



neox-networks.com

Product Brochure

Next-Generation Network Visibility Solution
for IT Observability and Security



NEOX PacketRaven Hybrid-Cloud TAP Series

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Copying Real-Time Data-in-Motion



NEOX PacketRaven Hybrid-Cloud TAP Series

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Copying Real-Time Data-in-Motion

IT NetSecOps

IT NetAppOps

Data Center

Multi-Cloud



Business Benefits

- Increased Business Continuity and Reduced Downtime
- Enabling CXO's Digital Transformation through Hybrid-Cloud Visibility
- Reduced Customer Churn through Lower MTTR, Enhanced Security, and Information Protection



Technical Benefits

- Setup Once, Benefit Forever, Network Visibility and Real-Time Wire-Data Access
- Foundation Layer to Build a Hierarchical Network Monitoring and Observability Practice
- Consistent Tools and Methods for Network-as-a-Service across the Hybrid Infrastructure



Infrastructure Security

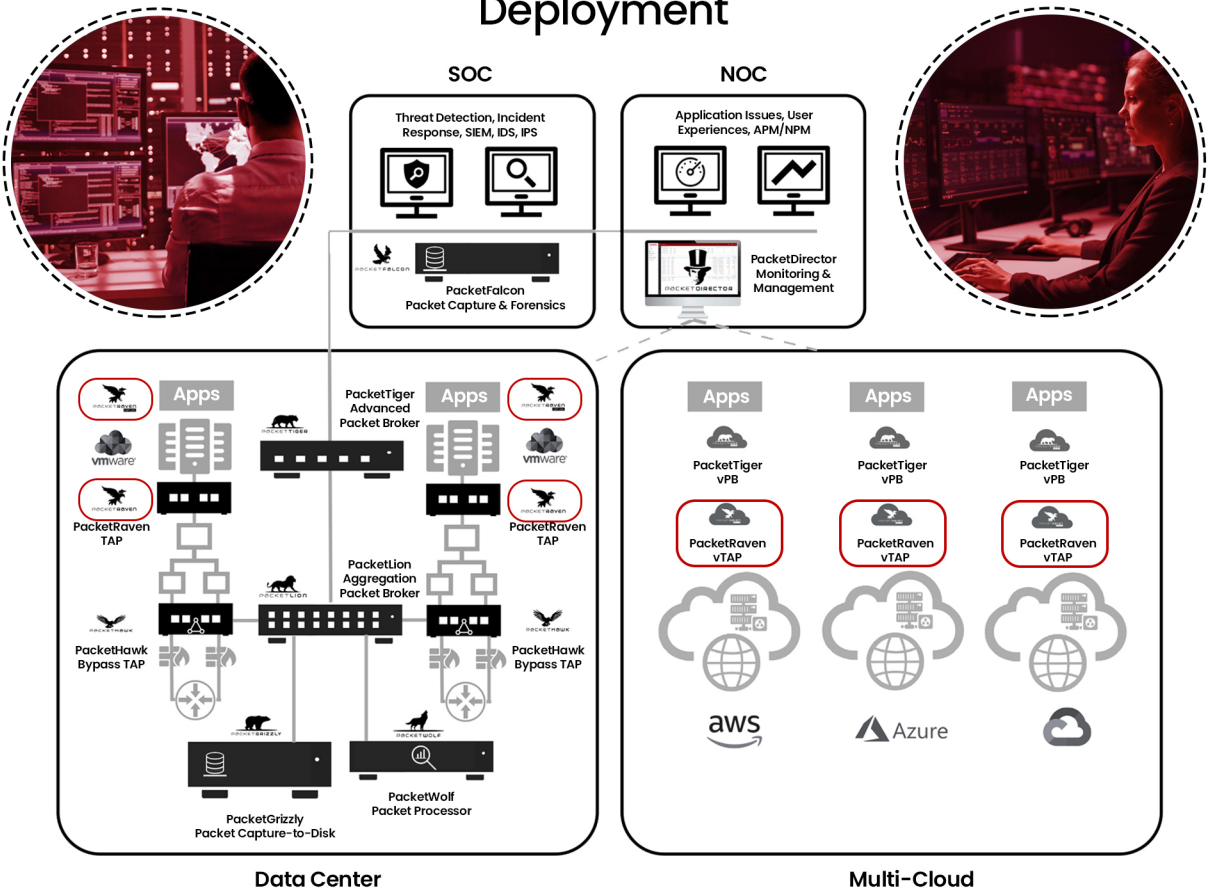
- Strengthened Network Security through Network Traffic Visibility across Hybrid-Cloud Infrastructure
- Real-Time Network Intelligence for Threat Detection and Network Detection and Response Tools
- Archived Network Data Access for Incident Response, Forensics, and Compliance



Application Performance

- Enhanced Application Performance, Responsiveness, and Availability through Network Visibility across Hybrid-Cloud Infrastructure
- Faster Troubleshooting for Application and User Experience Issues
- Reduced MTTR due to Always-On Network Visibility

Deployment



NEOXPacketRaven Portable Network TAPs

Full Network Visibility up to 400G

FPGA Chipset | Data Diode Function | Redundant Power



Up to 400Gbps



Full Network Transparency



No Impairment of Data Traffic



100% Network Data



Invisible for Attackers



No Network Access via Monitoring Port



Flexible to Use



Plug-n-Play



Failure Protection on Power Loss



PoE+ Power over Ethernet



Redundant Power Supplies



Various Split Ratios



Fast and Precise



Supports Jumbo Frames



Hardened & Secure



Made in Germany



PACKETRAVEN

SecurITy

Trust Seal
www.telnet.at/certnamig
made in Germany



Learn more at:
neoxn.eu/ptap



Network TAPs are decoupling elements for the secure and reliable tapping of network data in optical and copper-based networks. These TAPs are looped into the network line to be monitored and forward the entire data traffic without interruption or packet loss.

- With NEOXPacketRaven Network TAPs you get permanent network traffic access up to 400Gbps, for hybrid-cloud observability, application performance, and security tools, and provide 100% reliable network data.
- NEOXPacketRaven TAPs are untraceable for attackers and being at OSI layer-1, do not have a MAC/IP address. As the integrity of the outgoing data remains unaltered, they are used for network forensics, cybersecurity, incident response, and monitoring.
- NEOXPacketRaven TAPs provide an active monitoring port acting like a "Data Diode", physically isolating the monitoring ports from the network ports. Access to the network via the monitoring ports is prevented in hardware, blocking any backdoor access.
- NEOXPacketRaven Portable TAPs are available in optimally preconfigured "hardened" versions for high-security uses compliant with IEC 62443, and equipped with encrypted firmware, security seals, and security screws against unwanted openings.
- NEOXPacketRaven TAPs with passive monitoring ports are also available in an extra-secure version. These Secure Fiber TAPs have both, an additional optical isolator (Data Diode) and an optical filter, to block unwanted incoming light signals at the monitoring port, to protect the network from compromise.
- For the highest reliability, all NEOXPacketRaven TAPs with active monitoring ports have redundant power supplies but can also be operated with 12-48V DC voltage, and in some cases using PoE. Fiber TAPs do not require any power.
- The versatile NEOXPacketRaven can be used as Portable TAPs or installed in a 19" data center rack using a rack mounting kit, or on a DIN hat rail using a DIN rail clip.

NEOXPacketRaven Portable Hardened TAPs

High Security Network TAPs | CRITIS & IEC 62443 Approved
Secureboot Firmware | Optionally Preconfigured | Up to 1G

-  NEOXPacketRaven Portable Standard Features
-  (Optional) Fix Preconfigured
-  Secured and Encrypted Firmware
-  Security Seal against Unnoticed Opening
-  Safety Screws against Unwanted Opening
-  Made in Germany



Learn more at:
neoxn.eu/htap



NEOXPacketRaven Hardened Advanced Features:

- Optionally preconfigured – do not allow subsequent configuration changes
 - Secureboot Firmware – startup check for firmware valid signature and authorized public key
 - Security Seals – cannot be removed unnoticed
 - Safety Screws – special tool required
 - IEC 62443 and CRITIS approved
-
- NEOXPacketRaven Hardened TAPs are available for copper and active fiber connectivity, supporting speeds up to 1Gbps.
 - NEOXPacketRaven TAPs are available in the standard version to exclude an attack vector. For high-security areas per IEC 62443 and critical infrastructures (CRITIS), an additional hardened version is available.
 - NEOXPacketRaven Hardened TAPs ship with secured encrypted firmware, employing secure boot checks for valid signatures and authorized public key, each time the TAP is restarted. Otherwise, TAP cannot be put into operation.
 - NEOXPacketRaven Hardened TAPs can be delivered pre-configured, blocking any subsequent changes for security. In addition, they are secured against unwanted or unnoticed openings by special screws and security seals.

Certifications:

- 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

NEOXPacketRaven Modular Fiber TAPs

Full Network Visibility up to 400G | 100% Passive
Extra Secure Models Available



Up to
400Gbps



Full Network
Transparency



No Impairment
of Data Traffic



100% Lossless
Network Data



Invisible
for Attackers



No Network Access
via Monitoring Port



Plug-n-Play



No Power Supply
Necessary



Various
Split Ratios



Color Coded
Connectors



Scalable and
Modular



Extra Secure
Models Available



Made in
Germany



SecurITy
made
in
Germany



Learn more at:
neoxn.eu/mtap



Fiber TAPs are passive decoupling elements for the secure and reliable tapping of network data in optical networks. These TAPs are looped into the fiber optic line to be monitored and transmit the entire data traffic without interruption and without packet loss.

- With NEOXPacketRaven Modular Network TAPs you get permanent network traffic access up to 400Gbps, for hybrid-cloud observability, application performance, and security tools, and provide 100% reliable network data.
- NEOXPacketRaven Modular TAPs are designed for data center class and allow up to 30 "tapped" network segments in only 1U rack space.
- NEOXPacketRaven TAPs are passive and do not require power. NEOXPacketRaven TAPs are untraceable for attackers and being at OSI layer-1, do not have a MAC/IP address. As the integrity of the outgoing data remains unaltered, they are used for network forensics, cybersecurity, incident response, and monitoring.
- NEOXPacketRaven Fiber TAPs are among the most secure, even the standard version. For ultimate security and CRITIS infrastructures, NEOXPacketRaven Secure Modular TAPs are also available.
- Due to their optical isolator and optical filter capabilities, these Secure Fiber TAPs have both, an additional optical isolator (Data Diode) and an optical filter, to block unwanted incoming light signals at the monitoring port, to protect the network from compromise. A very high insertion loss on the return channel from the monitoring port to the network provides an additional security layer.
- Some of the NEOXPacketRaven TAPs support bidirectional (BiDi) technology based on Wavelength Division Multiplexing (WDM) and are suitable for both single-mode and multi-mode configurations using LC or MTP connectors.

NEOXPacketRaven Secure Fiber Network TAPs

High Security and CRITIS Compliant | Data Diode Functionality
Modular or Portable Passive TAPs | Up to 400G

-  Passive PacketRaven Standard Features
-  Data Diode Functionality against Undesired Light Injections
-  Security Seal against Unnoticed Opening
-  Safety Screws against Unwanted Opening
-  Made in Germany



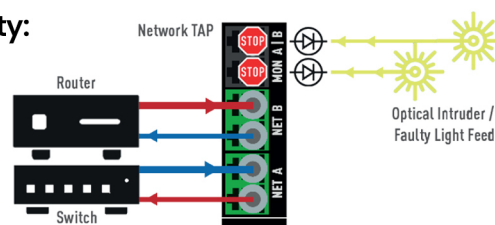
Learn more at:
neoxn.eu/stap



NEOXPacketRaven Passive Modular and Portable Secure Fiber TAPs feature both an additional optical isolator (Data Diode functionality) and an optical filter that blocks unwanted incoming light signals at the monitoring port, to protect the network from compromise. This adds another layer of security, providing increased protection against attackers and faulty configurations.

- With NEOXPacketRaven Secure Fiber TAPs you get permanent network traffic access up to 400Gbps, for hybrid -cloud observability, application performance, and security tools, and provide 100% reliable network data.
- NEOXPacketRaven Secure Fiber TAPs are passive and do not require power. NEOXPacketRaven TAPs are untraceable for attackers and being at OSI layer-1, do not have a MAC/IP address. As the integrity of the outgoing data remains unaltered, they are used for network forensics, cybersecurity, incident response, and monitoring.
- NEOXPacketRaven Secure Fiber TAPs are suitable for high security areas per IEC 62443 and critical infrastructures (CRITIS).
- NEOXPacketRaven Secure Fiber TAPs are available in two variants. The Modular Fiber TAPs are designed for data center class and allow up to 30 "tapped" network segments in only 1U rack space. While the Portable Fiber TAPs are great for field and mobile use, and can also be installed in a 19" data center rack, providing great flexibility.
- NEOXPacketRaven Modular Secure Fiber TAPs are 100% compatible with standard Modular TAPs without Data Diode function and can be installed together in the same enclosure. They are also protocol agnostic and compatible with all monitoring systems from leading vendors.

Data Diode functionality:



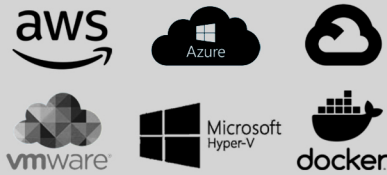
NEOXPacketRavenVirtual Virtual TAP

100% Network Access in Virtual & Multi-Cloud Environments
End-to-End East-West & North-South Traffic Visibility

-  Full Network Transparency
-  No Impairment of Data Traffic
-  100% Lossless Network Data
-  For different Environments
-  Unrestricted Network Speed
-  Flexible Deployable
-  Alternative to virtual Port Mirroring
-  Easy to Install & Configure
-  GRE/VxLAN Tunneling
-  OSI Layer 2-4 Stateful Filtering
-  Aggregation N : 1
-  Regeneration/ Replication 1 : N
-  Developed & Programmed in Germany



PACKETRAVEN



Learn more at:
neoxn.eu/vtap



With the increase in the use of virtual, hybrid-cloud, and multi-cloud environments, there also has been an increase in the number of network blind spots. NEOXPacketRaven Virtual TAPs (vTAPs) are designed to provide secure and reliable access to network traffic in virtual and cloud environments for extended east-west and north-south network visibility and overall hybrid observability.

- NEOXPacketRavenVirtual provides physical and virtual security and monitoring tools with complete network visibility in virtualized private, public, and hybrid-cloud/multi-cloud environments, including VMware, AWS, Microsoft Azure, and Google Cloud.
- Fastly deployed using a Debian package or Docker image, PacketRavenVirtual instantly provides full visibility of east-west traffic between virtual machines (VM). This extends traffic for security, availability, and performance monitoring in Linux and private-cloud environments without impacting performance or architecture, and without any changes to the network infrastructure.
- The often used and already existing (virtual) SPAN/mirror ports are unsuitable for long-term monitoring purposes. With port mirroring the entire data traffic is broadcasted to all destinations (security/monitoring tools), causing large inefficiencies and security risks. NEOXPacketRavenVirtual forwards the need-to-know granular data with N:1 (aggregation) or a 1:N (regeneration). With NEOXPacketRavenVirtual, it is also possible to mirror the traffic per direction. NEOXPacketRavenVirtual also offers connecting to physical devices via GRE/VXLAN tunneling, which is difficult or impossible with port mirroring.
- NEOXPacketRavenVirtual supports stateful filtering (connection-oriented filtering) to forward only the data that is relevant, relieving the expensive tools and reducing tool sprawl. Filter criteria on OSI layers 2-4 are supported. This is particularly useful in the cloud, saving huge data transfer bills. Some cloud providers can also restrict mirrored port mirror traffic, resulting in partial or total loss of network visibility.



NEOXPacketHawk Inline Bypass TAP

Strengthening Cybersecurity, Hybrid-Cloud Application Observability,
and Business Continuity, by Integrating the Network Intelligence
and Intelligent Traffic Rerouting



NEOX PacketHawk Inline Bypass TAP

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Intelligent Traffic Rerouting

IT NetSecOps

IT NetAppOps

Data Center

Multi-Cloud



Business Benefits

- Increased Business Continuity and Reduced Downtime
- Enabling CXO's Digital Transformation through Hybrid-Cloud Visibility
- Reduced Customer Churn through Lower MTTR, Enhanced Security, and Information Protection



Technical Benefits

- Setup Once, Benefit Forever, Network Visibility and Real-Time Wire-Data Access
- Foundation Layer to Build a Hierarchical Network Monitoring and Observability Practice
- Consistent Tools and Methods for Network-as-a-Service across the Hybrid Infrastructure



Infrastructure Security

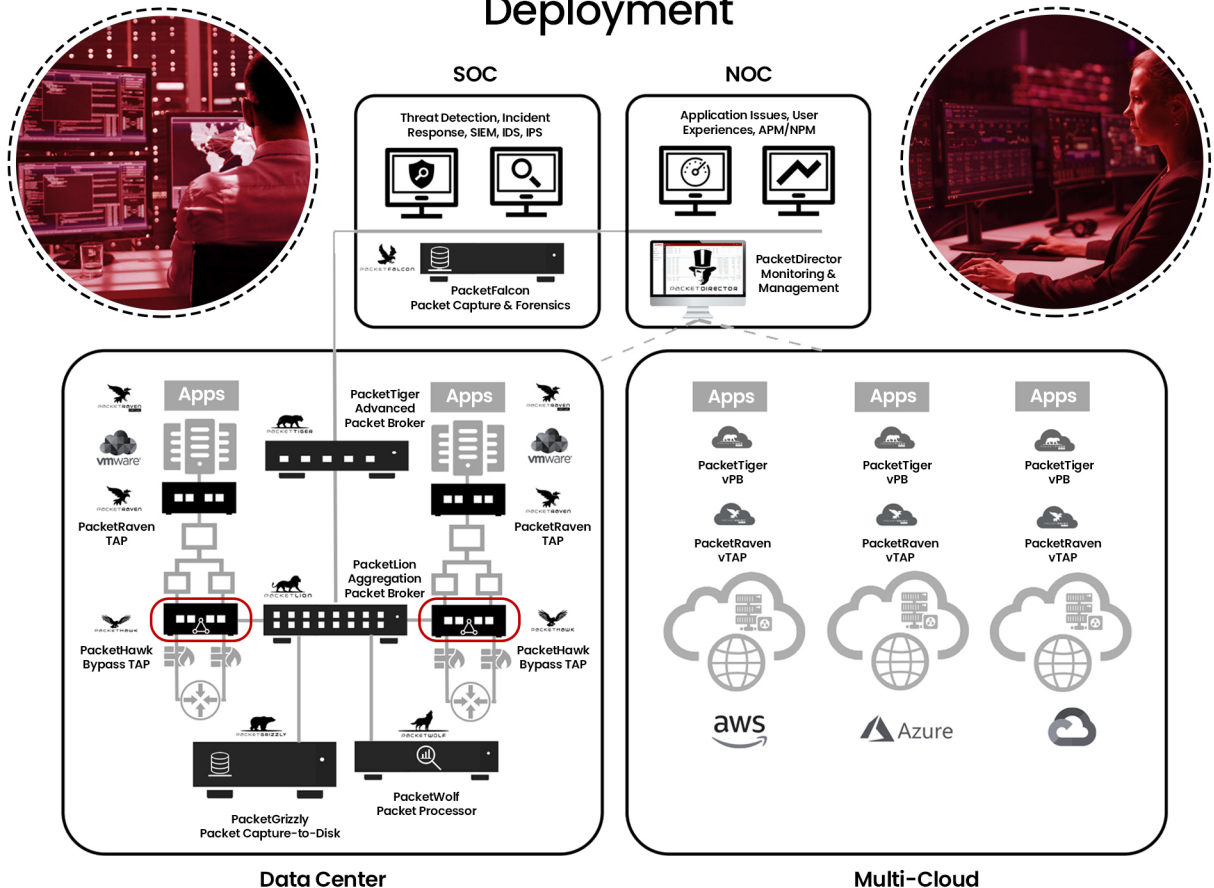
- Strengthened Network Security through Network Traffic Visibility across Hybrid-Cloud Infrastructure
- Real-Time Network Intelligence for Threat Detection and Network Detection and Response Tools
- Archived Network Data Access for Incident Response, Forensics, and Compliance



Application Performance

- Enhanced Application Performance, Responsiveness, and Availability through Network Visibility across Hybrid-Cloud Infrastructure
- Faster Troubleshooting for Application and User Experience Issues
- Reduced MTTR due to Always-On Network Visibility

Deployment



NEOXPacketHawk Inline Bypass TAP

Up to 100G | Modular | Service Chaining | Filtering

4x 100G QSFP28
Up to 4 x 100Gbps QSFP+/QSFP28

Modular Chassis

Service Chaining

Filtering

Breakout & Aggregation TAP Modes

User Specific Heartbeat

Made in Germany



SecurITy
made in Germany
Trust Seal
www.netops-001.com



Learn more at:
neoxn.eu/hawk



NEOXPacketHawk Advanced Features:

- Supports 10Gbps/40Gbps/100Gbps network inline bypass connectivity up to 2 inline devices on a single network
- 6 bypass modes: auto, semi-auto, force inline, force bypass, tap-separate, tap-aggregate
- Network and inline port health check and speed/duplex monitoring with heartbeat packets
- Link Loss Detection (LLD) in the event of a network connection failure
- Redundant bypass behavior in the event of a Bypass TAP failure: Active bypass, passive bypass
- Supports TAP mode: Net A, Net B traffic any-to-any mapping
- Supports mirror mode: mapping of Inline 1 to Inline 2, Inline 2 to Inline 1 port traffic
- Filtering by inline port IP, port: include or exclude

An Inline Bypass TAP is essential for maintaining uninterrupted data-in-motion delivery and ensuring seamless network and security operations without a compromise. It serves as a fail-safe mechanism in case of an "inline" network node or security tool failure, or maintenance activities, allowing traffic to continue to flow without disruption through an alternate protected route with a backup set of appliances and tools. Inline means that it must be deployed in the main traffic path.

- NEOXPacketHawk Inline Bypass TAP enables the network team to maintain uninterrupted connectivity and smooth network operation during downtime. It acts as a fail-safe mechanism if devices fail or require maintenance, allowing mainstream data center north-south data traffic to continue flowing without interruption. It also provides the flexibility to reroute traffic for security monitoring or analysis purposes without impacting the network performance.
- NEOXPacketHawk sends periodic heartbeat pulses to the inline security appliances network nodes and visibility tools (such as a network firewall, WAF, NIDS, and NIPS) and receives the responses. If the heartbeat is missed, it knows that the appliance is no longer functional. NEOXPacketHawk then automatically bypasses the appliance, rerouting the network traffic and ensuring that packet data continues to flow to its destinations. NEOXPacketHawk provides superior Bypass TAP functionality in hardware and at the actual wire level. It means that it physically reroutes the traffic in case of a network node or tool failure.
- NEOXPacketHawk allows NetOps and SecOps to perform maintenance and upgrades, or replace security or observability tools with peace of mind, without impacting the production network operations or causing downtime. This reduces risk and workload and increases business continuity and availability.



NEOXPacketLion & NEXOPacketTiger Hybrid-Cloud Packet Broker Series

Strengthening Cybersecurity, Hybrid-Cloud Application Observability,
and Business Continuity, by Integrating the Network Intelligence
and Forwarding the Right Data to the Right Tools



NEOXPacketLion & NEOXPacketTiger

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Forwarding the Right Data to the Right Tools

IT NetSecOps

IT NetAppOps

Data Center

Multi-Cloud



Business Benefits

- Increased Business Continuity and Reduced Downtime
- Enabling CXO's Digital Transformation through Hybrid-Cloud Visibility
- Reduced Customer Churn through Lower MTTR, Enhanced Security, and Information Protection



Technical Benefits

- Setup Once, Benefit Forever, Network Visibility and Real-Time Wire-Data Access
- Foundation Layer to Build a Hierarchical Network Monitoring and Observability Practice
- Consistent Tools and Methods for Network-as-a-Service across the Hybrid Infrastructure



Infrastructure Security

- Strengthened Network Security through Network Traffic Visibility across Hybrid-Cloud Infrastructure
- Real-Time Network Intelligence for Threat Detection and Network Detection and Response Tools
- Archived Network Data Access for Incident Response, Forensics, and Compliance



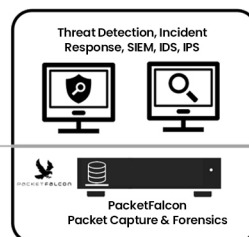
Application Performance

- Enhanced Application Performance, Responsiveness, and Availability through Network Visibility across Hybrid-Cloud Infrastructure
- Faster Troubleshooting for Application and User Experience Issues
- Reduced MTTR due to Always-On Network Visibility

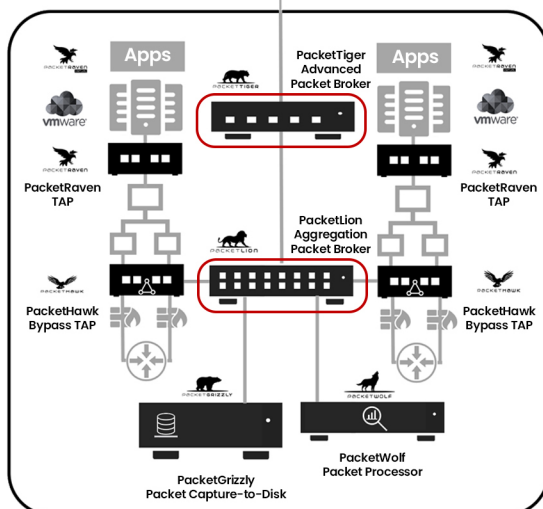
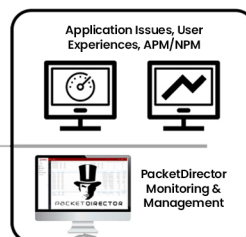
Deployment



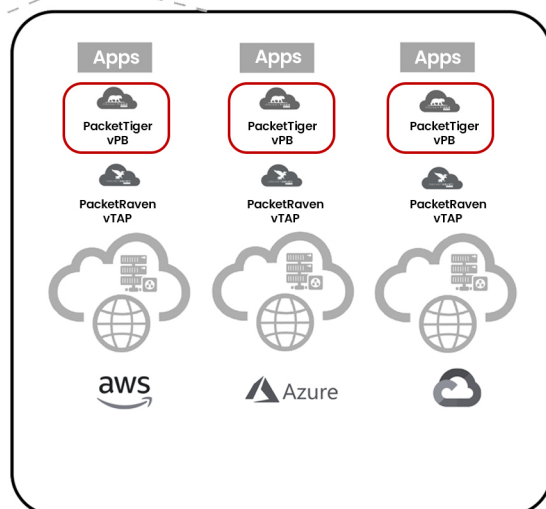
SOC



NOC




Data Center

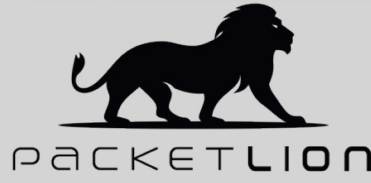


Multi-Cloud

NEOXPacketLion Packet Broker Series

Smart And High-Performance Network Packet Brokers With High Port Density

-  Up to 400Gbps
-  Port Splitting & Port Labeling
-  L3GRE Tunneling Protocol
-  Clustering Possible
-  Dig. Diagnostics Monitoring
-  Radius & TACACS
-  Flexible Port Allocation
-  Tunnel Filtering
-  Aggregation & Regeneration
-  User Defined Filter Rules
-  MPLS Stripping
-  Timestamping
-  Packet Slicing
-  8GB Deep Buffers
-  Development & QA in Germany



SecurITy
made in Germany

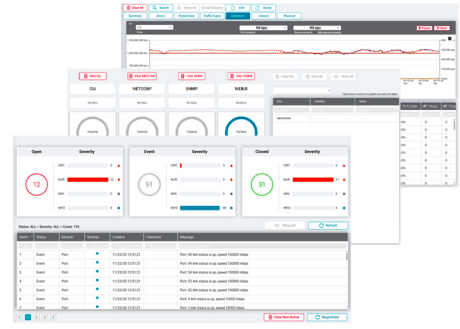


Learn more at:
neoxn.eu/lion



NEOXPacketLion Advanced Features:

- Flexible port assignment (1:1, N:N, N:1, 1:N)
- Aggregation of 1Gbps, 2.5Gbps, 10Gbps, 25Gbps, 40Gbps, 50Gbps, 100Gbps, 200Gbps and 400Gbps network ports
- Support for filtering rules (MAC, VLAN, IPv4/IPv6, TCP/UDP, DSCP, TCP Flags, MPLS, Ingress, Egress)
- Filtering within a tunnel (GTP, L2TP, MPLS, GRE, PPPoE, and VXLAN)
- 8GB Deep Buffer to eliminate packet loss because of micro bursts
- Aggregation and regeneration of any network traffic
- Support for User-Defined Filter rules (UDF)
- Multiple management options (CLI, SSH, SNMP V2/V3, WEB UI, Net CONF and REST API)
- Configure all NEOXPacketLion (and NEOXPacketTiger) Brokers via a Single-Pane-Of-Glass with our NEOXPacketDirector



A Network Packet Broker (NPB), also known as a Network Monitoring Switch, aggregates all data streams from Network TAPs distributed across the hybrid-cloud infrastructure, processes it to filter and manipulate the data to forward it in the right format, to the right destinations/tools, for monitoring and analysis.

- NEOXPacketLion Network Packet Broker acts as a high-density aggregation layer and a bridge between the network data access points i.e. TAPs, and the tool rail, such as security (NIDS, NIPS, NDR, SIEM), forensics (packet capture), and performance monitoring (APM, NPM) tools.
- NEOXPacketLion also acts as a gateway to interface network speeds of up to 400Gbps to lower speeds on the tools side, and depending on the version, supports all common transceiver standards (SFP, SFP+, QSFP-DD)
- NEOXPacketLion uses dedicated ASIC hardware to support simple or complex data filtering rules to ensure an optimized data flow, and the right data to the right analysis tools. It enables you to filter out unwanted data packets or entire data streams, thus reducing the overall load and tools-sprawl, and prolonging investments.

NEOXPacketTiger Packet Broker Series

Next Generation Network Packet Broker With Advanced Features

8x 100G Up to 8 x 100Gbps

NEOXPacketLion Parity Features

GTP Correlation

Data Masking

Deduplication

Advanced Filtering

NetFlow/IPFIX Support

Deep Packet Inspection

Tunnel Support

Packet Capture & Replay

GTP Tunneling & IMSI Filtering

Development & QA in Germany



Learn more at:
neoxn.eu/tiger



A Network Packet Broker (NPB), also known as a Network Monitoring Switch, aggregates all data streams from Network TAPs distributed across the hybrid-cloud infrastructure, processes it to filter and manipulate the data to forward it in the right format, to the right destinations/tools, for monitoring and analysis. Network protocols and tunnels change the format and length of the packets.

To gain insight into network traffic, in addition to the "metadata" extracted from the packet headers, the payload must also be analyzed. Such changes push the parsing capabilities of switch-ASIC-based NPBs to their limits and demand more sophisticated technologies and processing features.

- NEOXPacketTiger Advanced Network Packet Brokers allow full flexibility in parsing network packet headers and processing payloads and provide advanced technology for modifying and optimizing those packets.
- Advanced features such as IPv6-filtering in GTP tunneling, Regex, Deep Packet Inspection (DPI), and application-based metadata extraction are supported.
- NEOXPacketTiger uses modern, high-performance, modular, and scalable COTS hardware which can be configured for the desired processing capacity. This unique approach removes hardware performance constraints and enables better scaling and matching between hardware and performance requirements. The media type and speed of the network do not matter, as NEOXPacketTiger supports all major types (RJ45/SFP/SFP+/QSFP+/QSFP28 ports).
- The NEOXPacketTiger's advanced packet processing allows you to work more granularly and look deeper inside individual packets as compared to ordinary Network Packet Brokers. Even resource-intensive scenarios such as removing duplicates (dedup) in the network, masking, or blacking out content in the individual packets, are not an issue.
- NEOXPacketTiger Advanced Network Packet Brokers are available in different categories: Desktop Appliances, Network Appliances, and Servers, enabling a wide range of solutions.
- All in all, the NEOXPacketTiger Next-Gen Advanced Network Packet Brokers have significantly more functionalities and features for advanced applications across mission-critical data centers.

NEOXPacketTigerVirtual Virtual Packet Broker

Network Visibility in Hybrid-Cloud, Multi-Cloud, and On-Prem Virtual Environments



Virtual & Cloud Environments



GTP Correlation & Filtering



Inner IP LB & Tunnel Filtering



OSI L2-L4 & RegEx Filtering



User Defined Filters



Header Stripping & Editing



Deduplication



Data Masking



Packet Slicing



Metadata Extraction



Timestamping



Capture & Replay



NetFlow/IPFIX



NEOX Device Manager

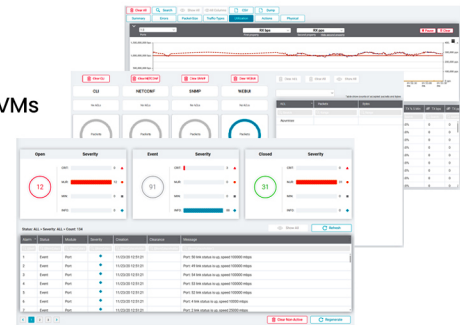


Learn more at:
neoxn.eu/vtiger



NEOXPacketTigerVirtual Advanced Features:

- Extend network visibility to virtual and cloud network traffic
- Aggregate traffic from multiple vTAPs from cloud VPCs or VMware VMs
- Redirect virtual network traffic to central monitoring/observability tool rail on-prem or in the cloud VPC
- Balance and optimize virtual and physical monitoring tools by filtering data



A Virtual Packet Broker (vPB) works just like a physical Network Packet Broker, as a scaled-down version that can run on a standard hypervisor in the virtualized data center or the cloud. It can aggregate, filter, and process the network traffic between the virtual machines (VM) in the east-west direction, and forward to the tools for monitoring and analysis, which is otherwise a major blind spot.

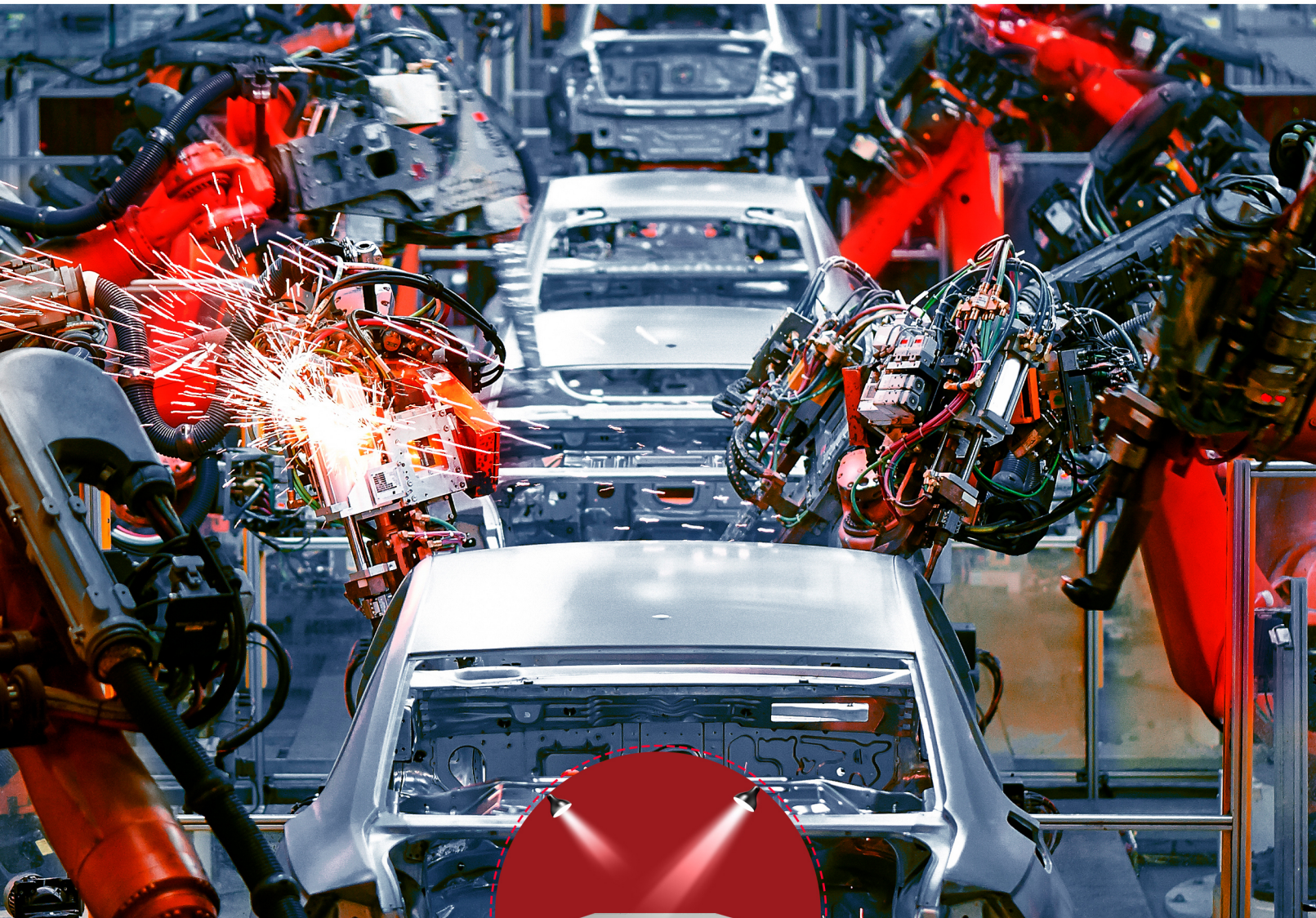
- NEOXPacketTigerVirtual provides a versatile Virtual Network Packet Broker solution to meet the need for increased visibility in virtualized environments such as Software-Defined Data Centers (SDDC), and public/private clouds, completing the equation. So you have end-to-end visibility of the hybrid-cloud/multi-cloud environment.
- Deployable as a Docker container, or as a virtual appliance, NEOXPacketTigerVirtual is validated and deployable in AWS, Microsoft Azure, and Google Cloud and can collect network data streams from multiple NEOXPacketRavenVirtual vTAPs within a VPC, and optimize the cloud network data processing and forwarding, reducing the cloud bills and improving security.
- NEOXPacketTigerVirtual can provide similar benefits in an on-premises virtual network, such as a VMware environment. Since most malware attacks enter through data center east-west traffic, this greatly reduces the security gaps and blind spots and completes the visibility picture.
- NEOXPacketTigerVirtual can also be deployed in a virtualized branch edge to provide visibility, such as in an SDWAN connectivity use case.



PACKETWOLF

NEOX PacketWolf Packet Processing

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Advanced Packet Processing and Analysis



NEOX PacketWolf Packet Processing

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Advanced Packet Processing and Analysis

IT NetSecOps

IT NetAppOps

Data Center

Multi-Cloud

Business Benefits

- Increased Business Continuity and Reduced Downtime
- Enabling CXO's Digital Transformation through Hybrid-Cloud Visibility
- Reduced Customer Churn through Lower MTTR, Enhanced Security, and Information Protection

Technical Benefits

- Setup Once, Benefit Forever, Network Visibility and Real-Time Wire-Data Access
- Foundation Layer to Build a Hierarchical Network Monitoring and Observability Practice
- Consistent Tools and Methods for Network-as-a-Service across the Hybrid Infrastructure

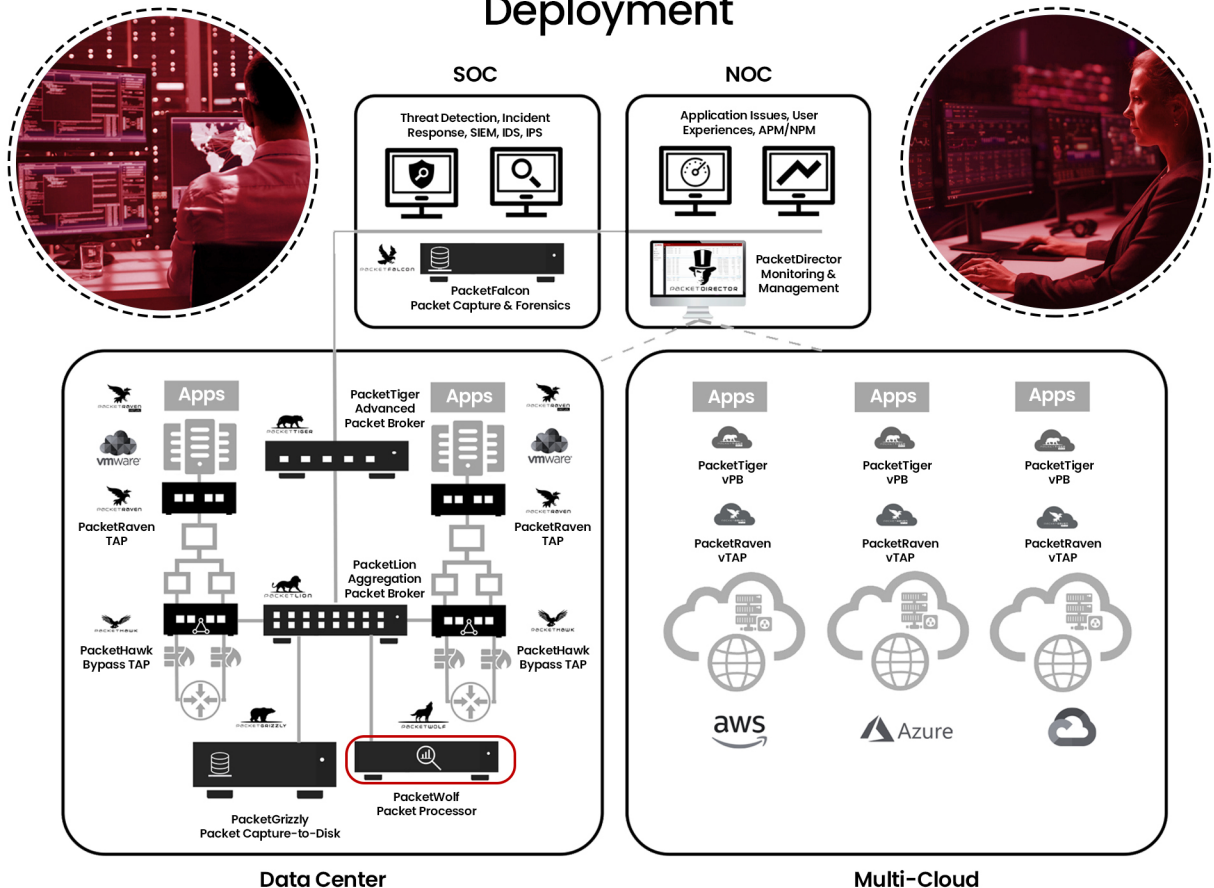
Infrastructure Security

- Strengthened Network Security through Network Traffic Visibility across Hybrid-Cloud Infrastructure
- Real-Time Network Intelligence for Threat Detection and Network Detection and Response Tools
- Archived Network Data Access for Incident Response, Forensics, and Compliance

Application Performance

- Enhanced Application Performance, Responsiveness, and Availability through Network Visibility across Hybrid-Cloud Infrastructure
- Faster Troubleshooting for Application and User Experience Issues
- Reduced MTTR due to Always-On Network Visibility

Deployment



NEOXPacketWolf Packet Processing

Advanced FPGA-based Packet Processing and Deep Packet Inspection

4x 100G QSFP28
Up to 4 x 100Gbps SFP28/QSFP28

Up to 400Gbps

FPGA Design

FPGA-based Nanosecond Timestamping

FPGA-based Deduplication

FPGA-based Packet Slicing

Protocol Header Stripping

Made in Germany



SecurITy
made in Germany
Trust Seal
www.teletrust.de/itsec



Learn more at:
neoxn.eu/wolf



The Packet Processing appliance is equipped with advanced architecture to process the network data at the individual packet level. This involved Deep Packet Inspection (DPI) technology at the hardware level for labor-intensive but faster lookups. A Packet Processing appliance can be deployed as a complement to a Network Packet Broker or as a stand-alone in an existing network monitoring infrastructure.

- The NEOXPacketWolf Advanced Packet Processing appliance is the ideal platform for advanced network data packet processing of up to 400Gbps throughput per appliance, thanks to its FPGA-based high-performance architecture.
- The data traffic requiring processing is normally fed through a basic Network Packet Broker such as NEOXPacketLion series or third-party packet brokers, but can also originate from other sources, such as a SPAN port or a Network TAP. The processed data is forwarded by NEOXPacketWolf on the same or a separate port to a monitoring/security tool destination or sent back to the source. Advanced packet brokers like NEOXPacketTiger do not need NEOXPacketFalcon to complement due to built-in packet processing capabilities.
- NEOXPacketWolf Advanced Packet Processing appliance offers several advanced features to offload the monitoring and observability tools through deduplication, advanced filtering, packet masking, packet slicing, dynamic and static header-stripping, tunnel termination, VLAN tagging, L2-L3-L4 loopback, PCAP view, replay, and edit.
- Additionally, functions such as packet slicing and packet masking can ensure meeting legal and compliance requirements. Particularly with GDPR, it may be necessary to use packet slicing to remove the user data before forwarding, or mask the personal information, as the metadata is often sufficient for an analysis.



NEOXPacketFalcon & NEXOPacketGrizzly 100G Packet Capture & Analysis Series

Strengthening Cybersecurity, Hybrid-Cloud Application Observability,
and Business Continuity, by Integrating the Network Intelligence
and Historic Data Correlation



NEOXPacketFalcon & NEXOPacketGrizzly

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Historic Data Correlation

IT NetSecOps

IT NetAppOps

Data Center

Multi-Cloud

Business Benefits

- Increased Business Continuity and Reduced Downtime
- Enabling CXO's Digital Transformation through Hybrid-Cloud Visibility
- Reduced Customer Churn through Lower MTTR, Enhanced Security, and Information Protection

Technical Benefits

- Setup Once, Benefit Forever, Network Visibility and Real-Time Wire-Data Access
- Foundation Layer to Build a Hierarchical Network Monitoring and Observability Practice
- Consistent Tools and Methods for Network-as-a-Service across the Hybrid Infrastructure

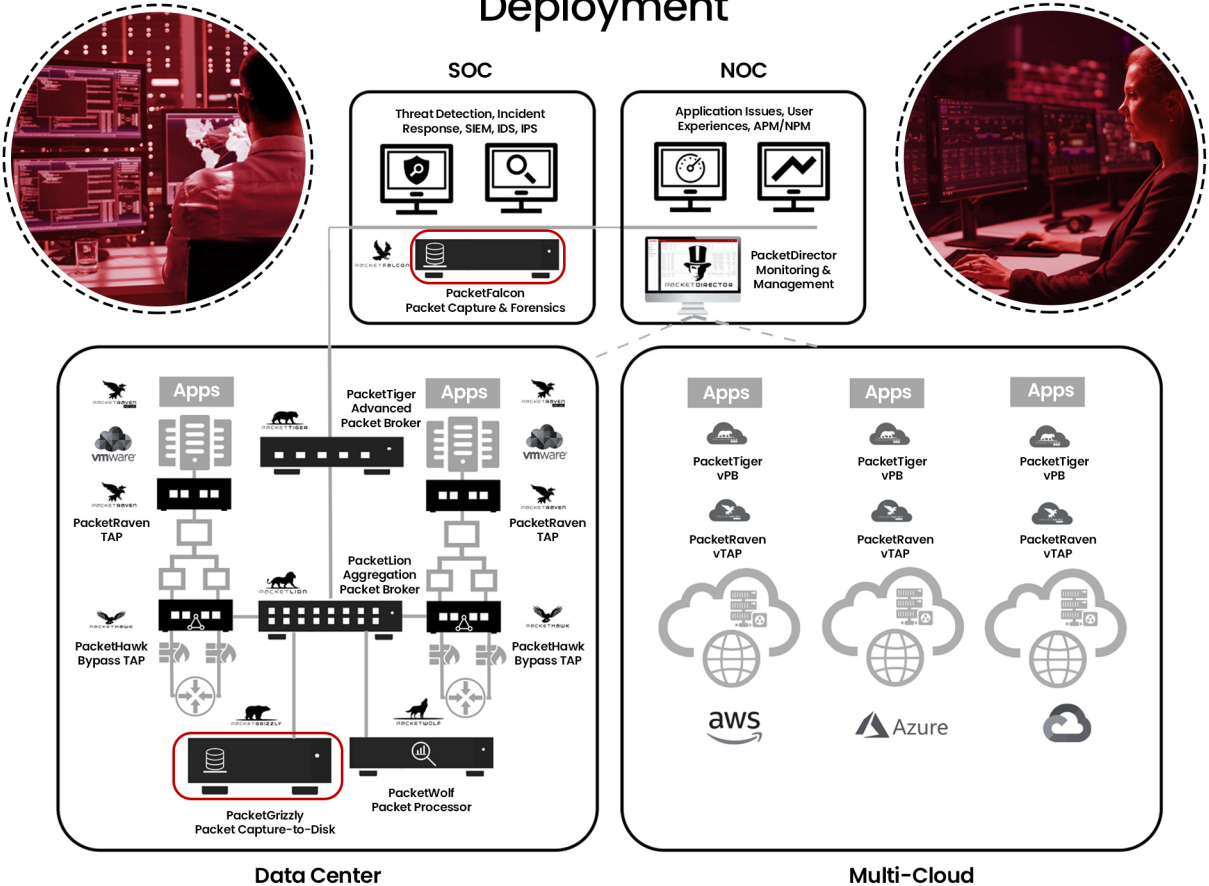
Infrastructure Security

- Strengthened Network Security through Network Traffic Visibility across Hybrid-Cloud Infrastructure
- Real-Time Network Intelligence for Threat Detection and Network Detection and Response Tools
- Archived Network Data Access for Incident Response, Forensics, and Compliance

Application Performance

- Enhanced Application Performance, Responsiveness, and Availability through Network Visibility across Hybrid-Cloud Infrastructure
- Faster Troubleshooting for Application and User Experience Issues
- Reduced MTTR due to Always-On Network Visibility

Deployment



NEOXPacketFalcon Portable 100G Packet Capture

Portable, Ultra-Fast, Packet Capture-to-Disk, Indexing, and Search, for Analysis, Security Forensics, and Compliance



Lossless Recording up to 100Gbps



Up to 3 FPGA Capture Cards



Storage Capacity of up to 240TB



HW Encrypted Capture Storage



FPGA-based Nanosecond Timestamping



FPGA-based Packet Slicing & Capture Filter



FPGA-based Deduplication



Hardware RAID 0,5,6,00,50,60



PCAP & PCAPNG Support



Optional Transport Case



Made in Germany

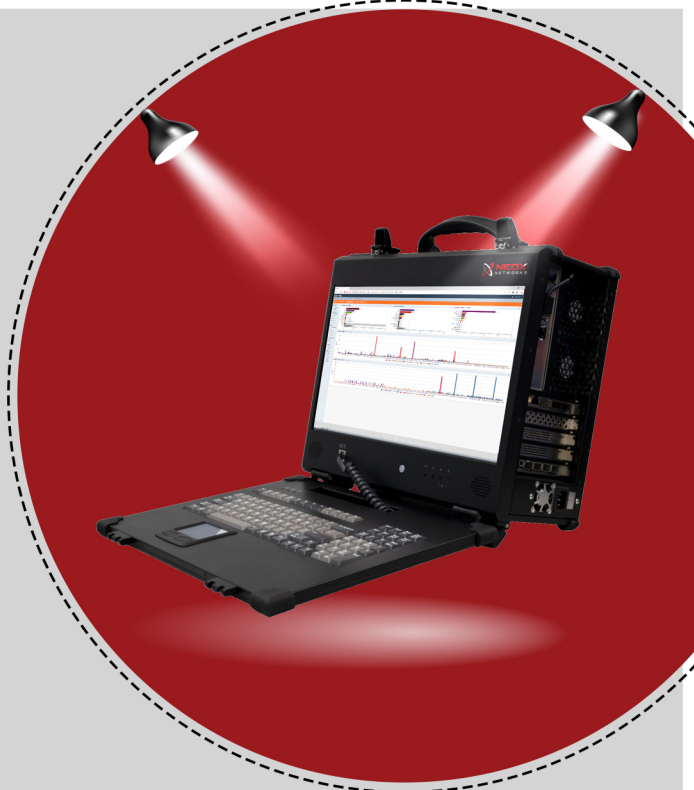


PACKETFALCON

SecurITy
made in Germany
Trust Seal
www.securit.com



Learn more at:
neoxn.eu/falcon



A Packet Capture Appliance uses specialized high-performance hyper-converged architecture to capture/record the network data in motion in a lossless fashion and store it permanently on built-in storage disks. The stored data can be retrieved and played back at any time just like a DVR, for troubleshooting, security forensics, or evidence.

- NEOXPacketFalcon Portable Packet Capture Appliance is a powerful solution to record the network packet data for up to 100Gbps speeds (1Gbps, 10Gbps, 25Gbps, 40Gbps, or 100Gbps). The onboard storage capacity options include 24TB, 51TB, 102TB, or 240TB of disk space depending on the use case and the length of the time the data must be stored.
- NEOXPacketFalcon enables IT NetOps and AppOps teams to reference the historical data at any time at their fingertips, recreate the data streams for troubleshooting, and perform session or conversation-level analysis, reducing finger-pointing and mean-time-to-resolution (MTTR) of customer issues.
- NEOXPacketFalcon is a must-have solution for network forensics and incident response for the IT SecOps teams in a post-breach situation for investigation and court evidence. The before, during, and after event data captured, can help narrow down the security loopholes, suspicious activities, and attacker's IP address.

NEOXPacketFalcon Compact 100G Packet Capture

Compact, Ultra-Fast Packet Data Capture-to-Disk, Indexing, and Search, for Analysis, Security Forensics, and Compliance



Lossless Recording up to 100Gbps



High-End FPGA Capture Cards



For 1Gbps-100Gbps Networks



Storage Capacity of up to 61TB



IEEE 1588v2 Precision Time Protocol



Portable & Rackmountable



FPGA-based Packet Slicing & Capture Filter



FPGA-based Nanosecond Timestamping



FPGA-based Deduplication



PCAP & PCAPNG Support



Cascading Possible



Optional Transport Case



Made in Germany



Security
made in Germany



Learn more at:
neoxn.eu/falconc



- NEOXPacketFalcon Compact Packet Capture Appliance is a powerful solution to record the network packet data for up to 100Gbps speeds (1Gbps, 10Gbps, 25Gbps, 40Gbps, or 100Gbps). The onboard storage capacity options include 31TB or 61TB of disk space depending on the use case and the length of the time the data must be stored. Its flexibility in terms of mobile and stationary applications makes it the ideal companion for NetSecOps. A hard-shell transport case is optionally available.
- NEOXPacketFalcon enables IT NetOps and AppOps teams to reference the historical data at any time at their fingertips, recreate the data streams for troubleshooting, and perform session or conversation-level analysis, reducing finger-pointing and mean-time-to-resolution (MTTR) of customer issues.
- NEOXPacketFalcon is a must-have solution for network forensics and incident response for the IT SecOps teams in a post-breach situation for investigation and court evidence. The before, during, and after event data captured, can help narrow down the security loopholes, suspicious activities, and attacker's IP address. By indexing the data and hardware/software filters (Berkeley Packet Filter), NEOXPacketFalcon enables SecOps teams to quickly investigate and block attacks.

NEOXPacketFalcon Mini 25G Packet Capture

Portable, Compact, Ultra-Fast Packet Data Capture-to-Disk, Indexing, and Search, for Analysis, Security Forensics, and Compliance



Lossless Recording up to 25Gbps



High Speed FPGA Capture Cards



Storage up to 32TB



Portable, Compact and Robust



Flexible due to SFP/SFP+/SFP28



FPGA-based Nanosecond Timestamping



FPGA-based Packet Slicing & Capture Filter



FPGA-based Deduplication



Lossless Full Packet Capture



PCAP & PCAPNG Support



IPFIX/NetFlow Export



Cascading Possible



Made in Germany



PACKETFALCON

SecurITy
made in Germany
Trust Seal
www.telecrat.de/iamity



Learn more at:
neoxn.eu/falconm



- NEOXPacketFalcon Mini Packet Capture Appliance is a powerful solution to record the network packet data for up to 25Gbps speeds (1Gbps, 10Gbps, or 25Gbps). The onboard storage capacity options include 8TB, 16TB, or 32TB of disk space depending on the use case and the length of time the data must be stored.
- NEOXPacketFalcon enables IT NetOps and AppOps teams to reference the historical data at any time at their fingertips, recreate the data streams for troubleshooting, and perform session or conversation-level analysis, reducing finger-pointing and mean-time-to-resolution (MTTR) of customer issues.
- NEOXPacketFalcon is a must-have solution for network forensics and incident response for the IT SecOps teams in a post-breach situation for investigation and court evidence. The before, during, and after event data captured, can help narrow down the security loopholes, suspicious activities, and attacker's IP address. By indexing the data and hardware/software filters (Berkeley Packet Filter), NEOXPacketFalcon enables SecOps teams to quickly investigate and block attacks.

NEOXPacketGrizzly 100G Packet Capture

Modular and Scalable, Ultra-Fast Packet Data Capture-to-Disk, Indexing, and Search, for Analysis, Security Forensics, and Compliance



Up to 100Gbps



High Speed FPGA Capture Cards



Storage Capacity of up to 8PB



HW Encrypted Capture Storage



IEEE 1588v2 Precision Time Protocol



FPGA-based Nanosecond Timestamping



FPGA-based Packet Slicing & Capture Filter



FPGA-based Deduplication



Hardware RAID or ADAPT



PCAP & PCAPNG Support



Supports SSL Decryption



Made in Germany



SecurITy
made in Germany



Learn more at:
neoxn.eu/grizzly



- NEOXPacketGrizzly Modular Packet Capture appliance is a powerful, industry-leading solution to record-network packet data for up to 100Gbps speeds (1Gbps, 10Gbps, 25Gbps, 40Gbps, or 100Gbps). The onboard storage capacity options include 504TB to 8PB of disk space, and up to 4 storage units, depending on the use case and the length of time the data must be stored. NEOXPacketGrizzly can accommodate the failure of up to 12 drives per unit without any data loss, setting a high bar for availability.
- NEOXPacketGrizzly supports Ethernet, VoIP, Video over IP network, and session-level or conversation-level analysis, and enables IT NetOps and AppOps teams to reference the historical data at any time at their fingertips, recreate the data streams for troubleshooting, reducing finger-pointing and mean-time-to-resolution (MTTR) of customer issues. High capture speed and ample storage capacity make NEOXPacketGrizzly a superior solution for NetOps to go back to network data for days, weeks, and months, to catch anomalies.
- NEOXPacketGrizzly is a must-have solution for network forensics and incident response for the IT SecOps teams in a post-breach situation for investigation and court evidence. The before, during, and after event data captured, can help narrow down the security loopholes, suspicious activities, and attacker's IP address. By indexing the data and hardware/software filters (Berkeley Packet Filter), NEOXPacketFalcon enables SecOps teams to quickly investigate and block attacks.
- As encrypted traffic becomes more common, NEOXPacketGrizzly can detect the encrypted traffic and slice the encrypted payload from the packets to extend the retention time. This is processed in the FPGA without any performance impact.

NEOX PacketDirector Network Management

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Single-Pane-of-Glass Manageability



NEOX PacketDirector Network Management

Strengthening Cybersecurity, Hybrid-Cloud Application Observability, and Business Continuity, by Integrating the Network Intelligence and Single-Pane-of-Glass Manageability

IT NetSecOps

IT NetAppOps

Data Center

Multi-Cloud

Business Benefits

- Increased Business Continuity and Reduced Downtime
- Enabling CXO's Digital Transformation through Hybrid-Cloud Visibility
- Reduced Customer Churn through Lower MTTR, Enhanced Security, and Information Protection

Technical Benefits

- Setup Once, Benefit Forever, Network Visibility and Real-Time Wire-Data Access
- Foundation Layer to Build a Hierarchical Network Monitoring and Observability Practice
- Consistent Tools and Methods for Network-as-a-Service across the Hybrid Infrastructure

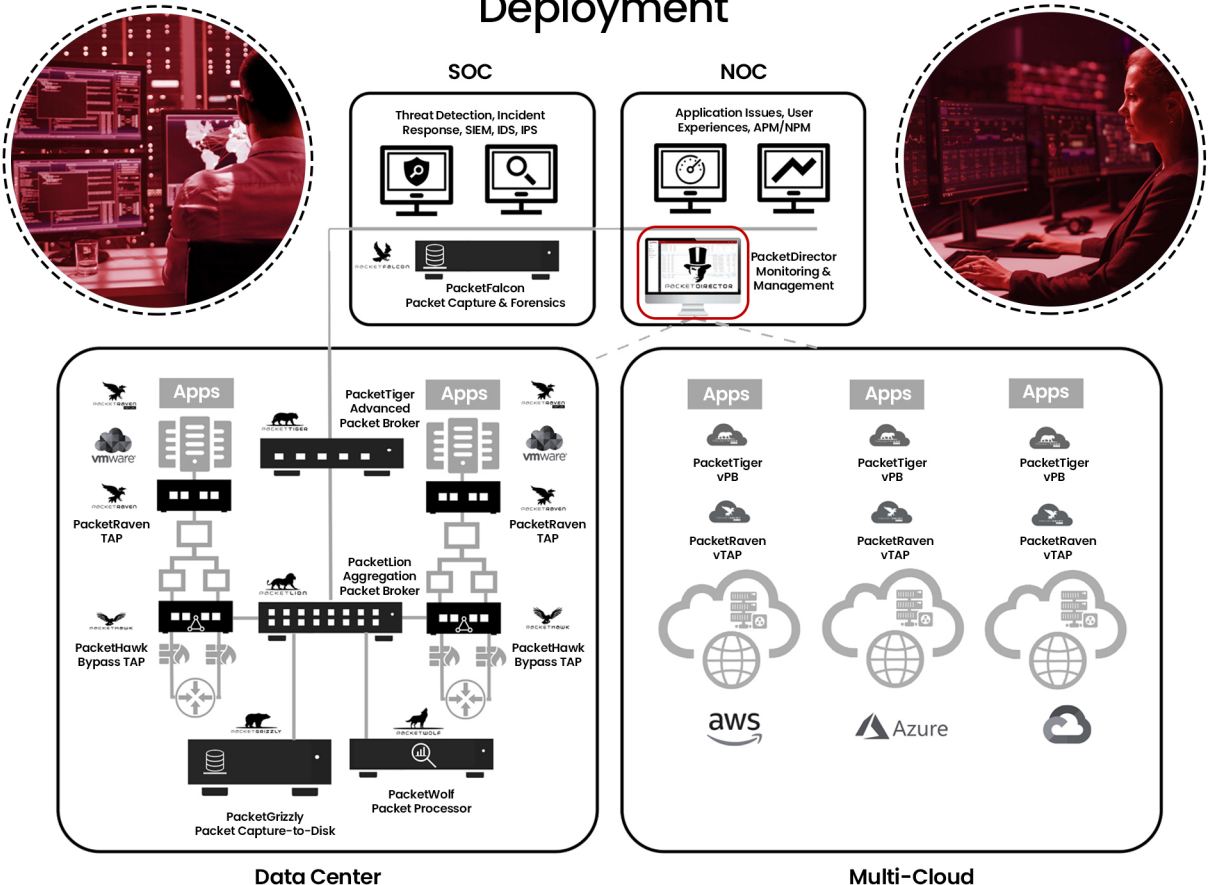
Infrastructure Security

- Strengthened Network Security through Network Traffic Visibility across Hybrid-Cloud Infrastructure
- Real-Time Network Intelligence for Threat Detection and Network Detection and Response Tools
- Archived Network TAP Data Access for Incident Response, Forensics, and Compliance

Application Performance

- Enhanced Application Performance, Responsiveness, and Availability through Network Visibility across Hybrid-Cloud Infrastructure
- Faster Troubleshooting for Application and User Experience Issues
- Reduced MTTR due to Always-On Network Visibility

Deployment



NEOXPacketDirector Network Management

Single-Pane-of-Glass Scalable Hybrid-Cloud Packet Broker Manager

-  Auto Discovery
-  Statistics Collection
-  Bulk Operation
-  Alarms Collection
-  Elastic Database
-  Graphical Dashboards
-  Email Notifications
-  Scheduler for Bulk Tasks
-  Upgrade Manager
-  Configuration Backup



Secur|Ty
made in Germany

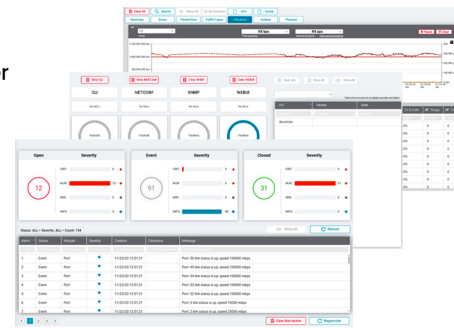


Learn more at:
neoxn.eu/dir



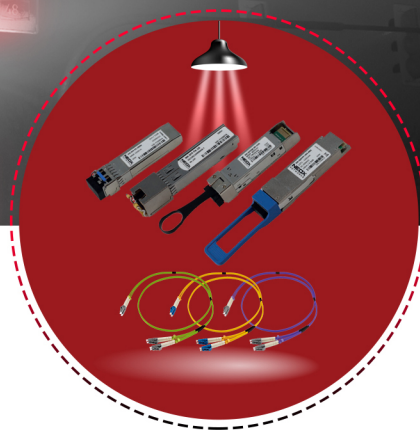
NEOXPacketDirector Advanced Features:

- Software-based solution that is available as both VM and container
 - Single tool for centralized management of both Neox physical and virtual Packet Brokers
 - Scheduler for bulk operations and tasks for multiple devices (configuration, backup, upgrade, reboot, scripting)
 - Centralized filter and rule management per-device rules and across-device rules via clustering
 - Clustering of up to 100 Neox Network Packet Brokers into a single unit, allowing for policy definition between cross-connected devices
-
- NEXOPacketDirector is a centralized management system for NEXOPacketLion, NEXOPacketTiger, and NEXOPacketTigerVirtual Series Packet Brokers to provision, monitor, and manage those in a single-pane-of-glass fashion. This greatly reduced the workload on NetOps and SecOps teams across large distributed hybrid or multi-site environments.
 - NEXOPacketDirector is a software-based solution that can be deployed as a VM or container on-prem or in the cloud.
 - NEXOPacketDirector enables the auto-discovery and management of hundreds of Neox physical and virtual Network Packet Brokers. It collects network statistics and traffic telemetry stored in elastic databases and displayed in real-time graphic visualization utilizing Kibana and Grafana dashboards. Users can define different events and triggers per device according to cross-device events, and alarms and events trigger email notifications from the NEXOPacketDirector.



Optical Transceivers and Cables

Strengthening Cybersecurity, Hybrid-Cloud Application Observability,
and Business Continuity, by Integrating the Network Intelligence
and Faster and Reliable Connectivity



Optical Transceivers and Cables

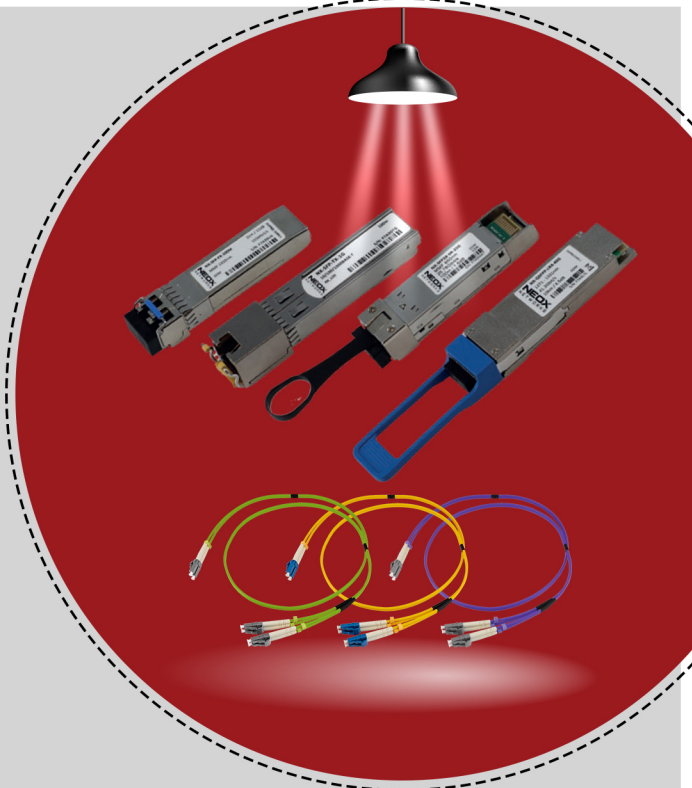
Pre-Qualified Faster and Reliable Connectivity



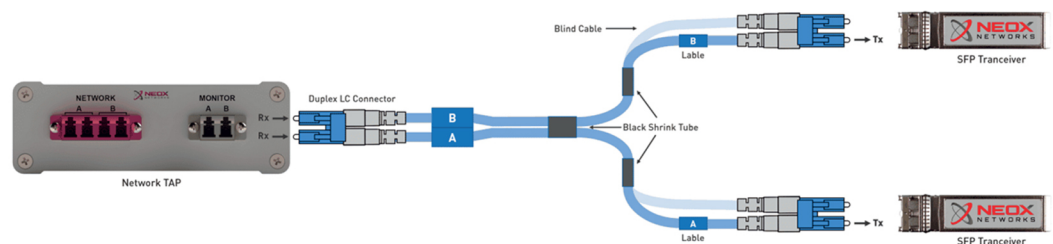
Learn more at:
neoxn.eu/trans



Learn more at:
neoxn.eu/ycable

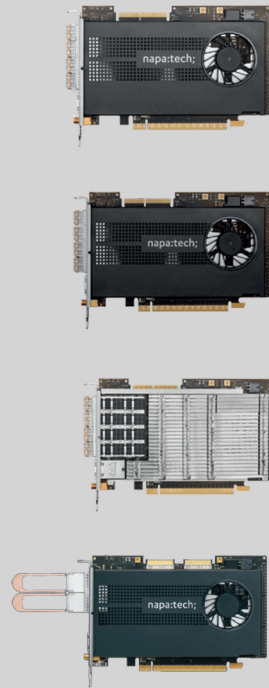


- Neox optical transceivers are pre-qualified with all Neox Next-Generation Network Visibility appliances for risk-free connectivity to the data center fabric, switches, or routers. Those are universally applicable and meet the highest quality requirements.
- Optical transceivers are MSA compliant and can therefore be used in Neox products, but also with devices from other manufacturers. Those are available for network connectivity of 1Gbps-400Gbps using standard SFP, SFP+, SFP28, QSFP+, QSFP28, QSFP56, or QSFP-DD.
- Neox pre-qualified cables and fibers assure risk-free connectivity for plug-and-play and faster deployment of the network visibility equipment. A NEOXPacketRaven TAP equipped with LC connectors has three duplex connectors, two of which are needed for looping through the network traffic to be analyzed, and one duplex connector for passively tapping the mirrored data for forwarding to a NEOXPacketTiger Network Packet Broker, an analysis or security tool (such as IDS/IPS).
- Data traffic is present on both sides of the monitoring port. Those two outputs must be fed into two monitoring ports using two transceivers to fully receive the bi-directional traffic, as only the receive side (Rx) of the transceivers can be used for recording. This presents a challenge because the output of the TAP is a duplex port, yet two separate ports are needed on the Rx side for two individual transceivers. To avoid this problem, it is best to use one of Neox's special Y-cables that converts one duplex connector into two duplex connectors so that the light is fed exclusively into the Rx side of the transceivers.



Accessories

Capture Cards, Mounting Kits, Transport Cases



Following Neox accessories are available for customization and extra care of Neox products during shipment, prolonging investments:

- High-performance Capture Cards for NeoxPacketFalcon and NEOXPacketGrizzly Packet Capture Appliances
- Network TAP mounting kits and cover plates for data center server racks, and DIN hat rails for NEOXPacketRaven series
- Robust transport cases
- Standard fiber optics cables, M12 cables, fan out cables, fiber loopback adapter, hat rail kits, etc.



NEOX NETWORKS GmbH

Monzastr. 4

63225 Langen

Germany

neox-networks.com

solutions@neox-networks.com

+49 6103 / 37 215 910