

Incident Response | Netzwerkforensik | Troubleshooting

Compliance | Zweigstelle | Remote Site

- Die NEOXPacketFalcon Mini X Packet Capture Appliance ist eine leistungsstarke Lösung zur Aufzeichnung von Netzwerk-Paketdaten für Geschwindigkeiten von bis zu 25 Gbps (1Gbps, 10Gbps oder 25Gbps). Die integrierte Speicherkapazität umfasst 7TB, 15TB oder 30TB, je nach Anwendungsfall und Speicherdauer der Daten.
- NEOXPacketFalcon ermöglicht es IT-NetOps- und AppOps-Teams, jederzeit auf historische Daten zuzugreifen, die Datenströme für die Fehlersuche wiederherzustellen und Analysen auf Sitzungs- oder Konversationsebene durchzuführen, wodurch die Fehlersuche und die Mean-Time-To-Resolution (MTTR) von Kundenproblemen merklich reduziert werden kann.
- NEOXPacketFalcon ist eine unverzichtbare Lösung für die Netzwerk-Forensik und die Reaktion auf Vorfälle für IT-SecOps-Teams in einer Post-Breach-Situation zur Untersuchung und gerichtlichen Beweisführung. Die vor, während und nach dem Ereignis erfassten Daten können dazu beitragen, die Sicherheitslücken, verdächtigen Aktivitäten und die IP-Adresse des Angreifers einzugrenzen. Durch die Indizierung der Daten und Hardware/Software-Filter (Berkeley Packet Filter) ermöglicht NEOXPacketFalcon den SecOps-Teams, Angriffe schnell zu untersuchen und zu blockieren.

NEOX NETWORKS

Packet Capture

NEOXPacketFalcon Portable Capture Appliance

Portabel & mobil | 100Gbps Capture-to-Disk | 480TB Speicher
Security-Forensik | Compliance | Out-of-Box Dashboards

- Verlustfreie Packeterfassung
- Dauerhaftes Capture-to-Disk bis zu 100Gbps
- Bis zu 3 High-Speed FPGA Capture-Karten
- Intelligentes & Kompressions-basiertes Capturing
- Bis zu 480TB Speicherkapazität
- HW-verschlüsselter (SED) Speicher
- Hardware RAID 0,5,6,00,50,60
- Portabel, mobil, und robust
- Flexible Konnektivität durch SFP, SFP+, SFP28, QSFP+, QSFP28
- FPGA-basiertes 10 Nanosekunden Timestamping
- FPGA-basiertes Packet Slicing & Capture Filter
- FPGA-basierte Deduplication
- PCAP & PCAPNG Support
- Optionaler Transportkoffer

PACKETFALCON

neoxn.de/falcon

Incident Response | Netzwerkforensik | Troubleshooting

Compliance | Ausseneinsatz | Remote Site

Eine Packet Capture Appliance verwendet eine spezielle, hochleistungsfähige, hyperkonvergente Architektur, um Netzwerkdaten verlustfrei aufzuzeichnen und sie dauerhaft in integrierten Speicherlaufwerken zu speichern.
Die gespeicherten Daten können wie bei einem DVR jederzeit abgerufen und wiedergegeben werden, z.B. zur Fehlersuche, für die Sicherheitsforensik oder als Beweismittel.

- Die NEOXPacketFalcon Portable Packet Capture Appliance ist eine leistungsstarke Lösung zur Aufzeichnung von Netzwerkpaketdaten für Geschwindigkeiten von bis zu 100 Gbps (1Gbps, 10Gbps, 25Gbps, 40Gbps oder 100Gbps). Die Onboard-Speicherkapazitätsoptionen umfassen 24TB, 51TB, 102TB, 240TB oder 480TB SSD-Speicher, je nach Anwendungsfall und Speicherdauer der Daten.
- NEOXPacketFalcon ermöglicht es IT-NetOps- und AppOps-Teams, jederzeit auf historische Daten zuzugreifen, Datenströme für die Fehlersuche neu zu generieren und Analysen auf Sitzungs- oder Konversationsebene durchzuführen, was die Fehlersuche und die Mean-Time-To-Resolution (MTTR) von Kundenproblemen deutlich reduzieren kann.
- NEOXPacketFalcon ist eine unverzichtbare Lösung für die Netzwerkforensik und die Reaktion auf Vorfälle für die IT-SecOps-Teams in einer Post-Breach-Situation zur Untersuchung und gerichtlichen Beweisführung. Die vor, während und nach dem Ereignis erfassten Daten können dazu beitragen, die Sicherheitslücken, verdächtigen Aktivitäten und die IP-Adresse des Angreifers einzugrenzen.

NEOX NETWORKS

Packet Capture

NEOXPacketFalcon Compact Capture Appliance

Kompakt | 100Gbps Capture-to-Disk | 300TB Speicher
Security-Forensik | Compliance | Out-of-Box Dashboards

- Verlustfreie Packeterfassung
- Dauerhaftes Capture-to-Disk bis zu 100Gbps
- High-Speed FPGA Capture-Karten
- Intelligentes & Kompressions-basiertes Capturing
- Bis zu 300TB Speicherkapazität
- HW-verschlüsselter (SED) Speicher
- Hardware RAID 0,5,6,00,50,60
- IEEE 1588v2 Precision Time Protocol
- Rackmountable
- Flexible Konnektivität durch SFP, SFP+, SFP28, QSFP+, QSFP28
- FPGA-basiertes 10 Nanosekunden Timestamping
- FPGA-basiertes Packet Slicing & Capture Filter
- FPGA-basierte Deduplication
- PCAP & PCAPNG Support
- Optionaler Transportkoffer

PACKETFALCON

neoxn.de/falconc

Incident Response | Netzwerkforensik | Troubleshooting

Compliance | Rechenzentrum | Service Provider

- Die NEOXPacketFalcon Compact Packet Capture Appliance ist eine leistungsstarke Lösung zur Aufzeichnung von Netzwerk-Paketdaten für Geschwindigkeiten von bis zu 100 Gbps (1Gbps, 10Gbps, 25Gbps, 40Gbps oder 100Gbps). Die integrierten Speicherkapazitätsoptionen umfassen 30TB bis 300TB Festplattenspeicher, je nach Anwendungsfall und Speicherdauer der Daten. Seine Flexibilität in Bezug auf mobile und stationäre Applikationen macht ihn zum idealen Begleiter für NetSecOps.
  Ein Hartschalentransportkoffer ist optional erhältlich.
- NEOXPacketFalcon ermöglicht es IT-NetOps- und AppOps-Teams, jederzeit auf historische Daten zuzugreifen, Datenströme für die Fehlersuche neu zu generieren und Analysen auf Sitzungs- oder Konversationsebene durchzuführen, was die Fehlersuche und die Mean-Time-To-Resolution (MTTR) von Kundenproblemen deutlich reduzieren kann.
- NEOXPacketFalcon ist eine unverzichtbare Lösung für die Netzwerk-Forensik und die Reaktion auf Vorfälle für IT-SecOps-Teams in einer Post-Breach-Situation zur Untersuchung und gerichtlichen Beweisführung. Die vor, während und nach dem Ereignis erfassten Daten können dazu beitragen, die Sicherheitslücken, verdächtigen Aktivitäten und die IP-Adresse des Angreifers einzugrenzen. Durch die Indizierung der Daten und Hardware/Software-Filter (Berkeley Packet Filter) ermöglicht NEOXPacketFalcon den SecOps-Teams, Angriffe schnell zu untersuchen und zu blockieren.

NEOX NETWORKS

Packet Capture

NEOXPacketGrizzly Capture Appliance

Modular & Skalierbar | 100Gbps Capture-to-Disk | 8PB Speicher
Security-Forensik | Compliance | Out-of-Box Dashboards

- Verlustfreie Packeterfassung
- Dauerhaftes Capture-to-Disk bis zu 100Gbps
- High-Speed FPGA Capture-Karten
- Intelligentes & Kompressions-basiertes Capturing
- Bis zu 8PB Speicherkapazität
- HW-verschlüsselter (SED) Speicher
- Hardware RAID 0,5,6,00,50,60 & ADAPT
- IEEE 1588v2 Precision Time Protocol
- Rackmountable
- Flexible Konnektivität durch SFP28, QSFP+, QSFP28
- FPGA-basiertes Nanosekunden Timestamping
- FPGA-basiertes Packet Slicing & Capture Filter
- FPGA-basierte Deduplikation
- PCAP & PCAPNG Support
- Optionaler Transportkoffer

PACKETGRIZZLY

neoxn.de/grizzly

Incident Response | Netzwerkforensik | Troubleshooting

Compliance | Rechenzentrum | Service Provider

- Die NEOXPacketGrizzly Modular Packet Capture Appliance ist eine leistungsstarke, branchenführende Lösung zur Aufzeichnung von Netzwerk-Paketdaten mit Geschwindigkeiten von bis zu 100Gbps (1Gbps, l0Gbps, 25Gbps, 40Gbps oder 100Gbps). Zu den Optionen für die Onboard-Speicherkapazität gehören 504TB bis 8PB Speicher und bis zu 4 Speichereinheiten, je nach Anwendungsfall und Dauer der Daten-speicherung. NEOXPacketGrizzly kann den Ausfall von bis zu 12 Laufwerken pro Einheit ohne Datenverlust verkraften und setzt damit eine hohe Messlatte für die Verfügbarkeit.

- NEOXPacketGrizzly unterstützt Ethernet-, VoIP- und Video-over-IP-Netzwerke sowie Analysen auf Sitzungs- oder Konversationsebene und ermöglicht es IT-NetOps- und AppOps-Teams, jederzeit auf historische Daten zuzugreifen, die Datenströme für die Fehlersuche neu zu erstellen und so FInger-Pointing und die Mean-Time-To-Resoluiton von Kundenproblemen (MTTR) merklich zu reduzieren.
Die hohe Erfassungsgeschwindigkeit und die große Speicherkapazität machen NEOXPacketGrizzly zu einer überlegenen Lösung für NetOps, um auf Netzwerkdaten von Tagen, Wochen und Monaten zurück-zugreifen, um Anomalien zu erkennen.

- NEOXPacketGrizzly ist eine unverzichtbare Lösung für die Netzwerk-Forensik und die Reaktion auf einen Vorfall für IT-SecOps-Teams in einer Situation nach einem Einbruch zur Untersuchung und zur gerichtli-chen Beweisführung. Die vor, während und nach dem Ereignis erfassten Daten können dazu beitragen, die Sicherheitslücken, verdächtigen Aktivitäten und die IP-Adresse des Angreifers einzugrenzen.
Durch die Indizierung der Daten und Hardware/Software-Filter (Berkeley Packet Filter) ermöglicht NEOX-PacketFalcon den SecOps-Teams, Angriffe schnell zu untersuchen und zu blockieren.

- Da verschlüsselter Datenverkehr immer häufiger zum Einsatz kommt, kann NEOXPacketGrizzly den ver-schlüsselten Datenverkehr erkennen und die verschlüsselte Nutzlast aus den Paketen herausschneiden, um die Speicherzeit zu verlängern. Dies wird im FPGA verarbeitet, ohne die Performance zu beeinträchti-gen.

NEOX**PacketFalcon** & NEOX**PacketGrizzly**

Stärkung der Cybersicherheit und Application Observability durch Integration historischer Netzwerkdaten und -forensik

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

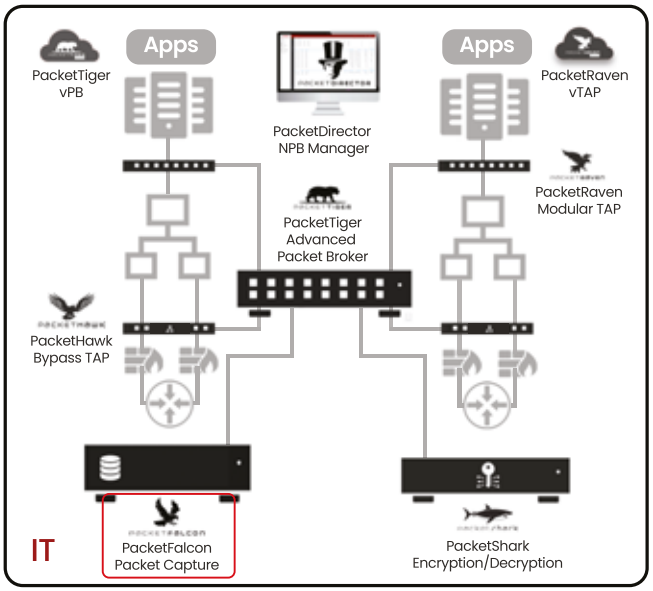
Deployment

SOC

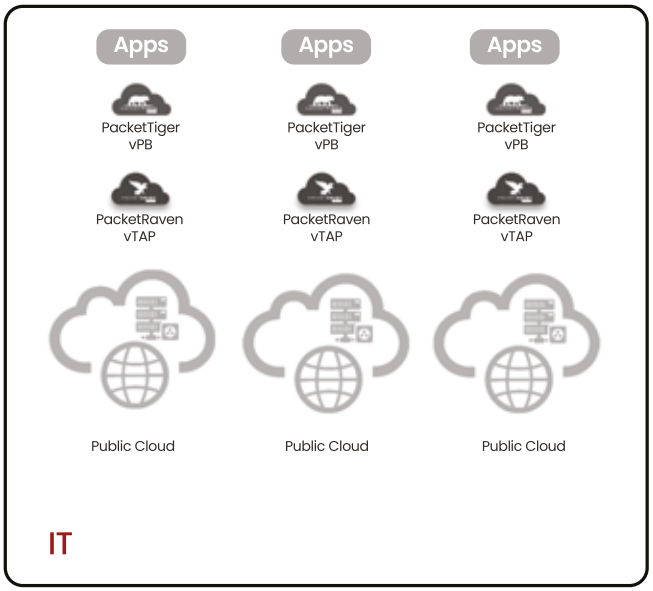
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

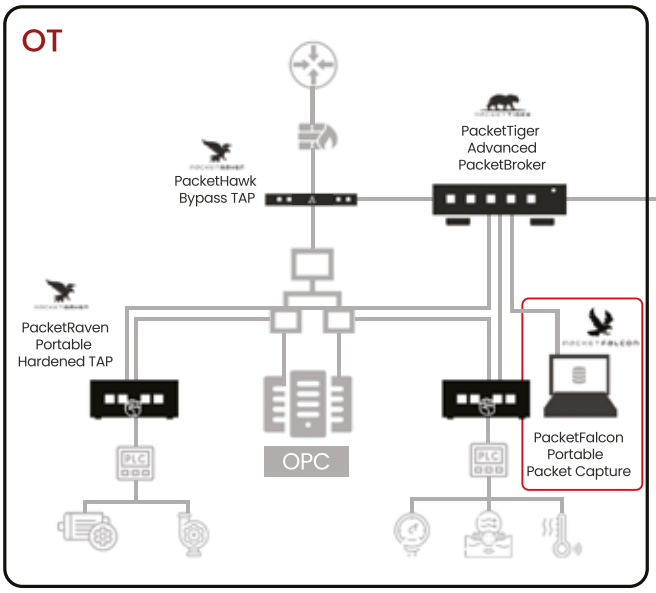
Application Issues, User Experiences, APM/NPM



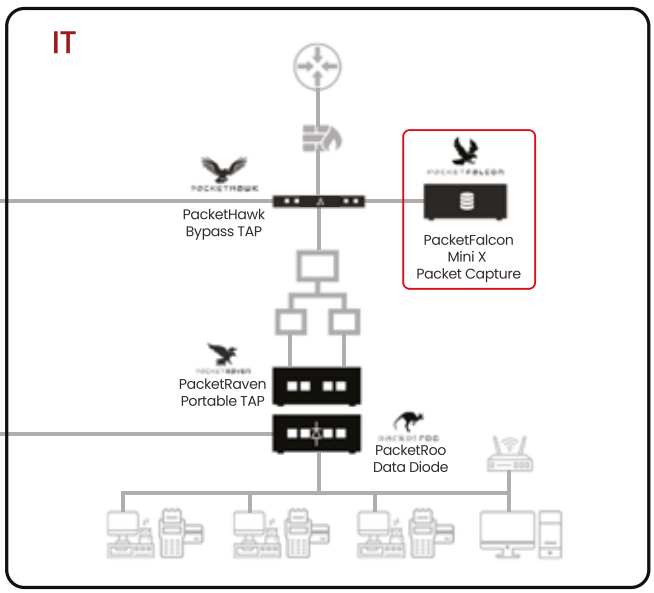
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX NETWORKS

NEOX**PacketFalcon** & NEOX**PacketGrizzly**

Stärkung der Cybersicherheit und Application Observability durch Integration historischer Netzwerkdaten und -forensik

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

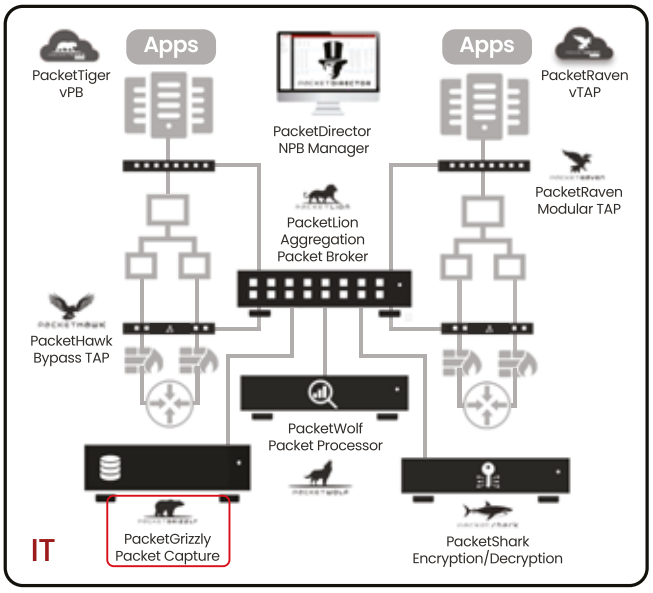
Deployment

SOC

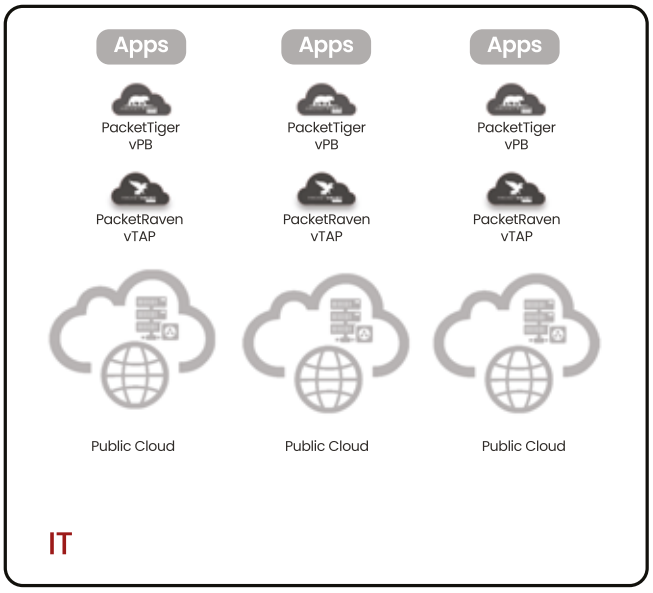
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

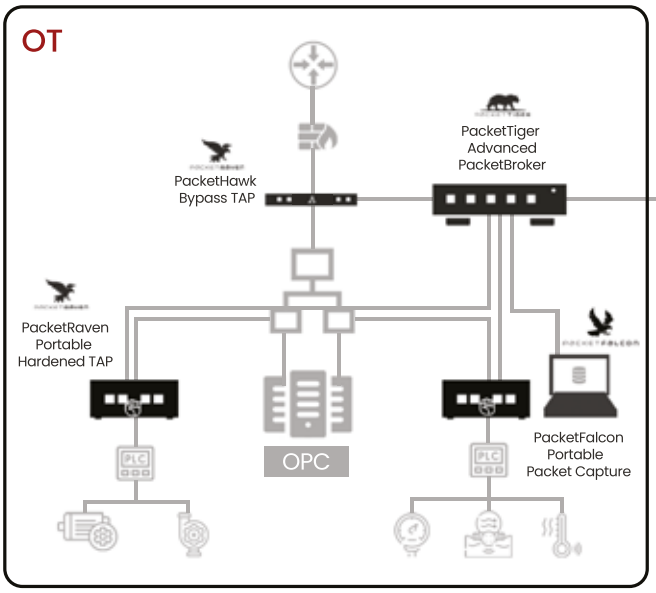
Application Issues, User Experiences, APM/NPM



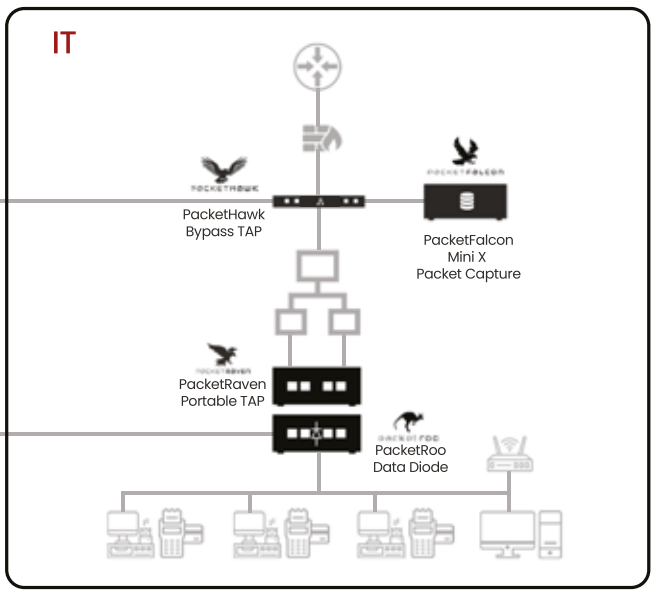
Rechenzentrum



Multi-Cloud



Industrieller Standort



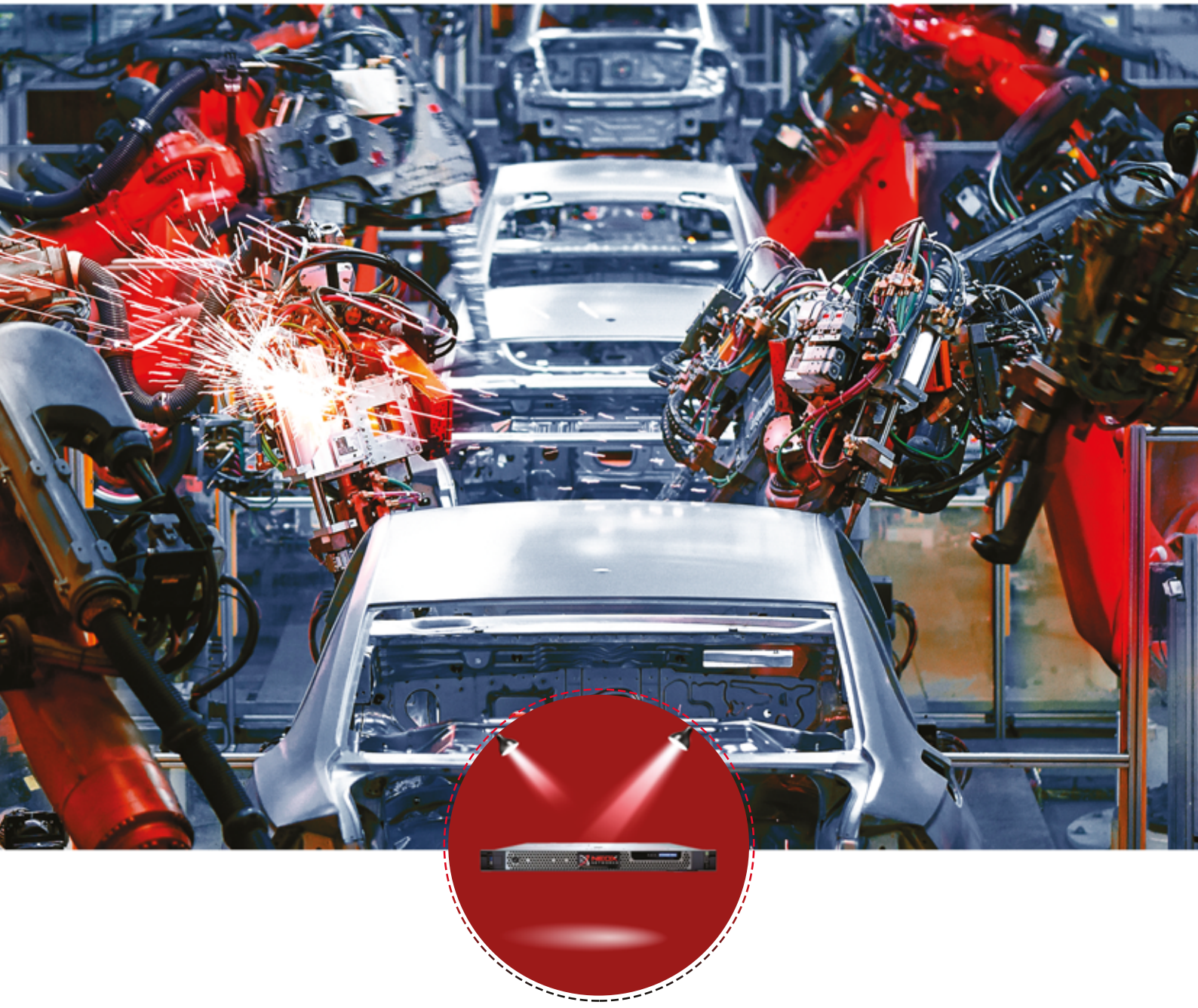
Zweigstelle

NEOX NETWORKS

PACKETWOLF

NEOX**PacketWolf Packet Processing**

Stärkung der Cybersicherheit und Application Observability durch die Integration erweiterter Paketverarbeitung und -analyse



NEOX NETWORKS

Packet Processor

NEOXPacketWolf Packet Processing

Fortschrittliches FPGA-basiertes Packet Processing
400Gbps Durchsatz | NetFlow und IPFIX Unstamped Export

- Bis zu 4x 100Gbps SFP28/QSFP28
- Bis zu 400Gbps
- FPGA-Design
- FPGA-basiertes Nanosekunden Timestamping
- FPGA-basierte Deduplication
- FPGA-basiertes Packet Slicing
- Protocol Header Stripping
- 100Gbps NetFlow & IPFIX Unsampled Export
- Flexible Konnektivität durch SFP, SFP+, SFP28, QSFP+, QSFP28
- Tunnel-Support (Encapsulation/ Decapsulation)
- Data Masking
- Extrem niedrige Latenz
- Suricata Unterstützung

PACKETWOLF

neoxn.de/wolf

NDR Support | Traffic Inspection | Troubleshooting

Tools Offload | Rechenzentrum | Service Provider

Eine Packet Processing Appliance besitzt eine fortschrittliche Architektur, um Netzwerkdaten auf der Ebene der einzelnen Pakete zu verarbeiten. Dies beinhaltet FPGA-basierte Technologie für arbeitsintensive, aber schnellere Suchvorgänge.
Eine Packet Processing Appliance kann als Ergänzung zu einem Network Packet Broker oder als eigenständiges Gerät in einer bestehenden Netzwerk-Monitoring-Infrastruktur eingesetzt werden.

- Die NEOXPacketWolf Advanced Packet Processing Appliance ist dank ihrer FPGA-basierten Hochleistungsarchitektur die ideale Plattform für die fortschrittliche Verarbeitung von Netzwerkdatenpaketen mit einem Durchsatz von bis zu 400Gbps pro Appliance.
- Der zu verarbeitende Datenverkehr wird normalerweise über einen Network Packet Broker wie die NEOXPacketLion-Serie oder Packet Broker von Drittanbietern eingespeist, kann aber auch aus anderen Quellen wie einem SPAN-Port oder einem Netzwerk-TAP stammen. Die verarbeiteten Daten werden vom NEOXPacketWolf auf demselben oder einem separaten Port an ein Monitoring-/Sicherheitstool weitergeleitet oder an die Quelle zurückgeschickt. Fortschrittliche Packet Broker wie die NEOXPacketTiger benötigen NEOXPacketWolf hingegen nicht zur Ergänzung, da sie über integrierte Paketverarbeitungsfunktionen verfügen.
- Die NEOXPacketWolf Advanced Packet Processing Appliance bietet mehrere fortschrittliche Funktionen zur Entlastung der Monitoring- und Observability-Tools durch Deduplizierung, erweiterte Filterung, Paketmaskierung, Packet Slicing, dynamisches und statisches Header-Stripping, Tunnel-Terminierung, VLAN-Tagging, L2-L3-L4-Loopback, PCAP-Ansicht, Replay und Edit.
- Darüber hinaus können Funktionen wie Packet Slicing und Packet Masking sicherstellen, dass rechtliche und Compliance-Anforderungen erfüllt werden. Insbesondere im Hinblick auf die DSGVO kann es notwendig sein, durch Packet Slicing die Benutzerdaten vor der Weiterleitung zu entfernen oder die persönlichen Informationen zu maskieren, da die Metadaten oft für eine Analyse ausreichen.

NEOX PacketWolf Packet Processing

Stärkung der Cybersicherheit und Application Observability durch die Integration erweiterter Paketverarbeitung und -analyse

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

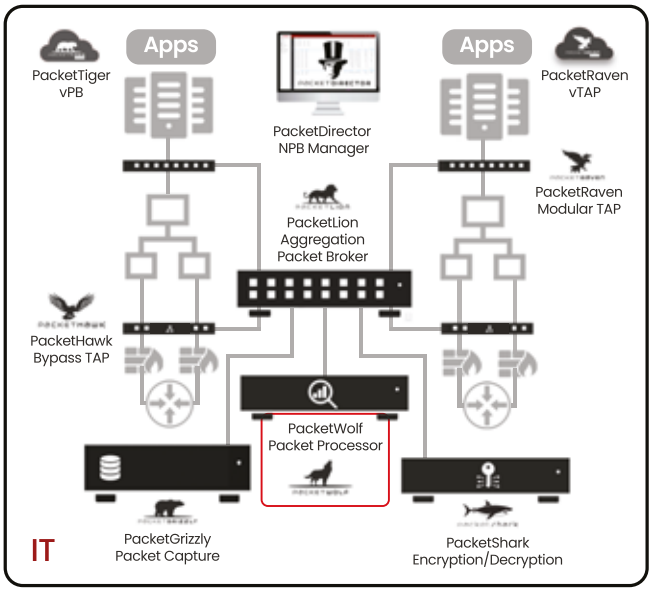
Deployment

SOC

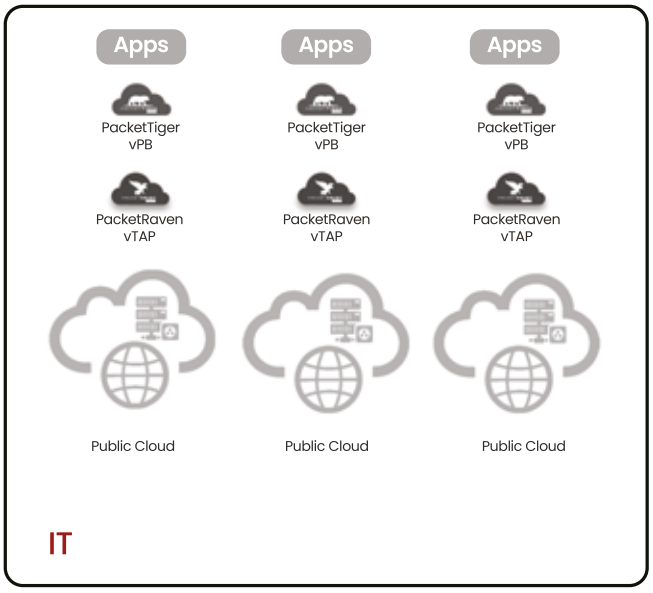
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

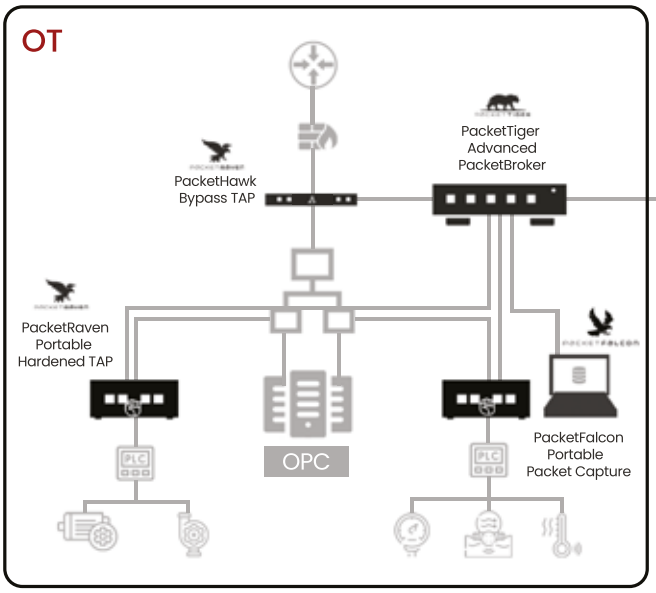
Application Issues, User Experiences, APM/NPM



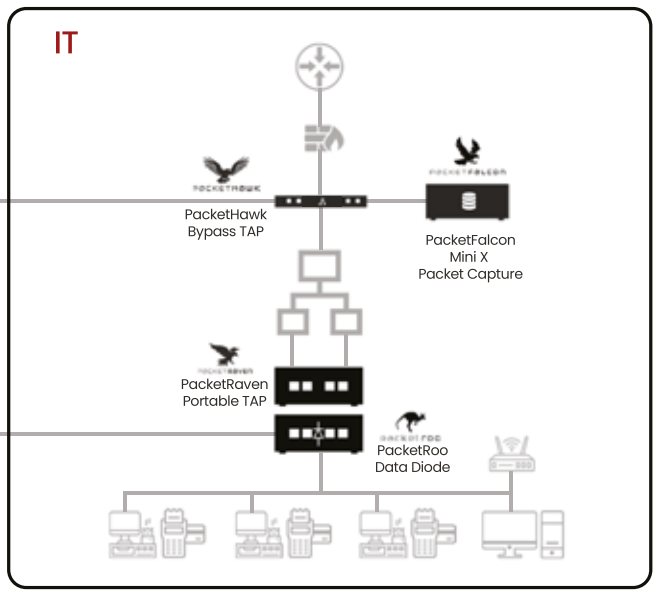
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX NETWORKS

packetshark

NEOXPacketShark Encryption & Decryption

Stärkung der Cybersicherheit und Application Observability durch Netzwerktransparenz in verschlüsseltem Datenverkehr

NEOX NETWORKS

Packet Processor

NEOX PacketShark Encryption & Decryption

TLS/SSL Traffic Visibility | Policy-Based Traffic Control
Zertifikate I Filtering & Bypass I Compliance

- TLS 1.3 & SSL Support
- SSL Decryption auf allen L4 Ports
- Behält 5-Tupel
- Bypass Funktionalität
- URL-Filtering
- Verteilung & Kontrolle von Zertifikaten
- Compliance & Datenschutz
- Unterstützt Forward Proxy & Reverse Proxy

packetshark

neoxn.de/shark

Cybersecurity | Betrugserkennung | Investigation

Rechenzentrum | Service Provider | Lawful Intercept

Eine Encryption/Decryption-Appliance bietet eine Komplettlösung zur Verbesserung der SSL-Infrastruktur, die Security-Devices Einblick in den TLS/SSL-verschlüsselten Datenverkehr gewährt und bestehende Sicherheitsinvestitionen optimiert. Sie unterstützt die richtlinienbasierte Verwaltung des Datenverkehrs und lässt sich problemlos in aktuelle Architekturen integrieren, während sie die Ver- und Entschlüsselung mit den neuesten Technologien im gesamten Sicherheitsrahmen zentralisiert.

- Der PacketShark ist eine modulare Lösung, die so konzipiert wurde, dass sie mit den ständig wachsenden Netzwerken Schritt hält, da sie die Möglichkeit bietet, NMC-Module zu verwenden, um die Portdichte bei Bedarf zu erhöhen. Um die Flexibilität weiter zu erhöhen, sind diese NMC-Module auch mit integrierter Bypass-Funktionalität erhältlich, die dem Benutzer die volle Kontrolle über die Netzwerkverbindungen überlässt. In Kombination mit einem externen PacketHawk Inline Bypass TAP und einem PacketLion Network Packet Brokern kann man sein Sicherheitsdesign unbegrenzt skalieren.
- Um ein Unternehmensnetzwerk effektiv vor internen und externen Bedrohungen zu schützen, ist eine Reihe von Security-Deevices erforderlich. Traditionell mussten Administratoren bei der Bewältigung von Sicherheitsherausforderungen verschiedene Produkte manuell miteinander verbinden, um einen "Security Stack" zu bilden. PacketShark lässt sich mit führenden Sicherheitsanbietern integrieren und ermöglicht den Einsatz innerhalb einer "sicheren Entschlüsselungszone", um das gesamte Netzwerk vor verschlüsselten Bedrohungen zu schützen.
- Die dynamische Dienstverkettung bietet einen flexibleren Ansatz, indem sie den Datenverkehr auf der Grundlage des Sicherheitsrichtlinienkontexts weiterleitet. Dadurch können bestimmte Arten von Datenverkehr durch maßgeschneiderte Dienstketten fließen, wie z. B. Layer-2- und Layer-3-Inline-Dienste, reine Empfangsdienste, ICAP und HTTP-Web-Proxy-Dienste, um die Sicherheit je nach Datenverkehrsanforderungen zu optimieren. PacketShark verwendet eine fortschrittliche URL-Klassifizierung, um den Datenverkehr von Domänen zu kategorisieren und so eine selektive Umgehung der Entschlüsselung zu ermöglichen, um sensible Daten wie medizinische oder finanzielle Daten zu schützen und die Einhaltung von Standards wie HIPAA zu gewährleisten. Darüber hinaus steigert die URL-Filterfunktion die Produktivität der Mitarbeiter und mindert Risiken, indem sie den Zugriff auf bösartige Websites blockiert, einschließlich solcher, die mit Malware, Spam und Phishing in Verbindung stehen.

NEOX PacketShark Encryption & Decryption

Stärkung der Cybersicherheit und Application Observability durch Netzwerktransparenz in verschlüsseltem Datenverkehr

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

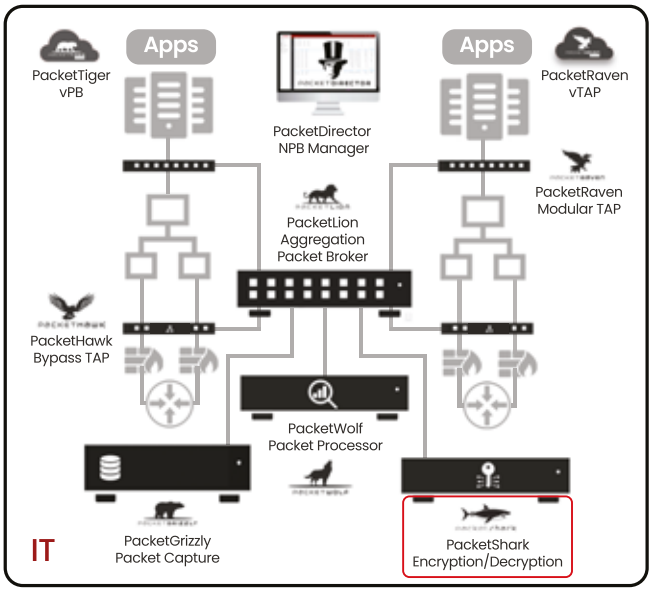
Deployment

SOC

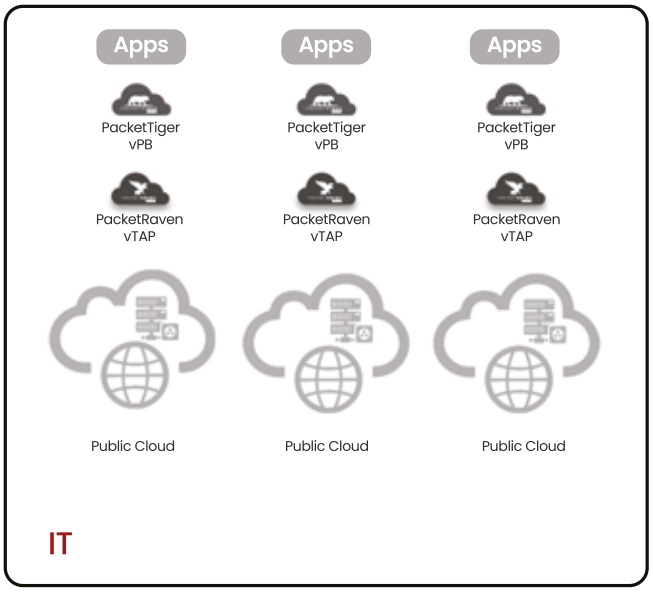
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

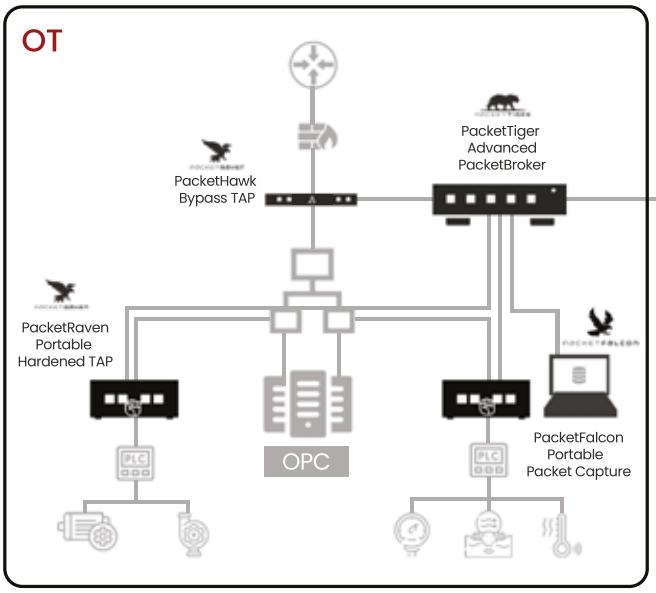
Application Issues, User Experiences, APM/NPM



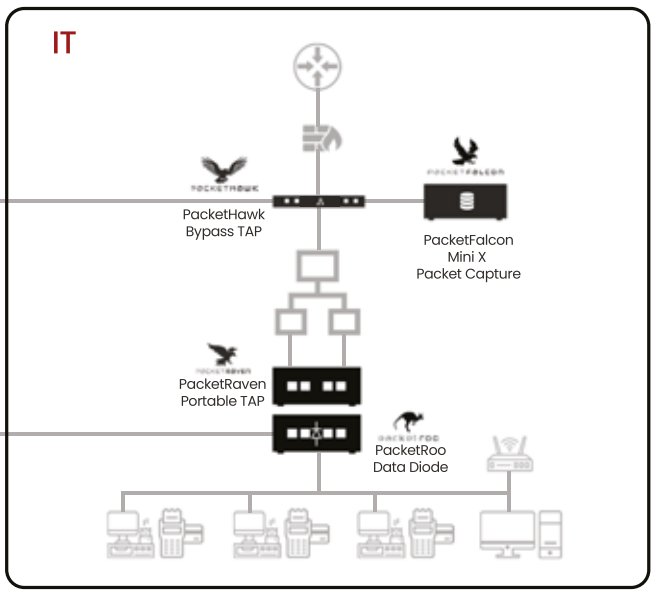
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX NETWORKS

PACKETLION PACKETTIGER

NEOX**PacketLion** & NEOX**PacketTiger** **Network Packet Broker Familie**

Stärkung der Cybersicherheit und Application Observability durch Konsolidierung und Weiterleitung der richtigen Daten an die richtigen Tools

NEOX NETWORKS

Packet Broker

NEOXPacketLion Packet Broker Familie

Hochperformante Aggregation | Non-Blocking Architektur
Hohe Portdichte | Inline Bypass oder Out-of-Band | Flexibles Stacking

- Bis zu 400Gbps
- Port Splitting & Port Labeling
- L3GRE Tunneling Protocol
- Stacking möglich
- Digital Diagnostics Monitoring
- Radius & TACACS
- Flexible Portzuordnung
- Tunnel Filtering
- Aggregation & Regeneration
- Benutzerdefinierte Filterregeln
- MPLS Stripping
- Timestamping
- Packet Slicing
- 8GB Deep Buffers

PACKETLION

neoxn.de/lion

Cybersecurity | NDR Feed | Troubleshooting

Rechenzentrum | Service Provider | Lawful Intercept

Ein Network Packet Broker (NPB), auch bekannt als Network Monitoring Switch, aggregiert Datenströme von Netzwerk-TAPs, die über die Hybrid-Cloud-Infrastruktur verteilt sind, verarbeitet sie, um die Daten zu filtern und zu manipulieren, damit sie im richtigen Format an die richtigen Ziele/Tools zur Überwachung und Analyse weitergeleitet werden.

- NEOXPacketLion Network Packet Broker fungieren als hochdichte Aggregationsschicht und als Brücke zwischen den Netzwerkdaten-Zugangspunkten, d.h. den TAPs, und der Tool-Schiene, wie z.B. Sicherheits- (NIDS, NIPS, NDR, SIEM), Forensik- (Packet Capture) und Performance-Monitoring-Tools (APM, NPM).
- NEOXPacketLion fungiert auch als Gateway, um Netzwerkgeschwindigkeiten von bis zu 400 Gbps mit niedrigeren Geschwindigkeiten auf der Toolseite zu verbinden, und unterstützt je nach Version alle gängigen Transceiver-Standards (SFP, SFP+, QSFP-DD)
- NEOXPacketLion verwendet spezielle ASIC-Hardware zur Unterstützung einfacher oder komplexer Datenfilterregeln, um einen optimierten Datenfluss und die richtigen Daten für die richtigen Analysetools zu gewährleisten. Damit können Sie unerwünschte Datenpakete oder ganze Datenströme herausfiltern und so die Gesamtlast und den Tool-Wildwuchs reduzieren und Investitionen verlängern.
  - Flexible Portzuordnung (1:1, N:N, N:1, 1:N)
  - Unterstützt Filterregeln (MAC, VLAN, IPv4/IPv6, TCP/UDP, DSCP, TCP Flags, MPLS, Ingress, Egress Filtering) innerhalb eines Tunnels (GTP, L2TP, MPLS, GRE, PPPoE, und VxLAN)
  - 8 GB Deep Buffer zur Vermeidung von Paketverlusten aufgrund von Micro Bursts
  - Unterstützt benutzerdefinierte Filterregeln (UDF)

NEOX NETWORKS

Packet Broker

NEOXPacketTiger Packet Broker Familie

Fortschrittliche Features | Deep Packet Inspection Application Metadata | NetFlow und IPFIX Export

- Bis zu 8x 100Gbps
- NEOXPacketLion Paritäts-Features
- GTP Correlation
- Data Masking
- Deduplication
- Advanced Filtering
- NetFlow/IPFIX Support
- Deep Packet Inspection
- Tunnel Support
- Packet Capture & Replay
- GTP Tunneling & IMSI Filtering

PACKETTIGER

neoxn.de/tiger

Cybersecurity | NDR Feed | Troubleshooting

Rechenzentrum | Service Provider | Lawful Intercept

- NEOXPacketTiger Advanced Network Packet Broker erlauben volle Flexibilität beim Parsen von Netzwerk-Paket-Headern und bei der Verarbeitung von Payloads und bieten fortschrittliche Technologien zur Modifizierung und Optimierung dieser Pakete.
- Fortschrittliche Funktionen wie IPv6-Filterung im GTP-Tunneling, Regex, Deep Packet Inspection (DPI) und anwendungsbasierte Metadatenextraktion werden unterstützt.
- NEOXPacketTiger verwendet moderne, leistungsstarke, modulare und skalierbare COTS-Hardware, die für die gewünschte Verarbeitungskapazität konfiguriert werden kann. Dieser einzigartige Ansatz beseitigt Hardware-Leistungsbeschränkungen und ermöglicht eine bessere Skalierung und Abstimmung zwischen Hardware- und Performance-Anforderungen. Der Medientyp und die Geschwindigkeit des Netzwerks spielen keine Rolle, da der NEOXPacketTiger alle wichtigen Typen unterstützt (RJ45/SFP/SFP+/QSFP+/QSFP28 Ports).
- Die fortschrittliche Paketverarbeitung des NEOXPacketTiger ermöglicht es Ihnen, im Vergleich zu gewöhnlichen Network Packet Brokern granularer zu arbeiten und tiefer in einzelne Pakete hineinzuschauen. Selbst ressourcenintensive Szenarien wie das Entfernen von Duplikaten (Dedup) im Netzwerk, oder das Maskieren oder Schwärzen von Inhalten in den einzelnen Paketen stellen kein Problem dar.
- NEOXPacketTiger Advanced Network Packet Broker sind in verschiedenen Kategorien erhältlich: Desktop Appliances, Network Appliances und Server, die eine breite Palette von Lösungen ermöglichen.
- Alles in allem verfügen die NEOXPacketTiger Next-Gen Advanced Network Packet Broker über deutlich mehr Funktionen und Merkmale für fortschrittliche Anwendungen in unternehmenskritischen Rechenzentren.

NEOX NETWORKS

Packet Broker

NEOXPacketTigerVirtual Virtual Packet Broker

Hybrid-Cloud | Multi-Cloud | On-Prem Virtual Environments
Inline oder Out-of-Band | Stateful Filtering | Load Balancing

- Virtuelle & Cloud Umgebungen
- GTP Correlation & Filtering
- Inner IP LB & Tunnel Filtering
- OSI L2-L4 & RegEx Filtering
- Benutzerdefinierte Filter
- Header Stripping & Editing
- Deduplication
- Data Masking
- Packet Slicing
- Metadata Extraction
- Timestamping
- Capture & Replay
- NetFlow/IPFIX
- NEOX Device Manager

PACKETTIGER VIRTUAL

neoxn.de/vtiger

Cybersecurity | NDR Feed | Troubleshooting

Cloud | Rechenzentrum | Service Provider

Ein Virtual Packet Broker (vPB) funktioniert genau wie ein physischer Network Packet Broker, der auf einem Standard-Hypervisor im virtualisierten Rechenzentrum oder in der Cloud laufen kann. Er kann den Netzwerkverkehr zwischen den virtuellen Maschinen (VM) in Ost-West-Richtung aggregieren, filtern und verarbeiten und an die Monitoring- und Analyse-Tools weiterleiten, was normalerweise einen toten Winkel darstellt.

- NEOXPacketTigerVirtual bietet eine vielseitige Virtual Network Packet Broker-Lösung, die den Bedarf an erhöhter Transparenz in virtualisierten Umgebungen wie bspw. Software-Defined Data Centers (SDDC) und öffentlichen/privaten Clouds erfüllt und so blinde Flecken beseitigt. So erhalten Sie eine durchgängige Transparenz der Hybrid-Cloud/Multi-Cloud-Umgebung.
- NEOXPacketTigerVirtual kann als Docker-Container oder als virtuelle Appliance eingesetzt werden und ist für AWS, Microsoft Azure und Google Cloud validiert und einsetzbar. Er kann Netzwerkdatenströme von mehreren NEOXPacketRavenVirtual vTAPs innerhalb einer VPC sammeln und die Verarbeitung und Weiterleitung von Cloud-Netzwerkdaten optimieren, wodurch die Cloud-Rechnungen reduziert und die Sicherheit erhöht wird.
- NEOXPacketTigerVirtual kann ähnliche Vorteile in einem virtuellen Netzwerk vor Ort bieten, z.B. in einer VMware-Umgebung. Da die meisten Malware-Angriffe über den Ost-West-Verkehr im Rechenzentrum erfolgen, werden Sicherheitslücken und blinde Flecken erheblich reduziert.
- NEOXPacketTigerVirtual kann auch in einem virtualisierten Zweigstellennetz eingesetzt werden, um Transparenz zu schaffen, z.B. bei SDWAN-Verbindungen.

  - Erweitern Sie Ihre Netzwerktransparenz für den virtuellen und Cloud-Netzwerkverkehr
  - Aggregieren Sie den Datenverkehr mehrerer vTAPs aus VPC-Clouds oder VMware VMs
  - Leiten Sie den virtuellen Netzwerkverkehr an eine Monitoring/Observability-Lösung vor Ort oder an eine VPC-Cloud weiter
  - Lasten für virtuelle und physische Überwachungstools durch Filtern von Daten gleichmässig verteilen und Optimieren

NEOX**PacketLion** & NEOX**PacketTiger**

Stärkung der Cybersicherheit und Application Observability durch Konsolidierung und Weiterleitung der richtigen Daten an die richtigen Tools

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

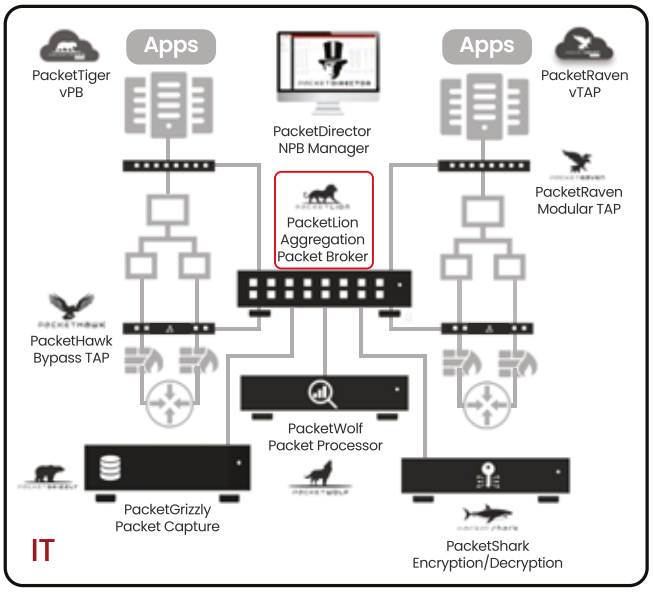
Deployment

SOC

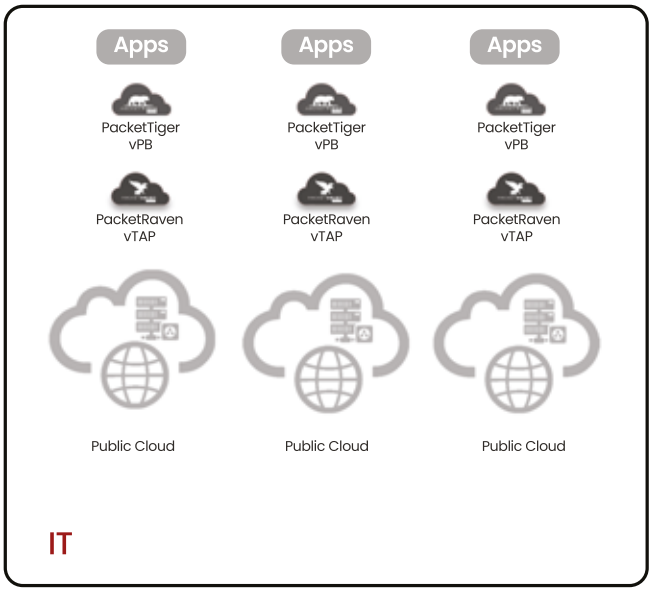
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

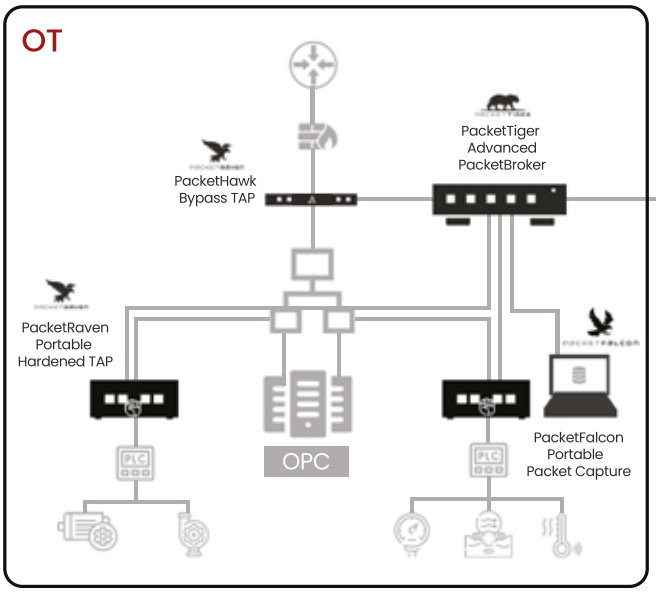
Application Issues, User Experiences, APM/NPM



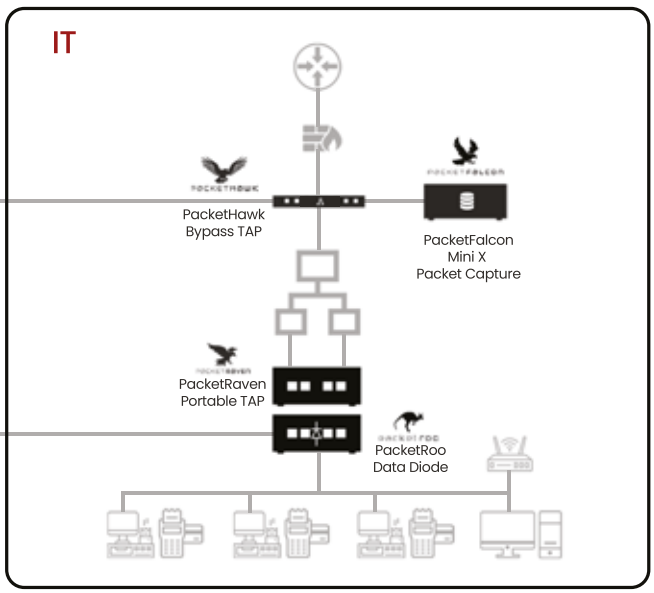
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX**PacketLion** & NEOX**PacketTiger**

Stärkung der Cybersicherheit und Application Observability durch Konsolidierung und Weiterleitung der richtigen Daten an die richtigen Tools

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

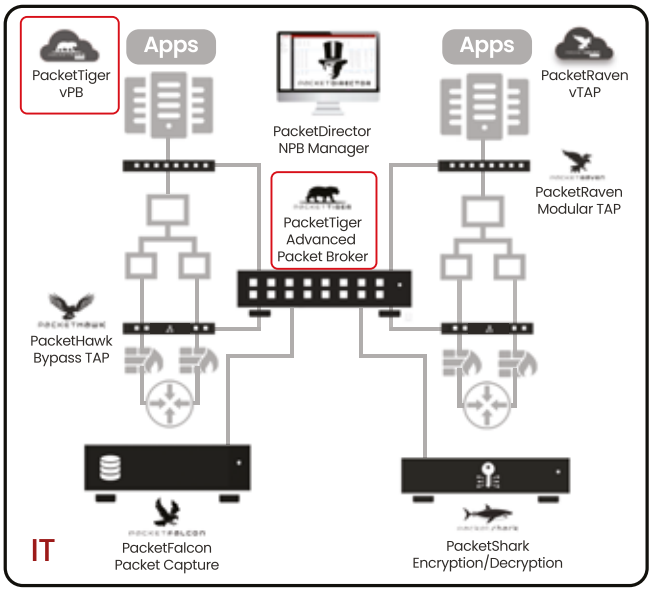
Deployment

SOC

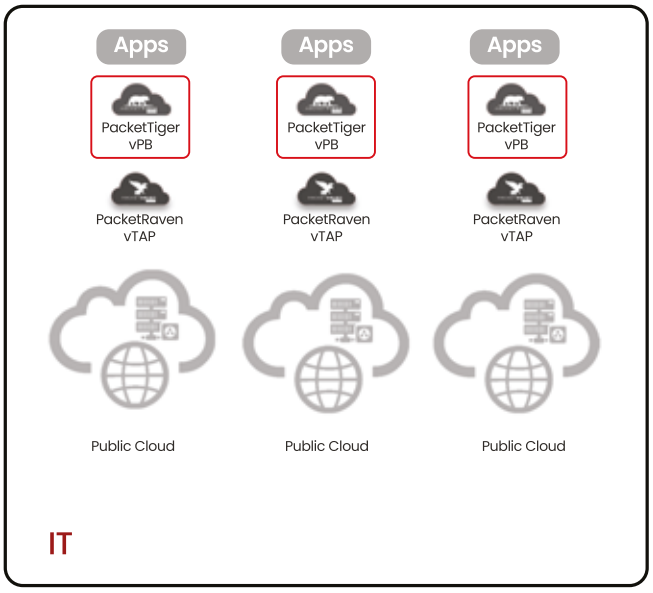
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

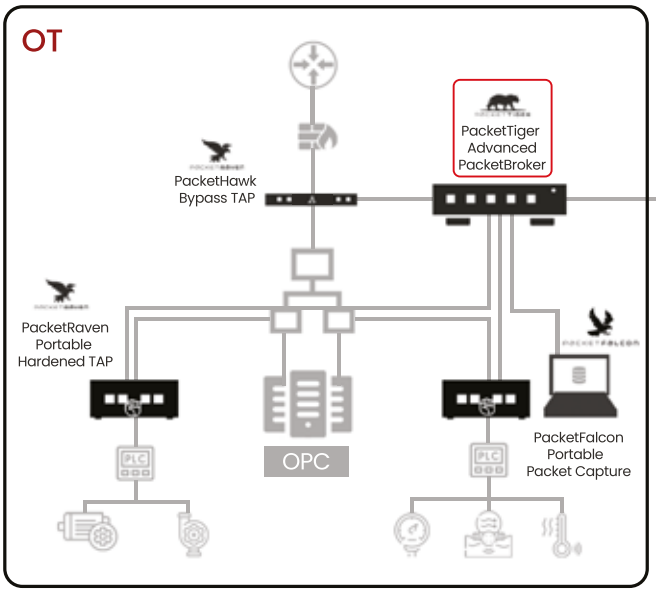
Application Issues, User Experiences, APM/NPM



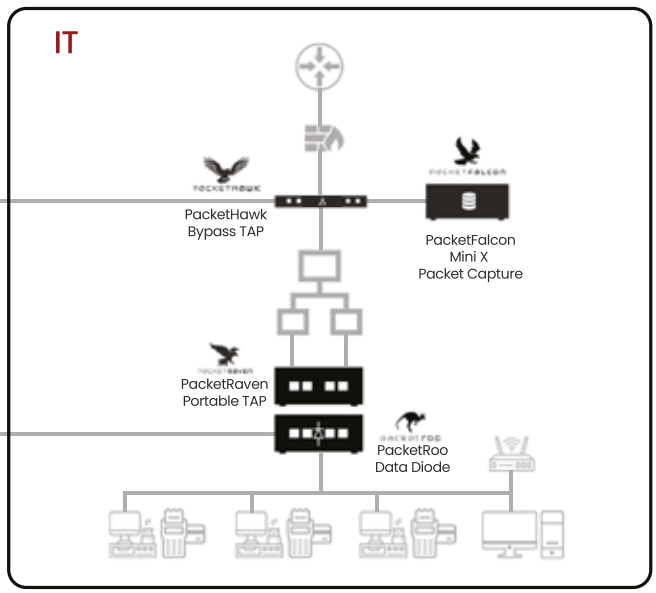
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX NETWORKS

PACKETDIRECTOR

NEOXPacketDirector Packet Broker Manager

Stärkung der Cybersicherheit und der Application Observability durch zentrale Verwaltung der richtigen Daten mit den richtigen Tools

NEOX NETWORKS

Netzwerkmanagement

NEOXPacketDirector Packet Broker Manager

Zentrales Management für bis zu 100 Devices
Bulk Provisioning & Regeln | Auto-Discovery | Netzwerkstatistiken

- Auto Discovery
- Statistik-Sammlung
- Bulk Operation
- Alarm-Sammlung
- Elastic Datenbank
- Grafische Dashboards
- Email Benachrichtigungen
- Planer für Bulk Tasks
- Upgrade Manager
- Konfigurations-Backup

PACKETDIRECTOR

neoxn.de/dir

Cybersicherheit | NDR-Feed | Troubleshooting

Cloud | Rechenzentrum | Service Provider

NEOXPacketDirector Advanced Features:

- Software-basierte Lösung, als VM und Container verfügbar
- Ein einziges Tool für die zentrale Verwaltung von physischen und virtuellen Neox Packet Brokern
- Planer für Bulk Operations und Tasks für verschiedene Geräte (Konfiguration, Backup, Upgrade, Reboot, Scripting)
- Zentralisierte Filter- und Regelverwaltung pro Gerät und geräteübergreifende Regeln via Clustering
- Clustering von bis zu 100 NEOX Network Packet Brokern in einer einzigen Einheit, die die Definition von Richtlinien zwischen vernetzten Geräten ermöglicht

- NEOXPacketDirector ist ein zentrales Managementsystem für NEOXPacketLion, NEOXPacketTiger und NEOX-PacketTigerVirtual Network Packet Broker, mit dem Sie diese übersichtlich bereitstellen, überwachen und verwalten können. Dadurch wird die Arbeitsbelastung der NetOps- und SecOps-Teams in großen, verteilten, hybriden oder standortübergreifenden Umgebungen erheblich reduziert.
- NEOXPacketDirector ist eine softwarebasierte Lösung, die als VM oder Container vor Ort oder in der Cloud implementiert werden kann.
- NEOXPacketDirector ermöglicht die automatische Erkennung und Verwaltung hunderter sowohl physischer, als auch virtueller Neox Network Packet Broker. Netzwerkstatistiken und Verkehrstelemetrie werden in einer Elastic Datenbank gespeichert und können in Echtzeit über Kibana- und Grafana-Dashboards grafisch visualisiert werden. Benutzer können verschiedene Ereignisse und Trigger pro Gerät definieren, je nach geräteübergreifenden Ereignissen. Alarme und Ereignisse lösen E-Mail-Benachrichtigungen via NEOXPack-etDirector aus.

NEOX PacketDirector Packet Broker Manager

Stärkung der Cybersicherheit und der Application Observability durch zentrale Verwaltung der richtigen Daten mit den richtigen Tools

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

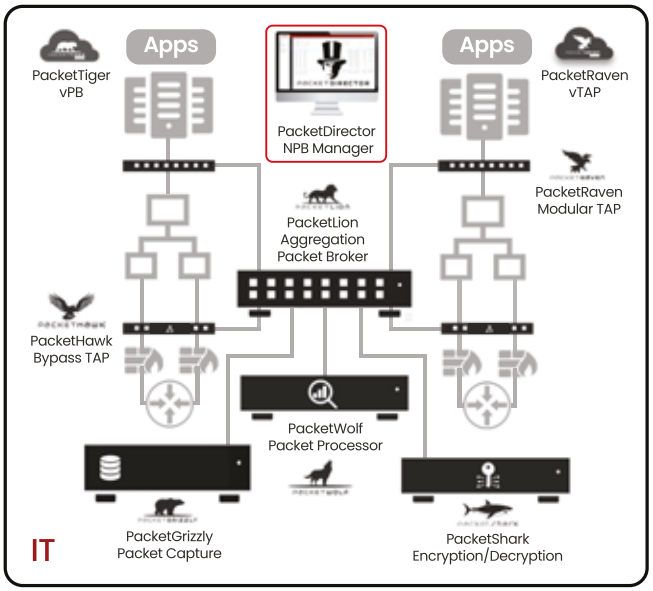
Deployment

SOC

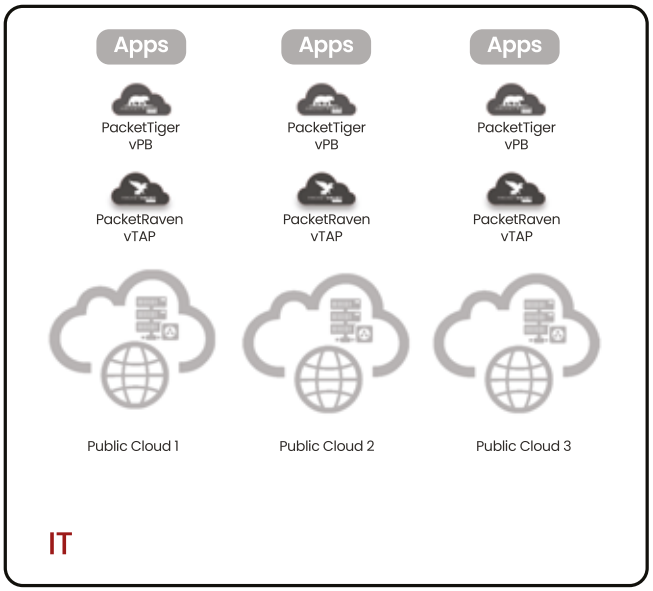
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

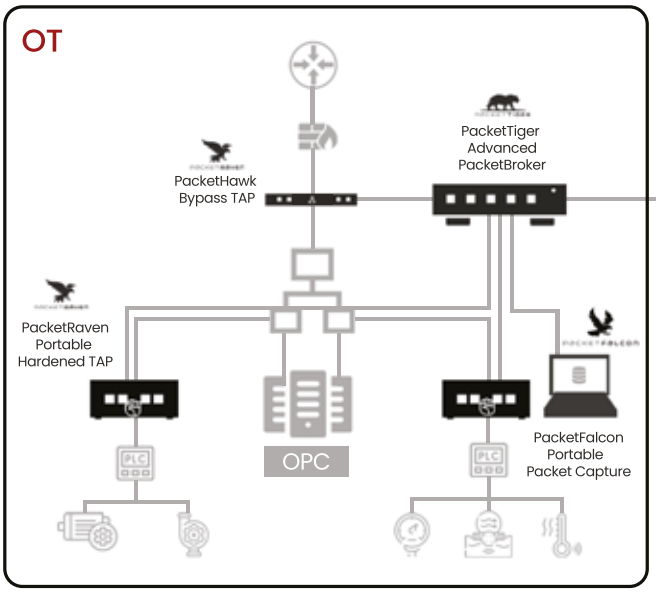
Application Issues, User Experiences, APM/NPM



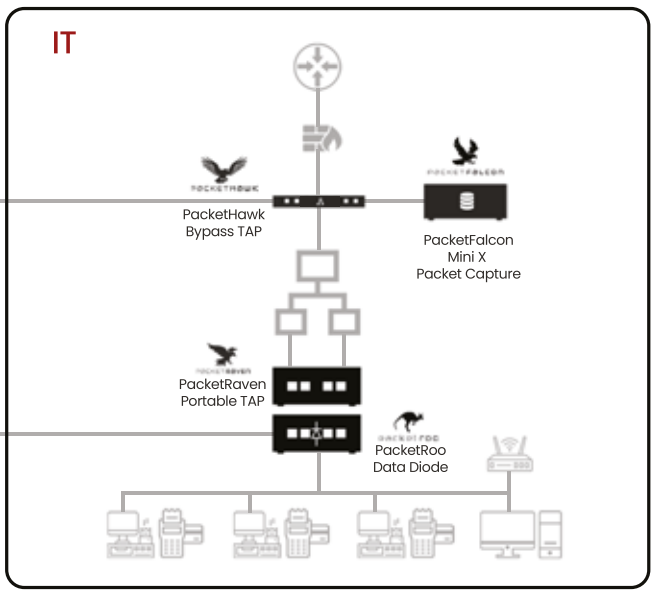
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX NETWORKS

PACKETHAWK

NEOX PacketHawk Inline Bypass-TAP

Stärkung der Cybersicherheit und Application Observability durch Integration von Network Traffic Rerouting in Echtzeit

NEOX NETWORKS

Bypass-TAP

NEOXPacketHawk Inline Bypass-TAP

Bis zu 100G | Modular | Service Chaining | Filtering Load Balancing | Inline oder Out-of-Band

- Bis zu 4x 100Gbps QSFP+/QSFP28
- Modulares Chassis
- Service Chaining
- Filtering
- Breakout & Aggregation TAP Modi
- Benutzerspezifischer Heartbeat
- Unsichtbar für Hacker
- 100% Netzwerkdaten
- Flexibel einsetzbar
- Ausfallsicherung bei Stromausfall

PACKETHAWK

neoxn.de/hawk

Cybersecurity | NDR Feed | Incident Response

Compliance | Rechenzentrum | Service Provider

Ein Inline Bypass-TAP ist unverzichtbar, um die unterbrechungsfreie Bereitstellung von Data-in-Motion aufrechtzuerhalten und einen nahtlosen Netzwerk- und Sicherheitsbetrieb ohne Kompromisse zu gewährleisten. Er dient als ausfallsicherer Mechanismus für den Fall, dass ein "Inline"-Netzwerkknoten oder ein Sicherheitstool ausfällt oder Wartungsarbeiten durchgeführt werden, so dass der Datenverkehr ohne Unterbrechung über eine alternative geschützte Route mit einem Backup-Set von Appliances und Tools weiterfließen kann.

- Der NEOXPacketHawk Inline Bypass-TAP ermöglicht dem Netzwerkverantwortlichen die Aufrechterhaltung einer unterbrechungsfreien Konnektivität und eines reibungslosen Netzwerkbetriebs während etwaiger Ausfallzeiten. Er fungiert als Fail-Safe-Mechanismus, wenn Geräte ausfallen oder gewartet werden müssen, so dass der Datenverkehr im Hauptrechenzentrum von Norden nach Süden ohne Unterbrechung weiterfließen kann. Außerdem bietet es die Flexibilität, den Datenverkehr zu Sicherheitsüberwachungs- oder Analysezwecken umzuleiten, ohne die Performance des Netzwerks zu beeinträchtigen.

- NEOXPacketHawk sendet in regelmäßigen Abständen Heartbeat-Impulse an die Netzwerkknoten der Inline Security Appliances und die Visibility-Tools (z.B. eine Netzwerk-Firewall, WAF, NIDS und NIPS) und empfängt die Antworten. Wenn der Heartbeat ausbleibt, weiß er, dass die Appliance nicht mehr funktionsfähig ist. NEOXPacketHawk umgeht dann automatisch die Appliance, leitet den Netzwerkverkehr um und stellt sicher, dass die Datenpakete weiterhin zu ihren Zielen fließen. NEOXPacketHawk bietet überlegene Bypass-TAP-Funktionalität in Hardware und auf der eigentlichen Leitungsebene. Das bedeutet, dass er den Datenverkehr im Falle eines Ausfalls eines Netzwerkknotens oder Tools physisch umleitet.

- Mit NEOXPacketHawk können NetOps und SecOps Wartungsarbeiten und Upgrades durchführen oder Sicherheits- oder Observability-Tools in aller Ruhe austauschen, ohne den Betrieb des Produktionsnetzwerks zu beeinträchtigen oder Ausfallzeiten zu verursachen.Dies reduziert das Risiko und die Arbeitsbelastung und erhöht die Geschäftskontinuität und Verfügbarkeit.

  - 6 Bypass-Modi: automatisch, halbautomatisch, Inline erzwingen, Bypass erzwingen, Tap-separate, Tap-aggregate
  - Link Loss Detection (LLD) im Falle eines Ausfalls der Netzwerkverbindung
  - Redundantes Bypass-Verhalten bei Ausfall eines Bypass-TAPs: Active Bypass, Passive Bypass
  - Unterstützt TAP-Modus: Net A, Net B Traffic Any-to-Any-Mapping
  - Unterstützt Mirror-Modus: Zuordnung von Inline 1 zu Inline 2, Inline 2 zu Inline 1 Port-Verkehr
  - Filterung nach Inline Port IP, Port: einschließen oder ausschließen

NEOX NETWORKS

NEOX PacketHawk Inline Bypass-TAP

Stärkung der Cybersicherheit und Application Observability durch Integration von Network Traffic Rerouting in Echtzeit

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

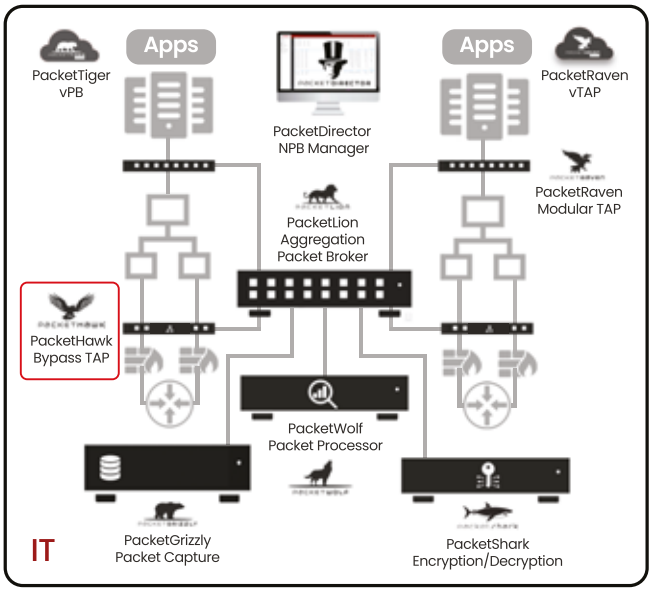
Deployment

SOC

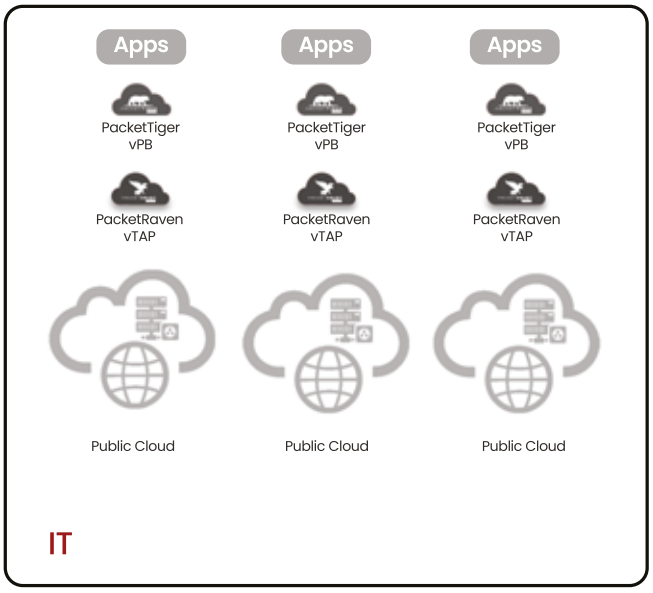
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

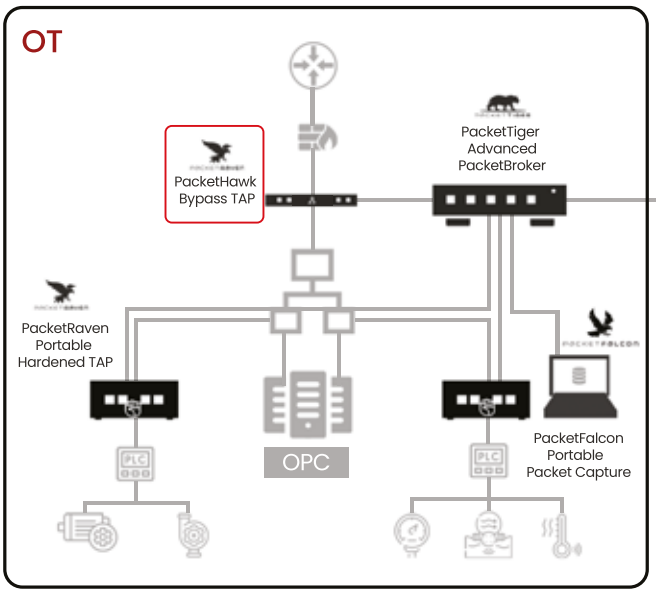
Application Issues, User Experiences, APM/NPM



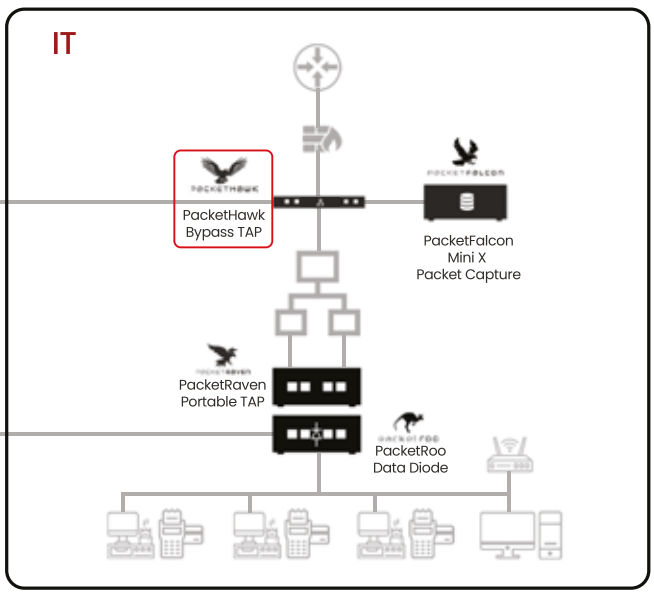
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX NETWORKS

PACKETRAVEN

NEOX**PacketRaven Netzwerk-TAP Familie**

Stärkung der Cybersicherheit und Application Observability durch Integration von Network-Wire-Data-Intelligence in Echtzeit

NEOX NETWORKS

Netzwerk-TAPs

NEOXPacketRaven Portable Netzwerk-TAPs

Volle Netzwerktransparenz bis 400G
FPGA-Chipsatz | Datendioden-Funktion | Redundante PSUs

- Bis zu 400Gbps
- Volle Netzwerk-transparenz
- Keine Beeinträchtigung des Datenverkehrs
- 100% Netzwerkdaten
- Unsichtbar für Angreifer
- Kein Netzwerkzugriff über den Monitoring-Port
- Flexibel einsetzbar
- Plug-n-Play
- Ausfallsicherung bei Stromausfall
- PoE+ Power over Ethernet
- Redundante Stromversorgung
- Verschiedene Split Ratios
- Schnell und präzise
- Unterstützt Jumbo Frames
- Gehärtete Version verfügbar

PACKETRAVEN

neoxn.de/ptap

Cybersecurity | NDR Feed | Incident Response

Compliance | Außenstelle | Industrieanlage

Netzwerk-TAPs sind Entkopplungselemente für den sicheren und zuverlässigen Abgriff von Netzwerkdaten in optischen und kupferbasierten Netzwerken. Die TAPs werden in die zu überwachende Netzwerkleitung eingeschleift und leiten den gesamten Datenverkehr ohne Unterbrechung oder Paketverlust weiter.

- Mit den NEOXPacketRaven Netzwerk-TAPs erhalten Sie permanenten Zugriff auf den Netzwerkverkehr mit bis zu 400 Gbps, für Observability in der Hybrid-Cloud, Performance von Applikationen und Sicherheitstools, und liefern 100% zuverlässige Netzwerkdaten.
- NEOXPacketRaven TAPs sind für Angreifer unauffindbar und da sie sich auf OSI-Schicht-1 befinden, haben sie keine MAC/IP-Adresse. Da die Integrität der ausgehenden Daten unverändert bleibt, werden sie für die Netzwerkforensik, Cybersicherheit, Reaktion auf Zwischenfälle und Überwachung eingesetzt.
- NEOXPacketRaven TAPs bieten einen aktiven Monitoring-Port, der wie eine "Datendiode" wirkt und die Monitoring-Ports physisch von den Netzwerk-Ports isoliert. Der Zugriff auf das Netzwerk über die Monitoring-Ports wird hardwaremäßig verhindert, so dass kein Backdoor-Zugang möglich ist.
- NEOXPacketRaven Portable TAPs sind optional auch in vorkonfigurierten "gehärteten" Versionen für Hochsicherheitsanwendungen erhältlich, sind IEC 62443 zertifiziert und mit verschlüsselter Firmware, Sicherheitssiegeln und Sicherheitsschrauben gegen unerwünschte Öffnungen ausgestattet.
- NEOXPacketRaven TAPs mit passiven Monitoring-Ports sind auch in einer besonders sicheren Version erhältlich. Diese sicheren Glasfaser-TAPs verfügen sowohl über einen zusätzlichen optischen Isolator (Datendiode) als auch über einen optischen Filter, um unerwünschte eingehende Lichtsignale am Monitoring-Port zu blockieren und so das Netzwerk vor Kompromittierung zu schützen.
- Für höchste Zuverlässigkeit verfügen alle NEOXPacketRaven TAPs mit aktiven Monitoring-Ports über redundante Stromversorgungen, können aber auch mit 12-48V Gleichspannung und in einigen Fällen mit PoE betrieben werden. Fiber-TAPs hingegen benötigen keinerlei Stromversorgung.
- Die vielseitigen NEOXPacketRaven können als portable TAPs verwendet oder mit einem Rack-Montage-Kit in einem 19"-Rack für Rechenzentren oder mit einem DIN-Schienenclip auf einer DIN-Hutschiene installiert werden.

NEOX NETWORKS

Netzwerk-TAPs

NEOX**PacketRaven Portable Hardened TAPs**

High-Security Netzwerk-TAPs | KRITIS approved & IEC 62443 zertifiziert
Secureboot Firmware | Optional vorkonfiguriert | Bis zu 1G

- NEOXPacketRaven Portable Standard Features
- (Optional) Fix vorkonfiguriert
- Gesicherte und verschlüsselte Firmware
- Sicherheitssiegel gegen unbemerktes Öffnen
- Sicherheitsschrauben gegen unerwünschtes Öffnen

PACKETRAVEN

neoxn.de/htap

Cybersecurity | NDR Feed | Incident Response

Compliance | Außeneinsatz | Industrieanlage

Hardened Netzwerk-TAP Advanced Features:

- Optional vorkonfiguriert - keine nachträglichen Konfigurationsänderungen möglich
- Secureboot Firmware – Startup-Prüfung auf gültige Signatur der Firmware und autorisierten öffentlichen Schlüssel
- Sicherheitssiegel – können nicht unbemerkt entfernt werden
- Sicherheitsschrauben – Spezialwerkzeug notwendig
- IEC 62443 zertifiziert und KRITIS Approved

Zertifizierungen:

- CE, FCC, RoHS, WEEE, EN 55032 KL. A/B, EN 55035, EN 61000-3-2, EN 61000-3-3, EN 61000-6-2, EN 50121-4:2016, EN 50129, IEC 62443-4-2:2019 Security Level Capability 2 (SL-C 2)

- NEOXPacketRaven Hardened TAPs sind für Kupfer- und aktive Glasfaserverbindungen erhältlich und unterstützen Geschwindigkeiten von bis zu 1 Gbit/s.
- NEOXPacketRaven TAPs sind in der Standardversion erhältlich, um einen Angriffsvektor auszuschließen. Für Hochsicherheitsbereiche gemäß IEC 62443 und kritische Infrastrukturen (KRITIS) ist eine zusätzliche gehärtete Version erhältlich.
- NEOXPacketRaven Hardened TAPs werden mit einer gesicherten, verschlüsselten Firmware ausgeliefert, die bei jedem Neustart des TAPs auf gültige Signaturen und einen autorisierten öffentlichen Schlüssel prüft. Andernfalls kann der TAP nicht in Betrieb genommen werden.
- NEOXPacketRaven Hardened TAPs können vorkonfiguriert geliefert werden und blockieren alle nachträglichen Änderungen aus Sicherheitsgründen. Außerdem sind sie durch spezielle Schrauben und Sicherheitssiegel gegen ungewolltes oder unbemerktes Öffnen gesichert.

NEOX NETWORKS

Netzwerk-TAPs

NEOXPacketRaven Modular Fiber-TAPs

Volle Netzwerktransparenz bis zu 400G | 100% Passive High Density | Extrasichere Modelle verfügbar

- Bis zu 400Gbps
- Volle Netzwerk-transparenz
- Keine Beeinträchtigung des Datenverkehrs
- 100% Netzwerkdaten
- Unsichtbar für Angreifer
- Kein Netzwerkzugriff über den Monitoring-Port
- Plug-n-Play
- Keine Stromversorgung nötig
- Verschiedene Split Ratios
- Farbkodierte Steckverbinder
- Skalierbar und Modular
- Extrasichere Modelle verfügbar

PACKETRAVEN

neoxn.de/mtap

Cybersecurity | NDR Feed | Incident Response

Compliance | Rechenzentrum | Service Provider

Fiber-TAPs sind passive Entkopplungselemente für den sicheren und zuverlässigen Abgriff von Netzwerkdaten in optischen Netzwerken. Diese TAPs werden in die zu überwachende Glasfaserleitung eingeschleift und übertragen den gesamten Datenverkehr ohne Unterbrechung und ohne Paketverlust.

- Mit den modularen Netzwerk-TAPs von NEOXPacketRaven erhalten Sie permanenten Zugriff auf den Netzwerkverkehr mit bis zu 400 Gbps. NEOX TAPs dienen der Observability in der Hybrid-Cloud, der Performanceoptimierung von Applikationen und Sicherheitstools, und stellen zu 100% zuverlässige Netzwerkdaten bereit.
- Die modularen TAPs von NEOXPacketRaven sind primär für den Einsatz in Rechenzentren konzipiert und ermöglichen bis zu 30 "abgegriffene" Netzwerksegmente in nur 1HE.
- NEOXPacketRaven TAPs sind passiv und benötigen keine Stromversorgung. NEOX TAPs sind für Angreifer nicht auffindbar und da sie sich auf OSI-Schicht-1 befinden, haben sie keine MAC/IP-Adresse. Da die Integrität der ausgehenden Daten unverändert bleibt, werden sie für die Netzwerkforensik, Cybersicherheit, Reaktion auf Zwischenfälle und Überwachung eingesetzt.
- NEOX Fiber-TAPs gehören zu den sichersten, selbst in der Standardversion. Für ultimative Sicherheit und KRITIS-Infrastrukturen sind auch extra-sichere NEOXPacketRaven Secure TAPs erhältlich.
- Diese Secure Fiber-TAPs verfügen über einen zusätzlichen optischen Isolator (Datendiode) und einen optischen Filter, um unerwünschte eingehende Lichtsignale am Port des Abgriffs zu blockieren und so das Netzwerk vor Kompromittierung zu schützen. Eine sehr hohe Einfügungsdämpfung auf dem Rückkanal vom Monitoring-Port zum Netzwerk bietet eine zusätzliche Sicherheitsebene.
- Einige der NEOXPacketRaven TAPs unterstützen die bidirektionale (BiDi) Technologie auf der Basis von WDM (Wavelength Division Multiplexing) und sind sowohl für Singlemode- als auch für Multimode-Konfigurationen mit LC- oder MTP-Steckern geeignet.

NEOX NETWORKS

Netzwerk-TAPs

NEOX**PacketRaven Secure Fiber Netzwerk-TAPs**

High Security und KRITIS Compliant | Datendioden-Funktion
Modulare oder portable Passive TAPs | Bis zu 400G

- NEOXPacketRaven Passive Standard Features
- Datendioden-Funktion gegen unerwünschte Lichteinspeisungen
- Sicherheitssiegel gegen unbemerktes Öffnen
- Sicherheitsschrauben gegen unerwünschtes Öffnen

PACKETRAVEN

neoxn.de/mtap

neoxn.de/ptap

Cybersecurity | NDR Feed | Incident Response

Compliance | Remote Site | Data Center

NEOXPacketRaven Passive modulare und portable Secure Fiber-TAPs verfügen sowohl über einen zusätzlichen optischen Isolator (Datendioden-Funktionalität) als auch über einen optischen Filter, der unerwünschte eingehende Lichtsignale am Monitoring-Port blockiert, um das Netzwerk vor Kompromitierung zu schützen. Dadurch wird eine weitere Sicherheitsebene hinzugefügt, die einen erhöhten Schutz vor Angreifern und fehlerhaften Konfigurationen bietet.

- Mit den modularen Netzwerk-TAPs von NEOXPacketRaven erhalten Sie permanenten Zugriff auf den Netzwerkverkehr mit bis zu 400 Gbps. NEOX TAPs dienen der Observability in der Hybrid-Cloud, der Performanceoptimierung von Applikationen und Sicherheitstools, und stellen zu 100% zuverlässige Netzwerkdaten bereit.
- NEOXPacketRaven Secure Fiber-TAPs sind passiv und benötigen keine Stromversorgung. NEOX TAPs sind für Angreifer unsichtbar und da sie sich auf OSI-Schicht-1 befinden, haben sie keine MAC/IP-Adresse. Da die Integrität der ausgehenden Daten unverändert bleibt, werden sie für die Netzwerkforensik, Cybersicherheit, Reaktion auf Zwischenfälle und Überwachung eingesetzt.
- NEOXPacketRaven Secure Fiber-TAPs sind für Hochsicherheitsbereiche gemäß IEC 62443 und kritische Infrastrukturen (KRITIS) geeignet.
- NEOXPacketRaven Secure Fiber-TAPs sind in zwei Varianten erhältlich. Die modularen Fiber-TAPs sind für den Einsatz Rechenzentrem konzipiert und ermöglichen bis zu 30 "abgegriffene" Netzwerksegmente in nur 1HE. Die portablen Fiber-TAPs eignen sich hervorragend für den Einsatz vor Ort und unterwegs und können aber auch in einem 19"-Rack oder auf einer Hutschiene installiert werden, was eine große Flexibilität bietet.
- Die modularen Secure Fiber-TAPs von NEOX sind zu 100% kompatibel mit den modularen Standard-TAPs ohne Datendioden-Funktion und können zusammen im selben Gehäuse installiert werden. Desweiteren sind sie protokollunabhängig und mit allen Überwachungssystemen führender Anbieter kompatibel.

NEOX NETWORKS

Netzwerk-TAPs

NEOXPacketRavenVirtual Virtual-TAP

100% Netzwerkzugriff in virtuellen & Multi-Cloud Umgebungen
End-to-End East-West & North-South Traffic Visibility

- Volle Netzwerktransparenz
- Keine Beeinträchtigung des Datenverkehrs
- 100% verlustfreie Netzwerkdaten
- Für verschiedene Umgebungen
- Unlimitierte Netzwerk-geschwindigkeit
- Flexibel einsetzbar
- Alternative zum virtuellen Port Mirroring
- Leicht zu installieren und konfigurieren
- GRE/VxLAN Tunneling
- OSI Layer 2-4 Stateful Filtering
- Aggregation N : 1
- Regeneration/ Replication 1 : N

PACKETRAVEN

neoxn.de/vtap

Cybersecurity | NDR Feed | Incident Response

Cloud | Rechenzentrum | Service Provider

Mit der zunehmenden Nutzung von virtuellen, Hybrid-Cloud- und Multi-Cloud-Umgebungen hat auch die Zahl der blinden Flecken im Netzwerk zugenommen. Die virtuellen TAPs (vTAPs) von NEOXPacketRaven wurden entwickelt, um einen sicheren und zuverlässigen Zugriff auf den Netzwerkverkehr in virtuellen und Cloud-Umgebungen zu ermöglichen und so eine erweiterte East-West- und North-South-Transparenz des Netzwerks und eine umfassende Observability zu gewährleisten.

- NEOXPacketRavenVirtual versorgt physische und virtuelle Sicherheits- und Überwachungstools mit vollständiger Netzwerktransparenz in virtualisierten privaten, öffentlichen und Hybrid-Cloud/-Multi-Cloud-Umgebungen, einschließlich VMware, AWS, Microsoft Azure und Google Cloud.
- PacketRavenVirtual lässt sich schnell über ein Debian-Paket oder ein Docker-Image bereitstellen und bietet umgehend vollständige Transparenz des East-West-Verkehrs zwischen virtuellen Maschinen (VM). Dadurch wird der Datenverkehr für die Überwachung von Sicherheit, Verfügbarkeit und Performance in Linux- und Private-Cloud-Umgebungen erweitert, ohne die Performance oder Architektur zu beeinträchtigen und ohne notwendige Änderungen an der Netzwerkinfrastruktur.
- Die häufig verwendeten und bereits vorhandenen (virtuellen) SPAN-/Mirror-Ports sind für langfristige Überwachungszwecke ungeeignet. Bei der Port-Spiegelung wird der gesamte Datenverkehr an alle Ziele (Sicherheits-/Überwachungstools) gesendet, was zu großen Ineffizienzen und Sicherheitsrisiken führt. NEOXPacketRavenVirtual leitet die benötigten granularen Daten mit N:1 (Aggregation) oder 1:N (Regeneration) weiter. Mit NEOXPacketRaven Virtual ist es auch möglich, den Datenverkehr pro Richtung zu spiegeln. NEOXPacketRavenVirtual bietet auch die Möglichkeit, sich über GRE/VXLAN-Tunneling mit physischen Geräten zu verbinden, was bei einer Port-Spiegelung schwierig oder unmöglich ist.
- NEOXPacketRavenVirtual unterstützt Stateful Filtering (verbindungsorientiertes Filtern), um nur relevante Daten weiterzuleiten und so die teuren Tools zu entlasten. Es werden Filterkriterien auf den OSI-Schichten 2-4 unterstützt. Dies ist besonders in der Cloud nützlich und spart enorme Kosten für die Datenübertragung. Einige Cloud-Anbieter können auch den gespiegelten Port-Mirror-Verkehr einschränken, was zu einem teilweisen oder vollständigen Verlust der Netzwerktransparenz führt.

NEOX PacketRaven Netzwerk-TAP Familie

Stärkung der Cybersicherheit und Application Observability durch Integration von Network-Wire-Data-Intelligence in Echtzeit

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

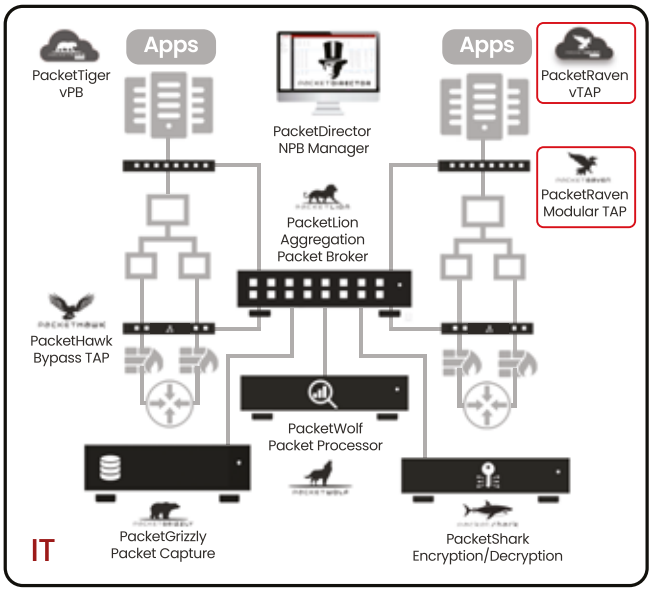
Deployment

SOC

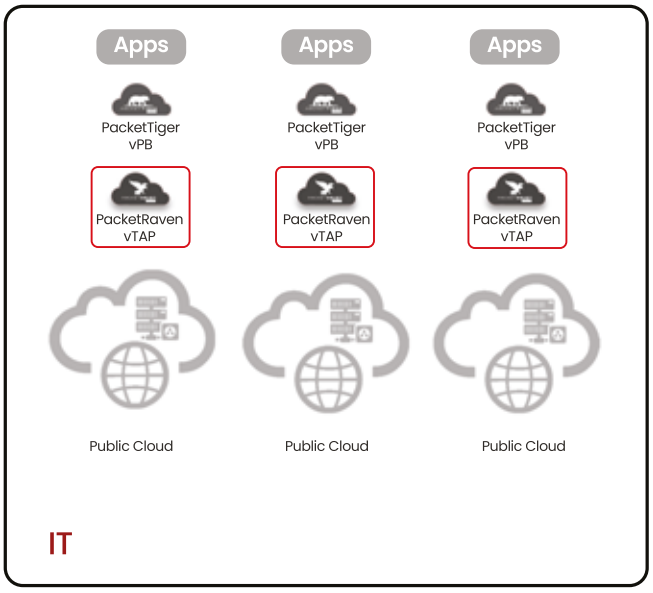
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

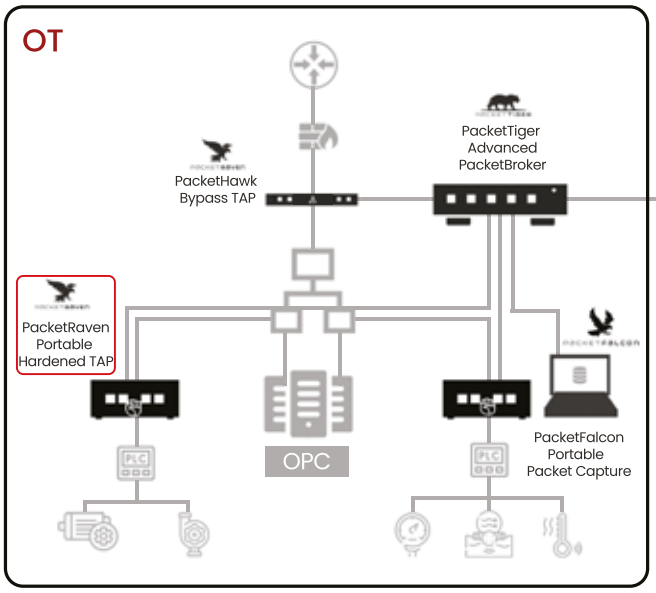
Application Issues, User Experiences, APM/NPM



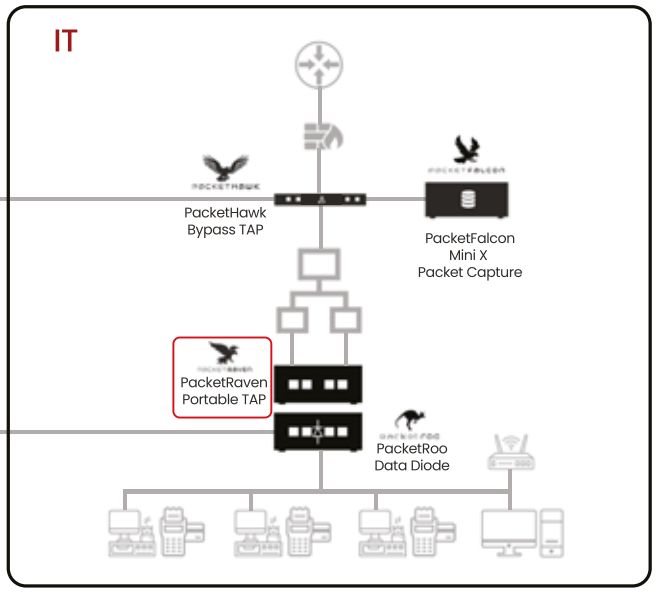
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

NEOX NETWORKS

packetroo

NEOX**PacketRoo Data Diode**

Stärkung der Cybersicherheit und Application Observability durch Integration von Network Wire-Data Intelligence in Echtzeit

NEOX NETWORKS

Datendiode

NEOXPacketRoo Netzwerk-Datendiode

Sicherer Dateitransfer | AirGap-Assurance | Galvanische Trennung

- Unidirektionaler Datenfluss
- Galvanische Trennung
- Hersteller-unabhängig
- AirGap-Assurance
- Für rauhe Umgebungen
- Automatischer Speed-Sync
- Link Loss Detection
- Fehlervermeidung durch fixe Konfiguration
- Windows & Linux Support

packetroo

neoxn.de/roo

Cybersecurity | NDR Feed | Incident Response

Compliance | Remote Site | Industrieanlage

Eine Datendiode ist eine spezielle Lösung, die eine vollständige galvanische Isolierung zwischen den Netzwerken erzwingt und gleichzeitig eine unidirektionale Signalübertragung ermöglicht, wobei der kritische AirGap erhalten bleibt. Um jegliche Angriffsfläche auf der physikalischen Ebene zu eliminieren, können Betreiber entweder Datenübertragungsmethoden verwenden, die die NEOXPacketRoo-Datendiodenfunktionalität nutzen, oder die NEOX-SecureFileTransmitter-Software einsetzen, die eine sichere, granulare und einseitige Dateiübertragung von der OT zur IT ermöglicht.

- In Kombination mit dem NEOXSecureFileTransmitter bietet PacketRoo eine skalierbare und leistungsstarke Lösung für Windows- und Linux-Hosts, die eine nahtlose unidirektionale Datenübertragung ermöglicht Jede Komponente des Pakets ist auch separat erhältlich. Wenn bereits eine Datendiode vorhanden ist, um die AirGap zwischen Netzwerken zu überbrücken, bleibt der NEOXSecureFileTransmitter vollständig herstellerunabhängig. Diese Flexibilität gilt auch für PacketRoo selbst.
- In kritischen Sektoren wie der Energieversorgung, dem Transportwesen, der Verteidigung und der industriellen Fertigung ist der Schutz von IT/OT-Netzwerken vor Cyberangriffen von entscheidender Bedeutung, insbesondere bei Anwendungen, die Sicherheitsintegritätsstufen (SIL) 3 und 4 erfordern. Die Implementierung einer AirGap zwischen OT- und IT-Umgebungen stärkt die Sicherheit durch die physische Trennung betrieblicher Technologiesysteme von externen IT-Netzwerken, wodurch sich das Risiko von Cyber-Bedrohungen deutlich verringert.
- Um das Risiko von Konfigurationsfehlern zu verringern, ist der PacketRoo nur in festen Konfigurationen verfügbar, ohne die Möglichkeit, die Port-Einstellungen nach der Installation zu ändern. Als vollständig versiegeltes System ist es sowohl für zivile als auch für militärische Anwendungsfälle konzipiert und gewährleistet einen robusten und sicheren Betrieb.

NEOX**PacketRoo Datendiode**

Stärkung der Cybersicherheit und Application Observability durch Integration von Network Wire-Data Intelligence in Echtzeit

IT NetSecOps | KRITIS | Rechenzentrum | Multi-Cloud

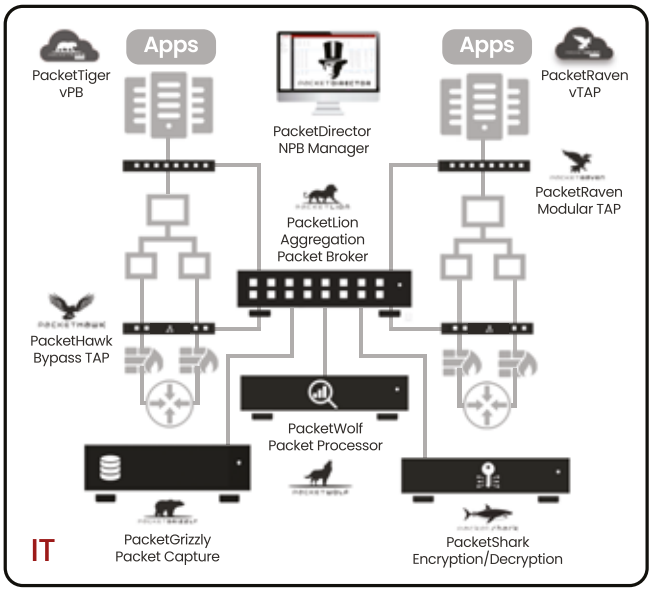
Deployment

SOC

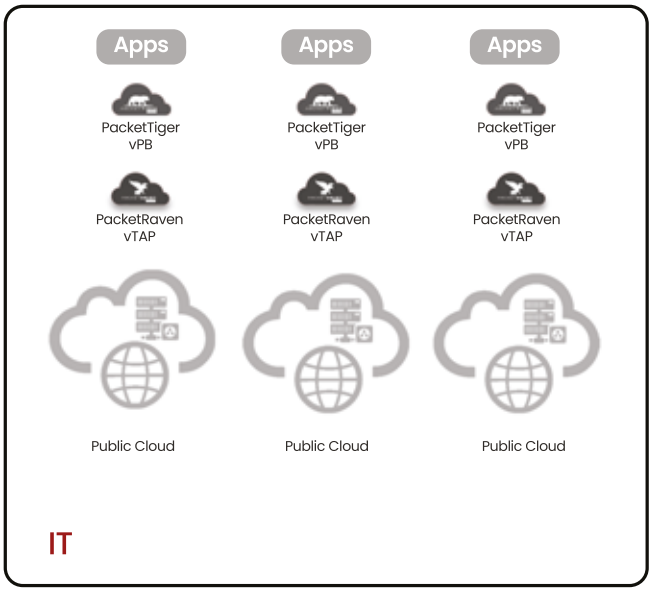
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

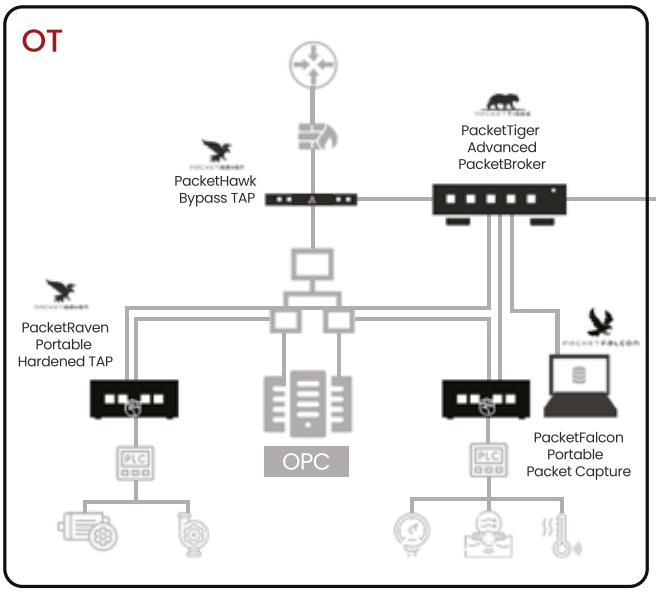
Application Issues, User Experiences, APM/NPM



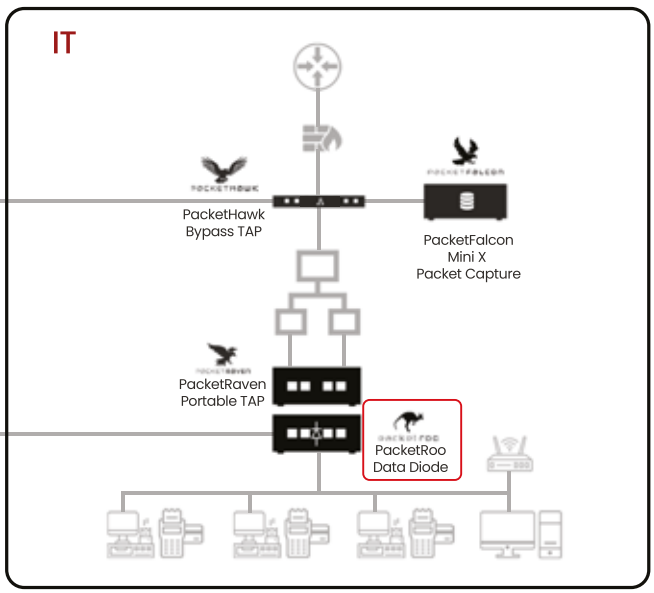
Rechenzentrum



Multi-Cloud



Industrieller Standort



Zweigstelle

Optische Transceiver und Kabel

Stärkung der Cybersicherheit und Application Observability durch Integration schnellerer und zuverlässiger Konnektivität

NEOX NETWORKS

Connectivity

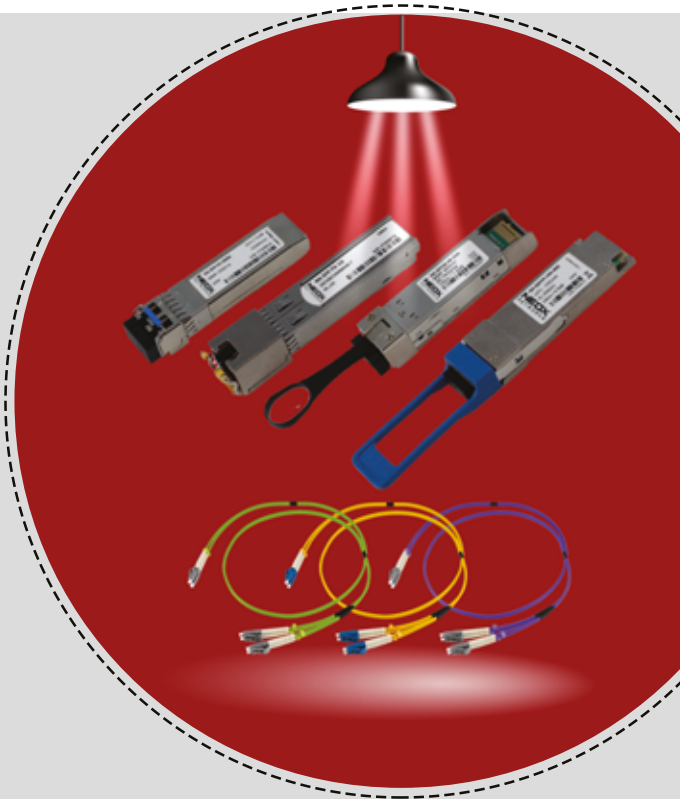
Optische Transceiver und Kabel

Vorqualifizierte, schnellere und zuverlässigere Konnektivität

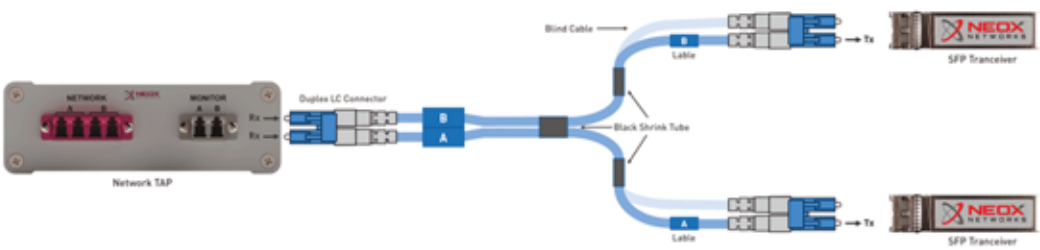
- Vorqualifiziert
- 1G - 400G — 1 Gbps - 400 Gbps
- MSA/Multi-Vendor Compliant
- Multiple Standards
- Qualitativ hochwertig
- Spezialkabel verfügbar

neoxn.de/trans

neoxn.de/ykabel

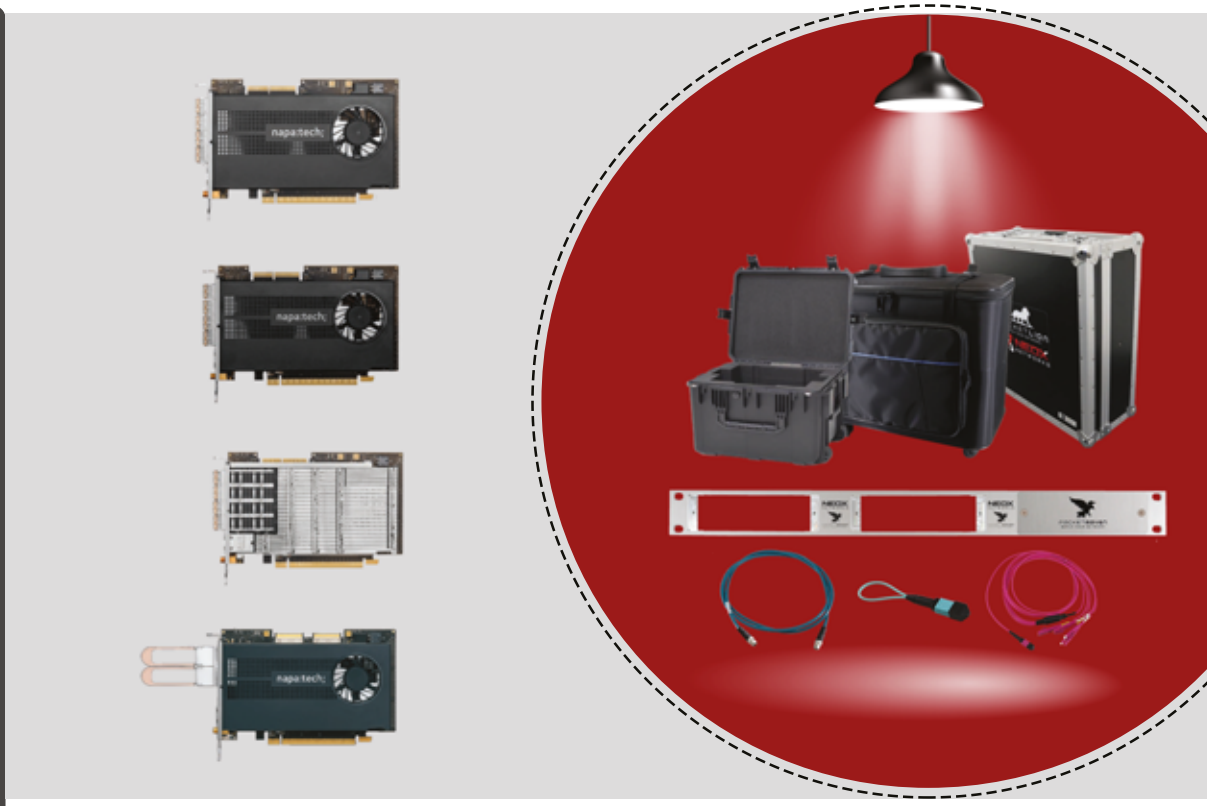


- Die optischen Transceiver von NEOX sind für alle NEOX Next-Generation Network Visibility Appliances vorqualifiziert, um eine risikofreie Konnektivität mit der Rechenzentrumsstruktur, den Switches oder Routern zu gewährleisten. Sie sind universell einsetzbar und erfüllen die höchsten Qualitätsanforderungen.
- Optische Transceiver sind MSA-konform und können daher sowohl in NEOX-Produkten, aber auch in Geräten anderer Hersteller verwendet werden.
  Diese sind für Netzwerkkonnektivitäten von 1Gbps - 400Gbps unter Verwendung von Standard-SFP, SFP+, SFP28, QSFP+, QSFP28, QSFP56 oder QSFP-DD erhältlich.
- Vorqualifizierte Glasfaserkabel von NEOX gewährleisten eine risikofreie Plug-and-Play Konnektivität und eine schnellere Bereitstellung der Netzwerk-Visibility-Equipments. Ein mit LC-Steckern ausgestatteter NEOXPacketRaven TAP verfügt über drei Duplex-Anschlüsse, von denen zwei zum Durchschleifen des zu analysierenden Netzwerkverkehrs benötigt werden und ein Duplex-Anschluss zum passiven Abgreifen der gespiegelten Daten zur Weiterleitung an einen NEOXPacketTiger Network Packet Broker, ein Analyse- oder Sicherheitstool (wie IDS/IPS).
- Der Datenverkehr wird auf beiden Seiten des Monitoring Ports zur Verfügung gestellt. Diese beiden Ausgänge müssen mittels zwei Transceivern in zwei Monitoring-Ports eingespeist werden, um den bidirektionalen Datenverkehr vollständig zu empfangen, da nur die Empfangsseite (Rx) der Transceiver für die Aufzeichnung verwendet werden kann. Dies stellt eine Herausforderung dar, da der Ausgang des TAP ein Duplex-Port ist, jedoch zwei separate Ports auf der Rx-Seite für zwei einzelne Transceiver benötigt werden. Um dieses Problem zu vermeiden, ist es am besten, eines der speziellen Y-Kabel von NEOX zu verwenden, das einen Duplex-Anschluss in zwei Duplex-Anschlüsse umwandelt, so dass das Licht ausschließlich in die Rx-Seite der Transceiver eingespeist wird.



Zubehör

Capture-Karten, Montagekits, Transportkoffer



Unser NEOX NETWORKS Zubehör bietet hochwertige, zuverlässige und perfekt abgestimmte Erweiterungen für unsere Netzwerk- und Monitoring-Lösungen – für maximale Performance, Effizienz und Convenience.

- Smarte High-Performance Capture-Karten für NeoxPacketFalcon und NEOXPacketGrizzly Packet Capture Appliances und PacketWolf Packet Processing Appliance
- Netzwerk-TAP Montagekits und Blindplatten für Server-Racks in Rechenzentren, sowie DIN Hut-schienen-Clips für die NEOXPacketRaven Portable Familie.
- Robuste Transportkoffer und -trolleys
- Standard Glasfaserkabel, M12-Kabel, Fan-out Kabel, Fiber Loopback Adapter, uvm.

NEOX NETWORKS

NEXT GENERATION NETWORK VISIBILITY

v2.31

FIRMENSITZ

NEOX NETWORK Inc.
Techmart Center
5201 Great America Parkway Suite 320
Santa Clara, CA 95054, USA

neoxnetworks.com
info@neox-networks.com
+1 408 850 7201

NEOX NETWORKS GmbH
Monzastraße 4
63225 Langen
Deutschland

neox-networks.com
info@neox-networks.com
+49 6103 37215 910

NEOX NETWORK
1F Shinsung building
5 Eonnam-gil, Seocho-gu
Seoul 06779, Südkorea

neoxnetworks.com
info@neox-networks.co.kr
+822 579 2904