NEOX NETWORKS

NEXT GENERATION NETWORK VISIBILITY

Product Brochure

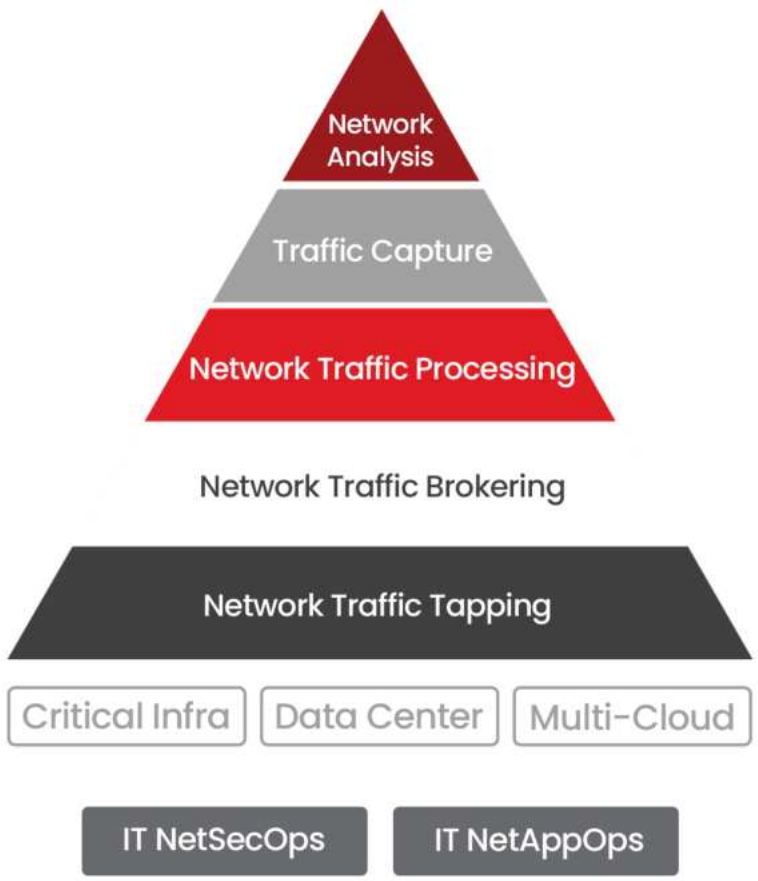
Next-Generation Network Visibility for IT & OT Observability and Security

Download

NEOX NETWORKS

NEOX Network Visibility Platform

Next-Generation Network Visibility for IT & OT Observability and Security



Business Benefits

- Digital Transformation and Modernization through Hybrid-Cloud Observability
- Increased Business Continuity and Reduced Downtime
- Reduced Customer Churn through Better Experiences, Enhanced Security, and Data Protection

Technical Benefits

- Setup Once, Monitor Forever Network Visibility and Real-Time Wire-Data Access for Tools
- Scalable Foundation Layer for Building a Network Monitoring, Security, and Observability Practice
- Consistent Network Visibility for Provisioning Network-as-a-Service across the Hybrid-Cloud Infrastructure

Security & Data Protection

- Strengthened Network Security through Direct Access and Consolidation of Network Packet Data
- Real-Time Network Intelligence for Threat Hunting and Network Detection and Response
- Historic Network Data Access for Forensics, Incident Response, and Compliance

Application Observability

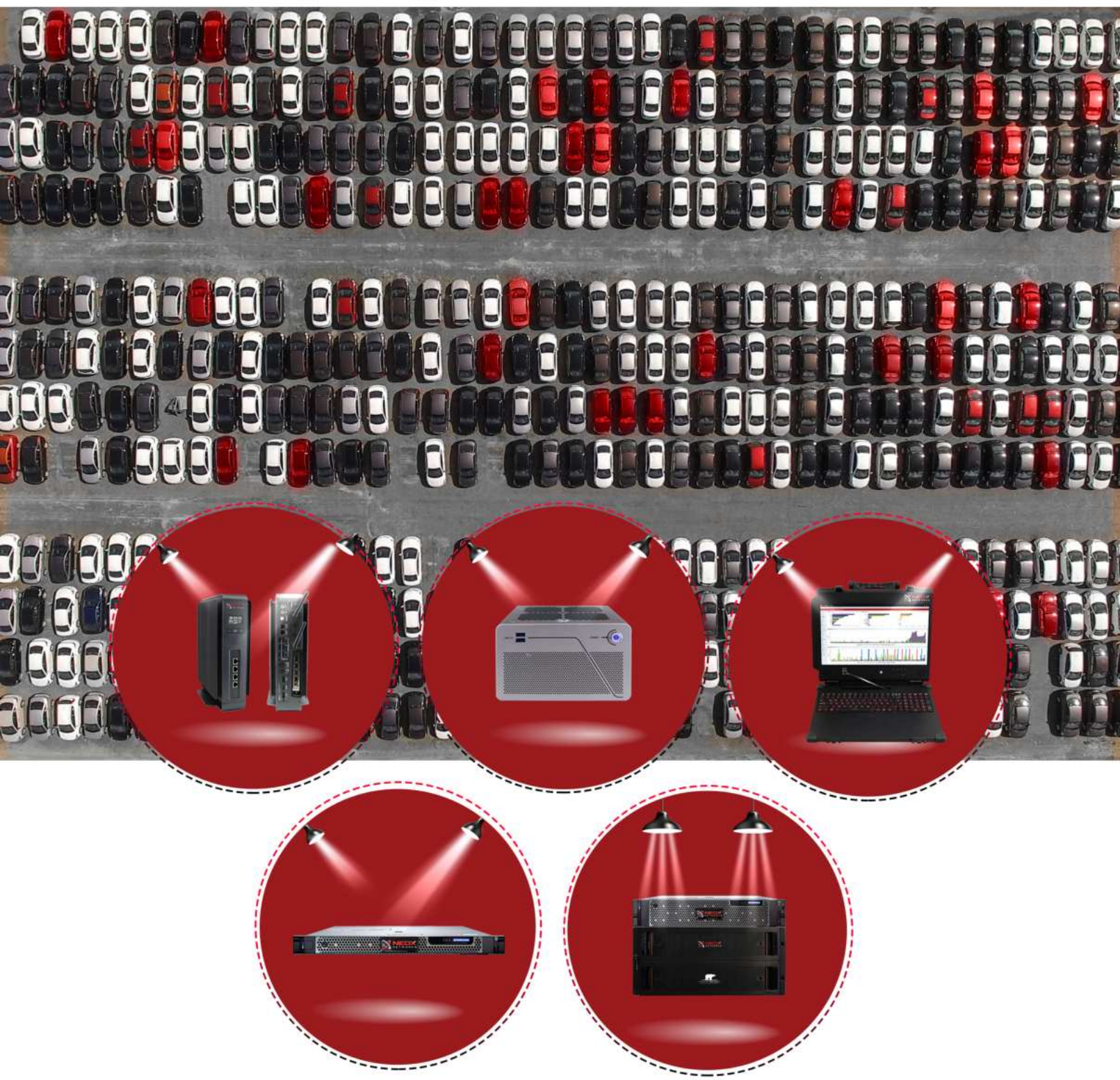
- Enhanced Application Performance, Response, and Availability through Network Dependency Mapping
- Faster Troubleshooting for User Experience Issues
- Reduced Mean-Time-to-Resolution

NEOX NETWORKS

PACKETFALCON PACKETGRIZZLY

NEOXPacketFalcon & NEOXPacketGrizzly Packet Capture & Analysis Series

Strengthening Cybersecurity and Application Observability by Integrating the Historic Network Data and Forensics



NEOX NETWORKS

Packet Capture

NEOXPacketFalcon Mini Capture Appliance

Portable & Compact | 10Gbps Capture-to-Disk | 32TB Storage
Security Forensics | Compliance | Out-of-Box Dashboards

- Lossless Full Packet Capture
- Sustained Capture-to-Disk up to 10Gbps
- High-Speed FPGA Capture Cards
- Intelligent & Compression-based Capture
- Storage up to 32TB
- Portable, Compact and Robust
- Fanless Design
- Flexible Connectivity through SFP/SFP+/SFP28
- FPGA-based 10 Nanosecond Timestamping
- FPGA-based Packet Slicing & Capture Filter
- FPGA-based Deduplication
- PCAP & PCAPNG Support

PACKETFALCON

neoxnetworks.com/
packetfalcon-packet-capture

Incident Response | Network Forensics | Troubleshooting

Compliance | Branch Office | Remote Site

- NEOXPacketFalcon Mini Packet Capture Appliance is a powerful solution to record the network packet data for up to 10Gbps speeds. 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.

NEOX NETWORKS

Packet Capture

NEOXPacketFalcon Mini X Capture Appliance

Portable & Compact | 25Gbps Capture-to-Disk | 32TB Storage
Security Forensics | Compliance | Out-of-Box Dashboards

- Lossless Full Packet Capture
- Sustained Capture-to-Disk up to 25Gbps
- High-Speed FPGA Capture Cards
- Intelligent & Compression-based Capture
- Storage up to 32TB
- Portable, Compact and Robust
- Fanless Design
- Flexible Connectivity through SFP/SFP+/SFP28
- FPGA-based 10 Nanosecond Timestamping
- FPGA-based Packet Slicing & Capture Filter
- FPGA-based Deduplication
- PCAP & PCAPNG Support

PACKETFALCON

neoxnetworks.com/
packetfalcon-packet-capture

Incident Response | Network Forensics | Troubleshooting

Compliance | Branch Office | Remote Site

- NEOXPacketFalcon Mini X Packet Capture Appliance is a powerful solution to record the network packet data for up to 25Gbps speeds. 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 converstion-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.

NEOX NETWORKS

Packet Capture

NEOXPacketFalcon Portable Capture Appliance

Portable & Mobile | 100Gbps Capture-to-Disk | 480TB Storage
Security Forensics | Compliance | Out-of-Box Dashboards

- Lossless Full Packet Capture
- Sustained Capture-to-Disk up to 100Gbps
- Up to 3 FPGA Capture Cards
- Intelligent & Compression-based Capture
- Storage Capacity of up to 480TB
- HW Encrypted (SED) Storage
- Hardware RAID 0,5,6,00,50,60
- Portable, Mobile, and Robust
- Flexible Connectivity through SFP, SFP+, SFP28, QSFP+, QSFP28
- FPGA-based 10 Nanosecond Timestamping
- FPGA-based Packet Slicing & Capture Filter
- FPGA-based Deduplication
- PCAP & PCAPNG Support
- Optional Transport Case

PACKETFALCON

neoxnetworks.com/
packetfalcon-packet-capture

Incident Response | Network Forensics | Troubleshooting

Compliance | Field | Remote Site

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, 240TB, or 480TB 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.

NEOX NETWORKS

Packet Capture

NEOXPacketGrizzly Capture Appliance

Modular & Extensible | 100Gbps Capture-to-Disk | 8PB Storage
Security Forensics | Compliance | Out-of-Box Dashboards

- Lossless Full Packet Capture
- Sustained Capture-to-Disk up to 100Gbps
- High-Speed FPGA Capture Cards
- Intelligent & Compression-based Capture
- Storage Capacity of up to 8PB
- HW Encrypted (SED) Storage
- Hardware RAID 0,5,6,00,50,60 & ADAPT
- IEEE 1588v2 Precision Time Protocol
- Rackmountable
- Flexible Connectivity through SFP, SFP+, SFP28, QSFP+, QSFP28
- FPGA-based 10 Nanosecond Timestamping
- FPGA-based Packet Slicing & Capture Filter
- FPGA-based Deduplication
- PCAP & PCAPNG Support
- Optional Transport Case

PACKETGRIZZLY

neoxnetworks.com/
packetfalcon-packet-capture

Incident Response | Network Forensics | Troubleshooting

Compliance | Data Center | Service Provider

- 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 NETWORKS

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

Strengthening Cybersecurity and Application Observability by Integrating the Historic Network Data and Forensics

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

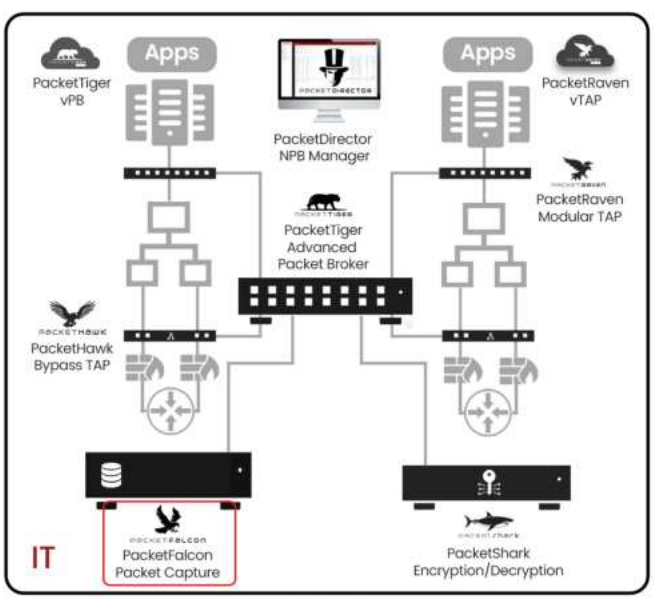
Deployment

SOC

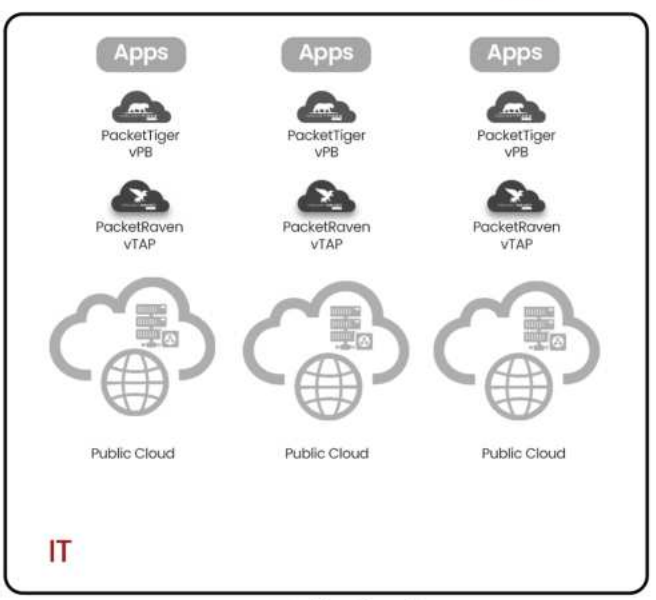
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

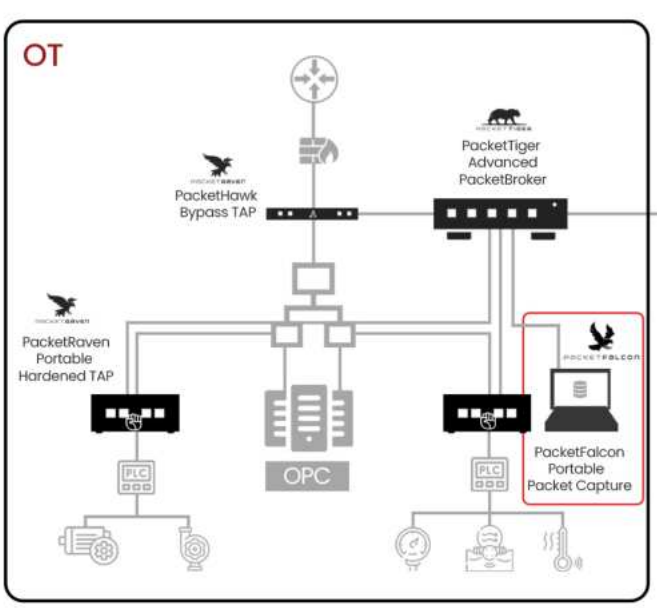
Application Issues, User Experiences, APM/NPM



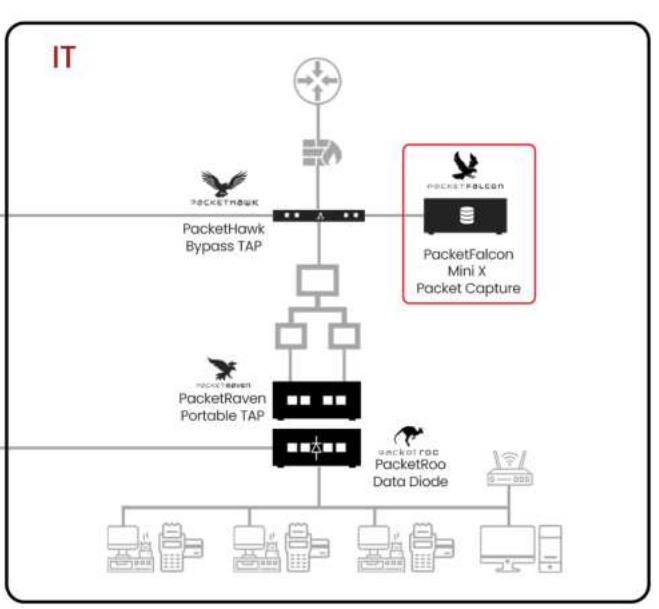
Data Center



Multi-Cloud



Industrial Site



Branch

NEOX NETWORKS

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

Strengthening Cybersecurity and Application Observability by Integrating the Historic Network Data and Forensics

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

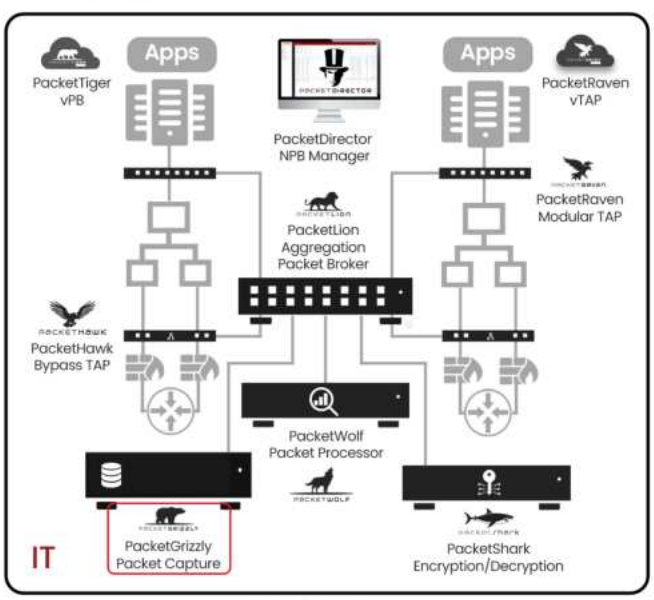
Deployment

SOC

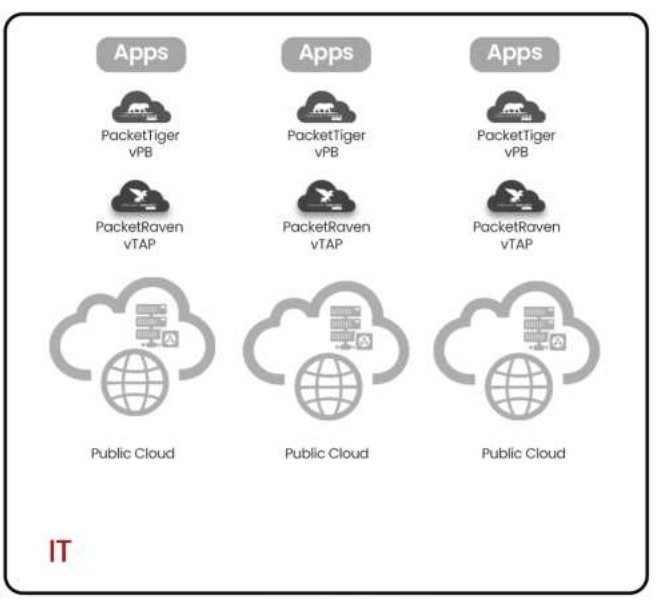
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

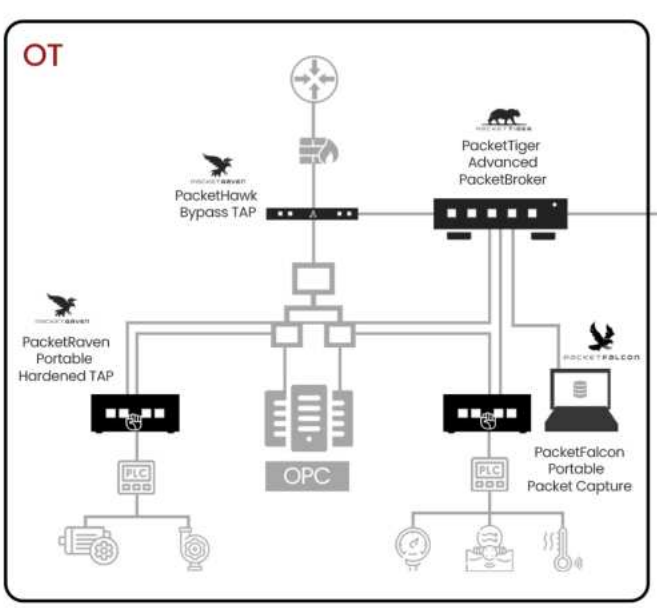
Application Issues, User Experiences, APM/NPM



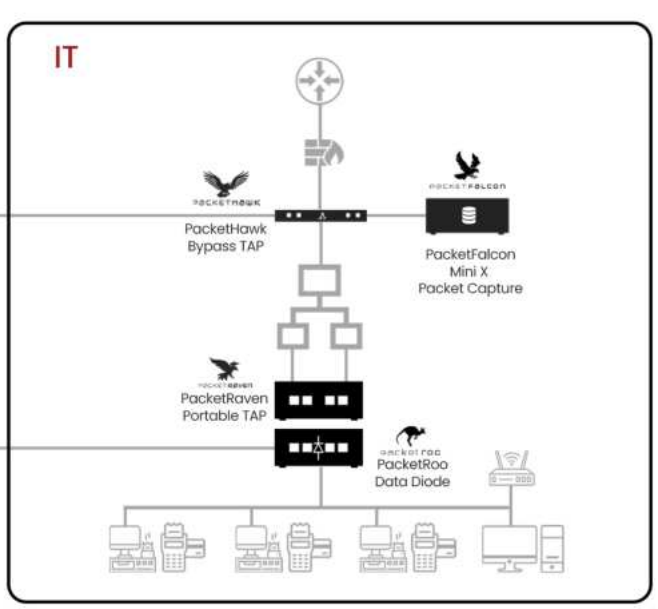
Data Center



Multi-Cloud



Industrial Site



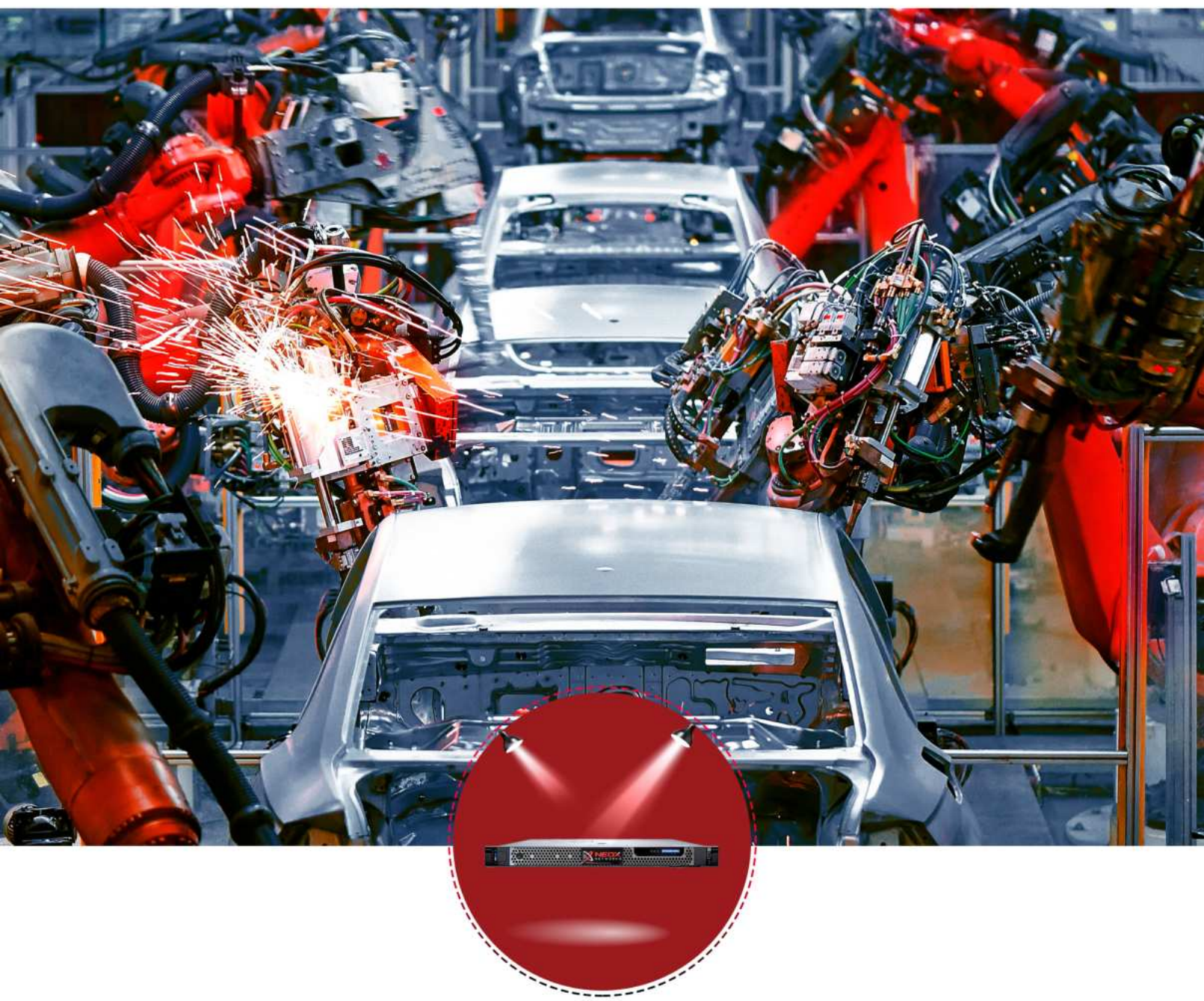
Branch

NEOX NETWORKS

PACKETWOLF

NEOX PacketWolf Packet Processing

Strengthening Cybersecurity and Application Observability by Integrating the Advanced Packet Processing and Analysis



NEOX NETWORKS

Packet Processor

NEOXPacketWolf Packet Processing

Advanced FPGA-based Packet Processing | 400Gbps Throughput NetFlow and IPFIX Unstamped Export

- 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
- 100Gbps NetFlow & IPFIX Unsampled Export
- Flexible Connectivity through SFP, SFP+, SFP28, QSFP+, QSFP28
- Tunnel Support (Encapsulation/ Decapsulation)
- Data Masking
- Ultra low-latency
- Suricata Support

PACKETWOLF

neoxnetworks.com/
packetwolf-packet-processor

NDR Support | Traffic Inspection | Troubleshooting

Tools Offload | Data Center | Service Provider

A Packet Processing appliance is equipped with advanced architecture to process the network data at the individual packet level. This involves FPGA-based technology 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 device 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.

NEOX NETWORKS

NEOX PacketWolf Packet Processing

Strengthening Cybersecurity and Application Observability by Integrating the Advanced Packet Processing and Analysis

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

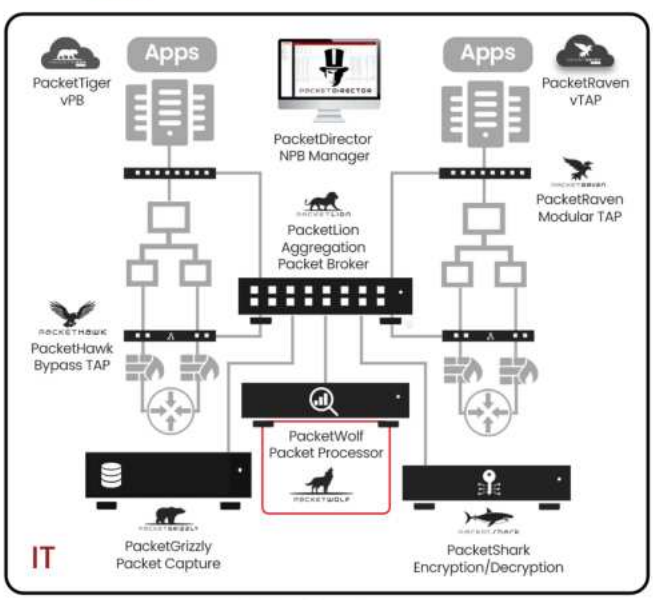
Deployment

SOC

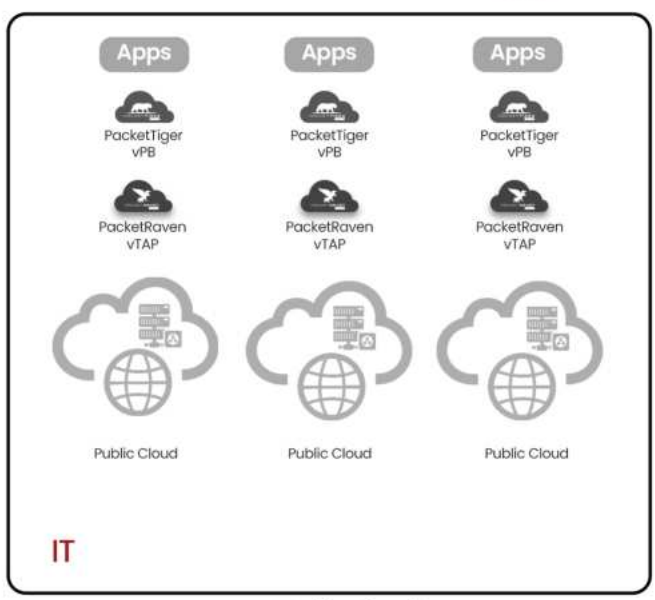
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

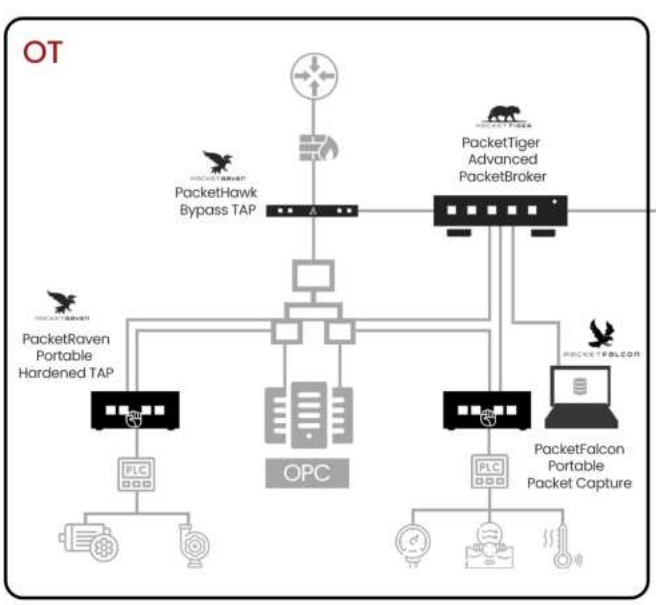
Application Issues, User Experiences, APM/NPM



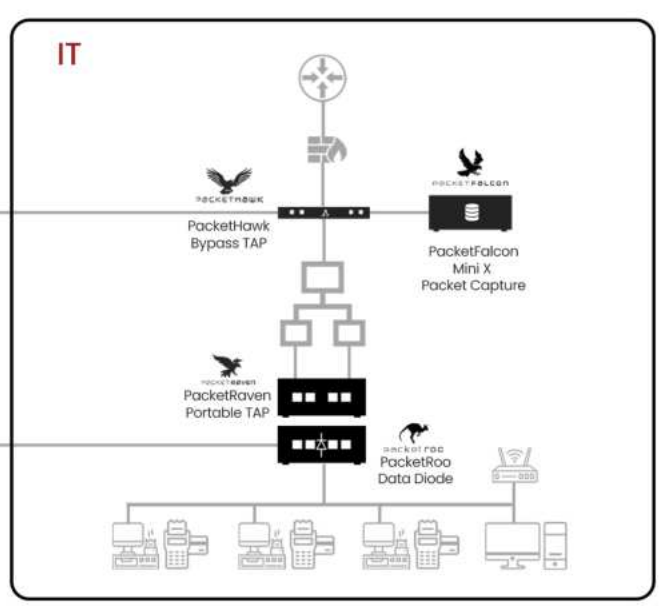
Data Center



Multi-Cloud



Industrial Site



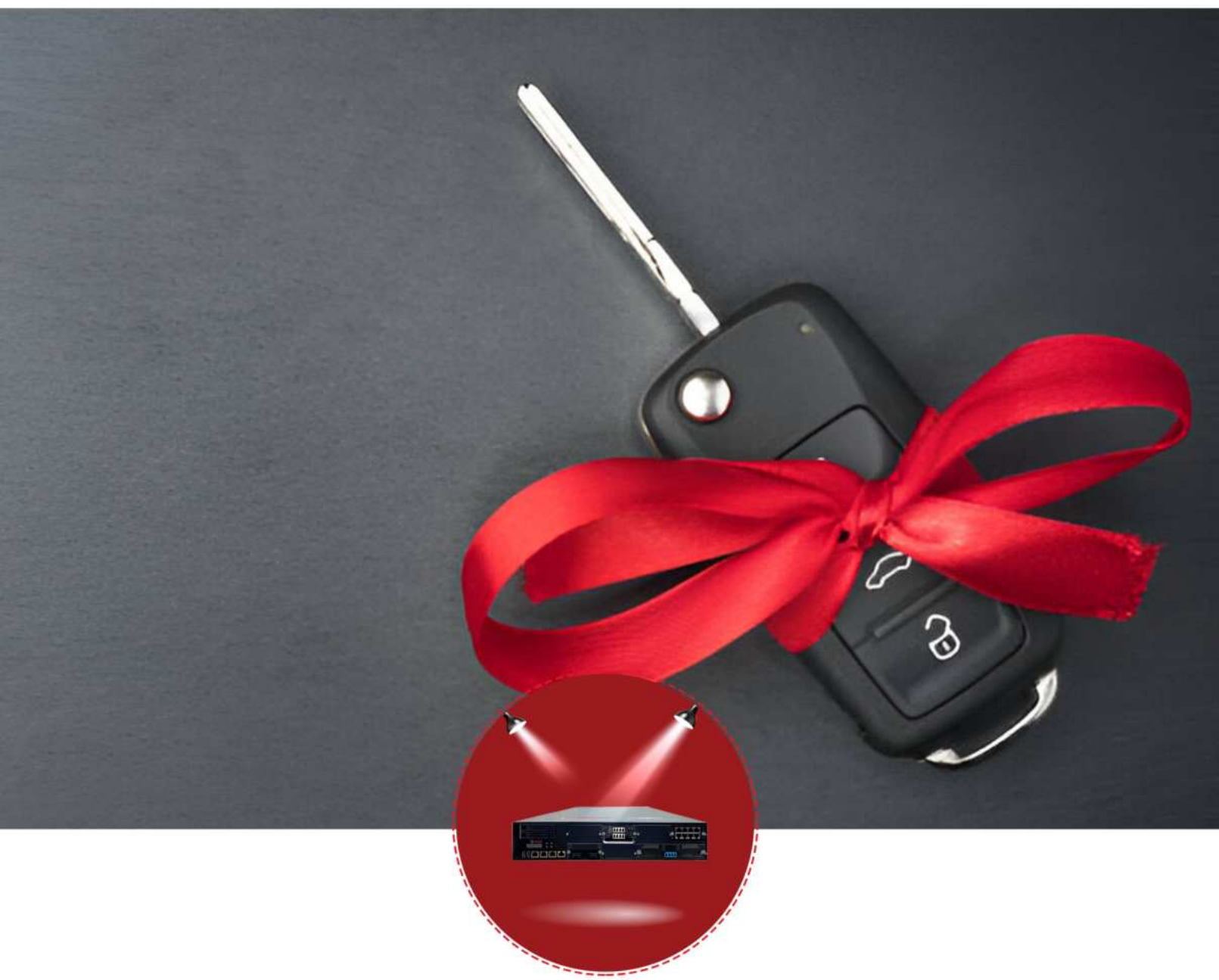
Branch

NEOX NETWORKS

packetshark

NEOXPacketShark Encryption & Decryption

Strengthening Cybersecurity and Application Observability by Network Transparency Into Encrypted Traffic



NEOX NETWORKS

Packet Processor

NEOX PacketShark Encryption & Decryption

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

- TLS 1.3 & SSL Support
- SSL Decryption on all L4 Ports
- Maintains 5-Tuple
- Bypass Funtionality
- URL Filtering
- Certificate Distribution & Control
- Compliance & Privacy
- Supports Forward Proxy & Reverse Proxy

packetshark

neoxnetworks.com/
packetshark

Cybersecurity | Fraud Detection | Investigation

Data Center | Service Provider | Lawful Intercept

An Encryption/Decryption Appliance offers an all-in-one solution to improve SSL infrastructure, providing security devices with visibility into TLS/SSL encrypted traffic and optimizing existing security investments. It supports policy-based traffic management and easily integrates with current architectures, while centralizing encryption and decryption using the latest technologies across the security framework.

- The PacketShark is a modular solution that keeps up with the process of ever-growing networks with its possibility to utilize NMC modules to increase the port density if required. To add more protection to the solution these NMC modules are also available with integrated Bypass functionality, handing over full control of the network links to the user. In combination with an external PacketHawk Inline Bypass and PacketLion Network Packet Brokers one can scale their security design to an unlimited degree.
- To effectively protect an enterprise network from both internal and external threats, a range of security devices is essential. Traditionally, addressing security challenges has involved administrators manually linking various point products to form a „security stack". PacketShark integrates with leading security vendors, allowing deployment within a "secure decrypt zone" to safeguard the entire network against encrypted threats.
- Dynamic service chaining offers a more flexible approach by routing traffic based on the Security Policy context. This enables specific types of traffic to flow through tailored chains of services, such as layer 2 and layer 3 inline services, receive-only services, ICAP, and HTTP web proxy services, optimizing security based on traffic needs. PacketShark uses advanced URL classification to categorize traffic from domains, allowing selective bypass of decryption to protect sensitive data such as medical or financial records, ensuring compliance with standards like HIPAA. Additionally, its URL filtering feature boosts employee productivity and mitigates risks by blocking access to malicious websites, including those linked to malware, spam, and phishing.

NEOX PacketShark Encryption & Decryption

Strengthening Cybersecurity and Application Observability by Network Transparency Into Encrypted Traffic

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

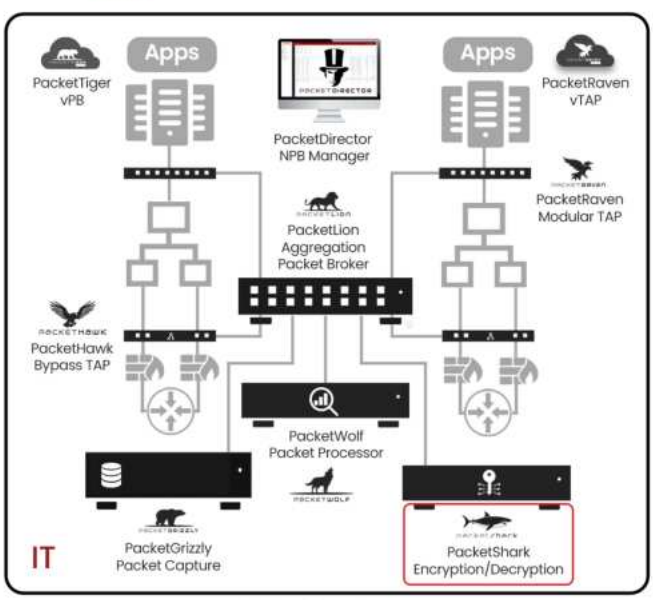
Deployment

SOC

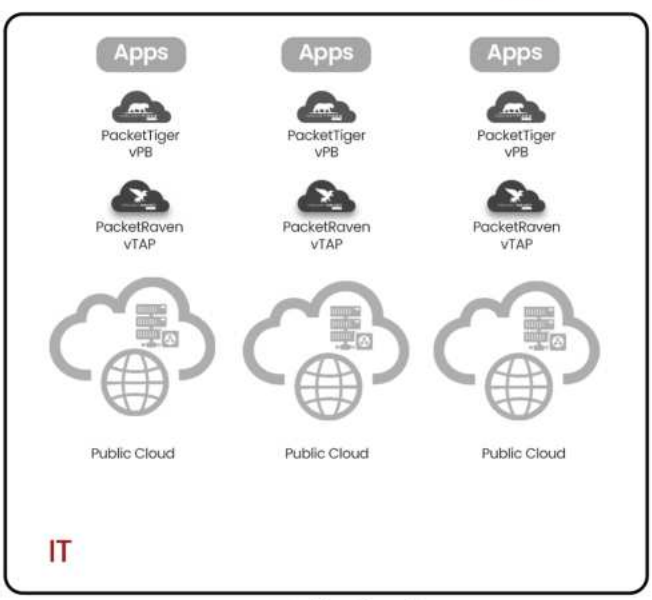
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

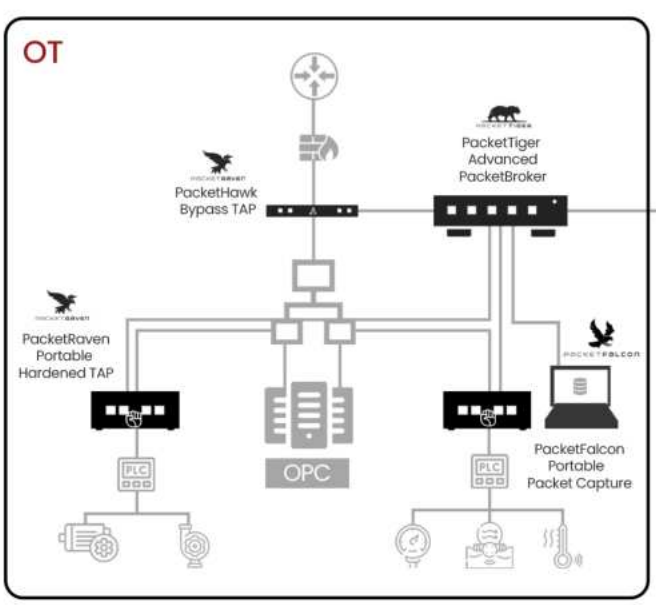
Application Issues, User Experiences, APM/NPM



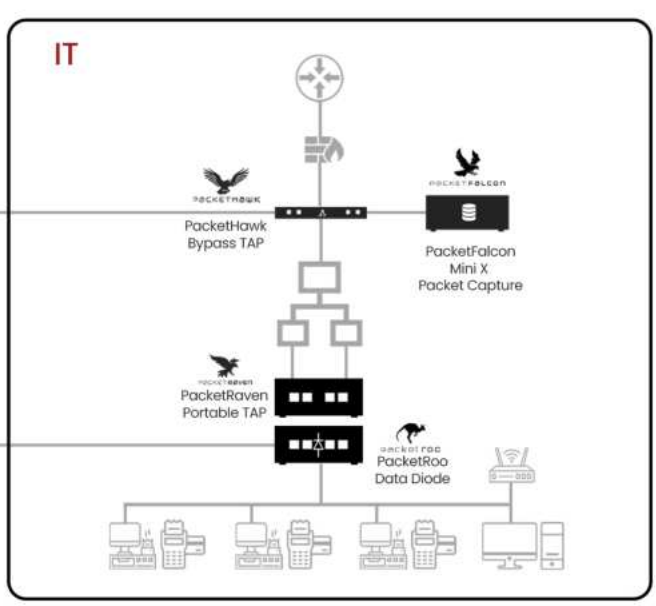
Data Center



Multi-Cloud



Industrial Site



Branch

NEOX NETWORKS

PACKETLION PACKETTIGER

NEOXPacketLion & NEOXPacketTiger Network Packet Broker Series

Strengthening Cybersecurity and Application Observability by Consolidating and Forwarding the Right Data to the Right Tools

NEOX NETWORKS

Packet Broker

NEOXPacketLion Packet Broker Series

High-Performance Aggregation | Non-Blocking Architecture
High Port Density | Inline Bypass or Out-of-Band | Flexible Stacking

- 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

PACKETLION

neoxnetworks.com/
packetlion-aggregation-packet-broker

Cybersecurity | NDR Feed | Troubleshooting

Data Center | Service Provider | Lawful Intercept

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.
  - Flexible port assignment (1:1, N:N, N:1, 1:N)
  - 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
  - Support for User-Defined Filter rules (UDF)

NEOX NETWORKS

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

Strengthening Cybersecurity and Application Observability by Consolidating and Forwarding the Right Data to the Right Tools

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

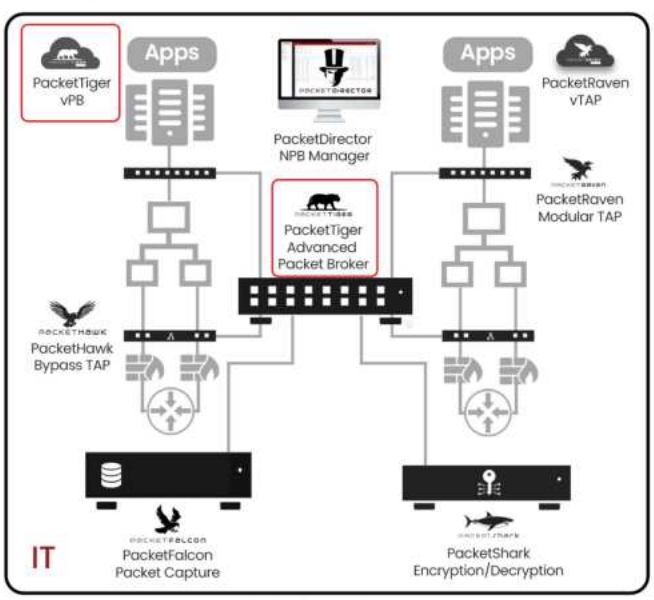
Deployment

SOC

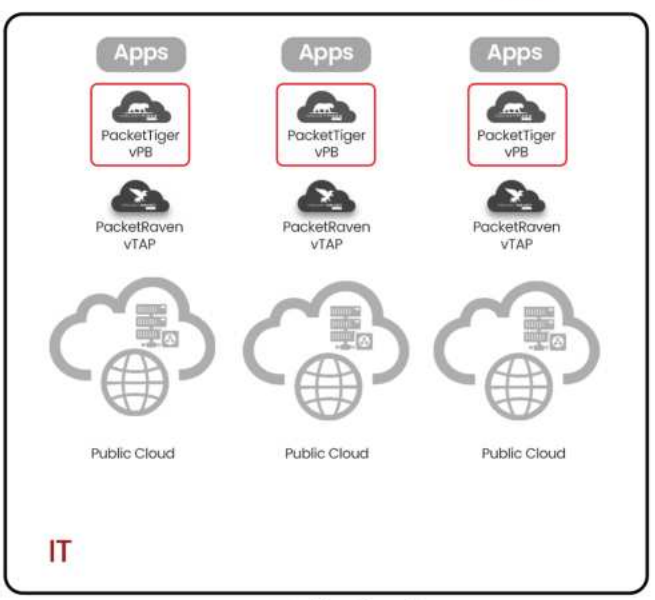
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

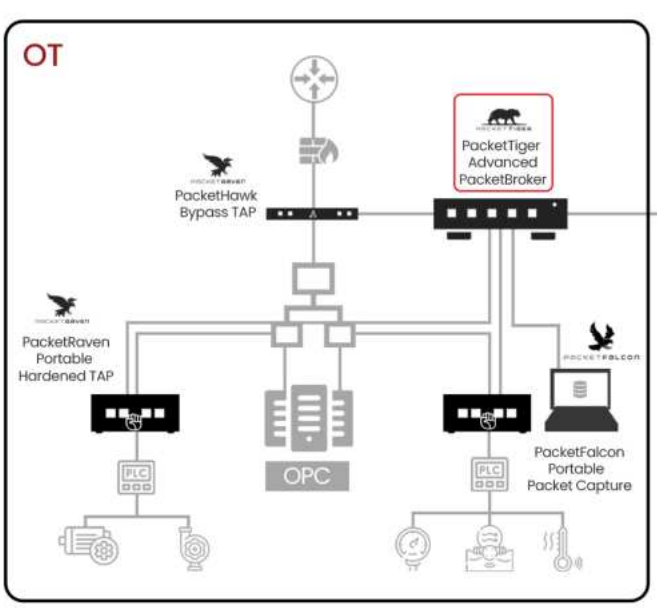
Application Issues, User Experiences, APM/NPM



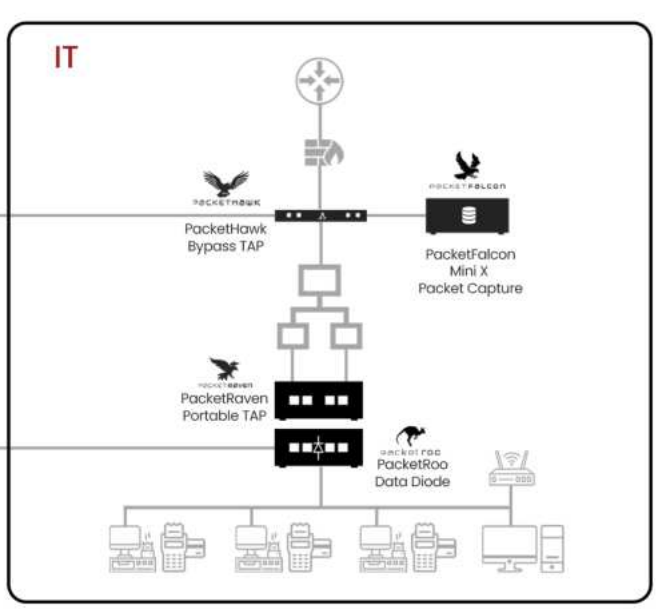
Data Center



Multi-Cloud



Industrial Site



Branch

NEOX NETWORKS

PACKETDIRECTOR

NEOXPacketDirector Packet Broker Manager

Strengthening Cybersecurity and Application Observability by Centrally Managing the Right Data to the Right Tools

NEOX NETWORKS

Network Management

NEOXPacketDirector Packet Broker Manager

Single-Pane-of-Glass Management of up to 100 Devices
Bulk Provisioning & Rules | Auto-Discovery | Network Statistics

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

PACKETDIRECTOR

neoxnetworks.com/
packetdirector

Cybersecurity | NDR Feed | Troubleshooting

Cloud | Data Center | Service Provider

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

- NEOXPacketDirector is a centralized management system for NEOXPacketLion, NEOXPacketTiger, and NEOXPacketTigerVirtual 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.
- NEOXPacketDirector is a software-based solution that can be deployed as a VM or container on-prem or in the cloud.
- NEOXPacketDirector 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 NEOXPacketDirector.

NEOX NETWORKS

NEOX PacketDirector Packet Broker Manager

Strengthening Cybersecurity and Application Observability by Centrally Managing the Right Data to the Right Tools

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

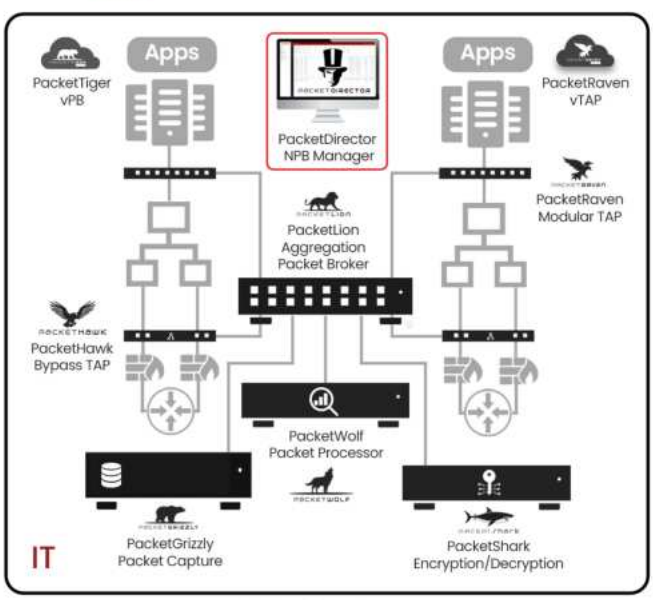
Deployment

SOC

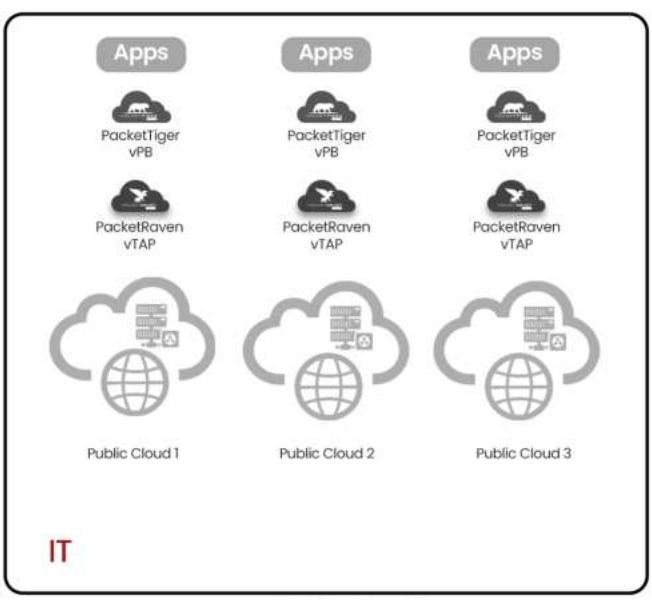
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

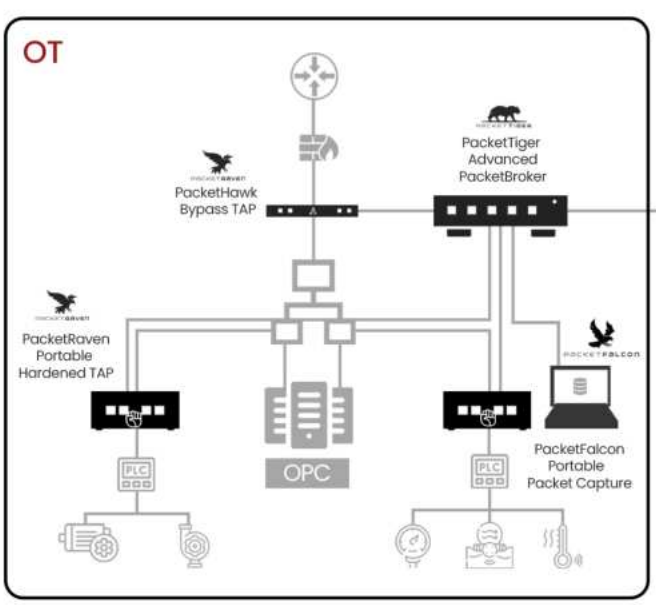
Application Issues, User Experiences, APM/NPM



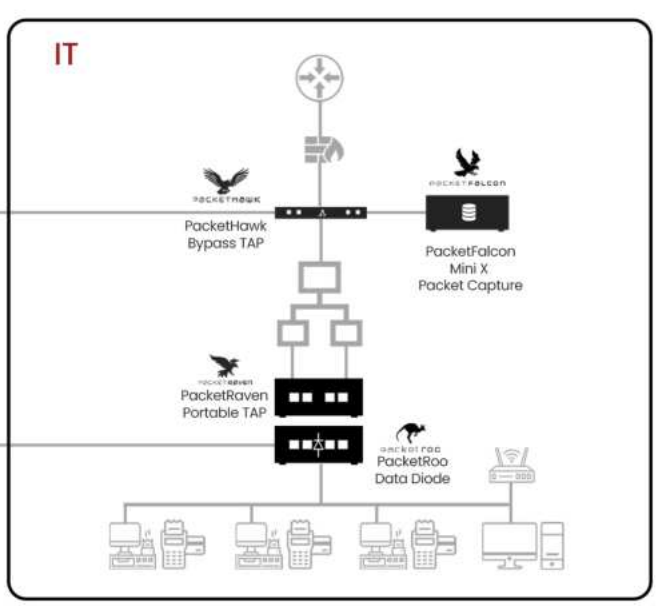
Data Center



Multi-Cloud



Industrial Site



Branch

NEOX NETWORKS

PACKETHAWK

NEOXPacketHawk Inline Bypass TAP

Strengthening Cybersecurity and Application Observability, by Integrating the Real-Time Network Traffic Rerouting

NEOX NETWORKS

Bypass TAP

NEOXPacketHawk Inline Bypass TAP

Up to 100G | Modular | Service Chaining | Filtering Load Balancing | Inline or Out-of-Band

- Up to 4 x 100Gbps QSFP+/QSFP28
- Modular Chassis
- Service Chaining
- Filtering
- Breakout & Aggregation TAP Modes
- User Specific Heartbeat
- Invisible for Hackers
- 100% Network Data
- Flexible to Use
- Failure Protection on Power Loss

PACKETHAWK

neoxnetworks.com/
packethawk-inline-bypass-network-tap

Cybersecurity | NDR Feed | Incident Response

Compliance | Data Center | Service Provider

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. 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.
  - 6 bypass modes. Network and inline port health check and speed/duplex monitoring with heartbeat
  - 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

NEOX NETWORKS

NEOX PacketHawk Inline Bypass TAP

Strengthening Cybersecurity and Application Observability, by Integrating the Real-Time Network Traffic Rerouting

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

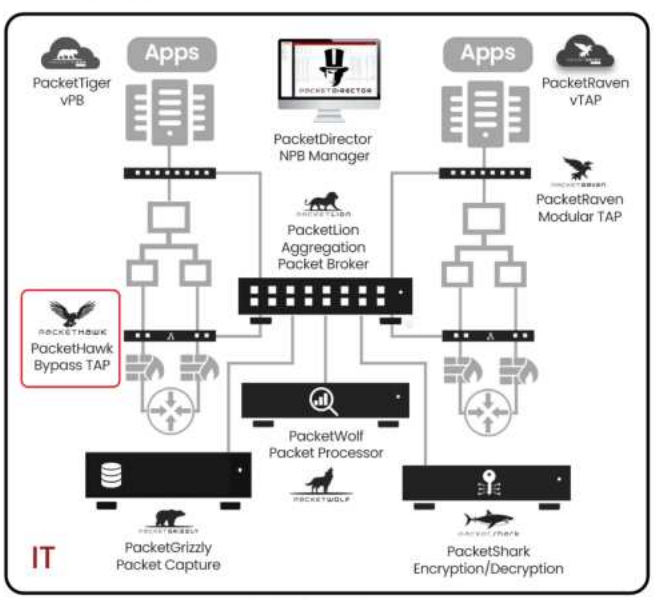
Deployment

SOC

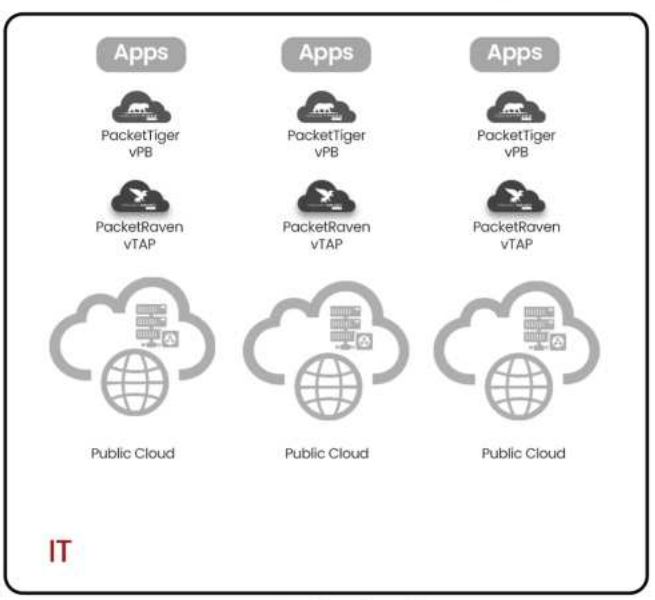
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

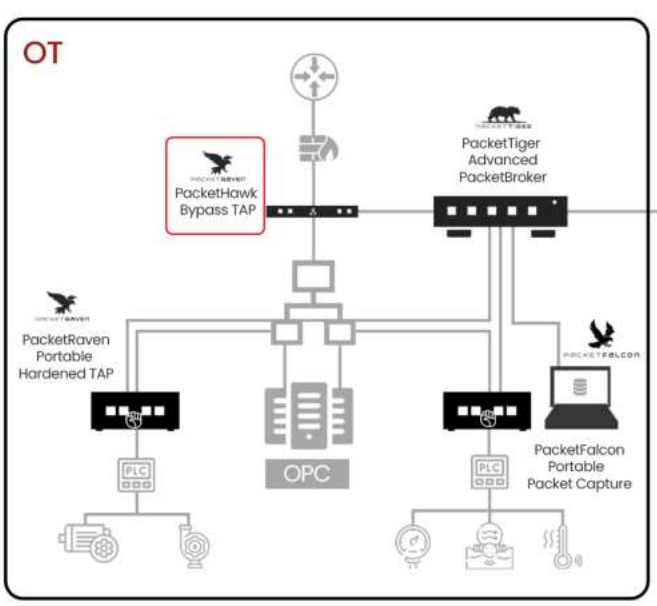
Application Issues, User Experiences, APM/NPM



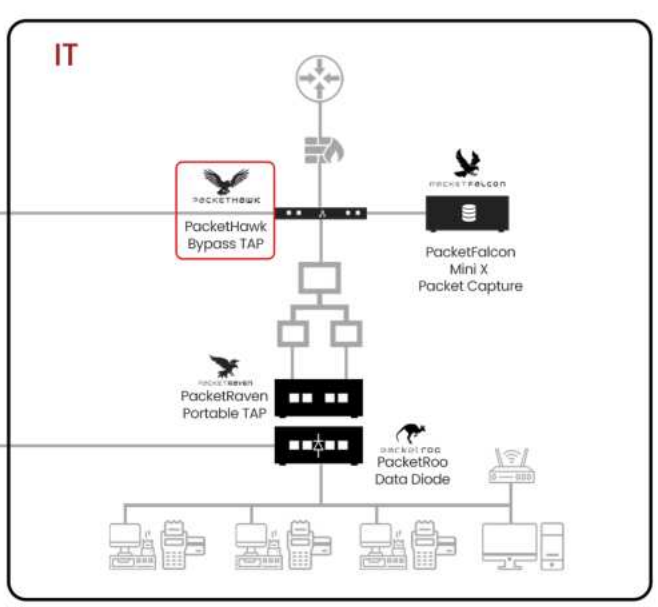
Data Center



Multi-Cloud



Industrial Site



Branch

NEOX NETWORKS

PACKETRAVEN

NEOXPacketRaven Network TAP Series

Strengthening Cybersecurity and Application Observability, by Integrating the Real-Time Network Wire-Data Intelligence

NEOX NETWORKS

Network TAPs

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

PACKETRAVEN

neoxnetworks.com/
packetraven-portable-network-tap

Cybersecurity | NDR Feed | Incident Response

Compliance | Remote Site | Industrial Facility

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 Certified
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

PACKETRAVEN

neoxnetworks.com/
packetraven-portable-network-tap

Cybersecurity | NDR Feed | Incident Response

Compliance | Outdoor Location | Industrial Facility

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 certified and CRITIS approved

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 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.

NEOX NETWORKS

Network TAPs

NEOXPacketRavenVirtual Virtual TAP

100% Network Data 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

PACKETRAVEN

neoxnetworks.com/
packetraven-virtual-network-tap

Cybersecurity | NDR Feed | Incident Response

Cloud | Data Center | Service Provider

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 NEOXPacketRaven Virtual, 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.

NEOX NETWORKS

NEOX PacketRaven Network TAP Series

Strengthening Cybersecurity and Application Observability, by Integrating the Real-Time Network Wire-Data Intelligence

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

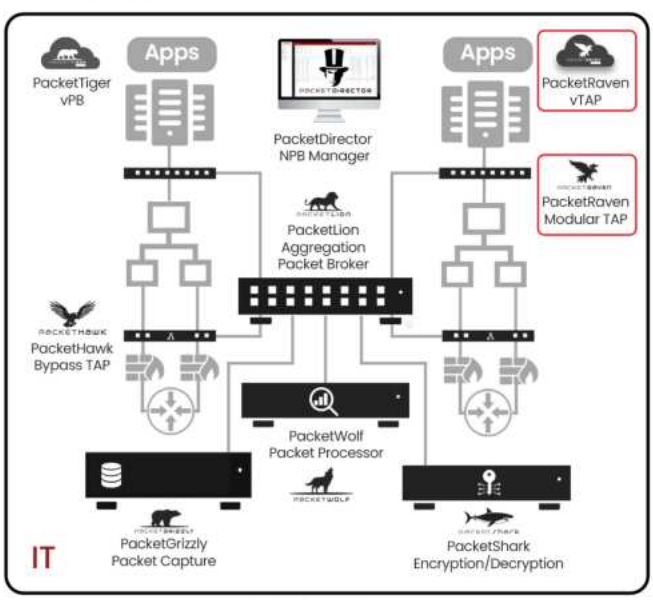
Deployment

SOC

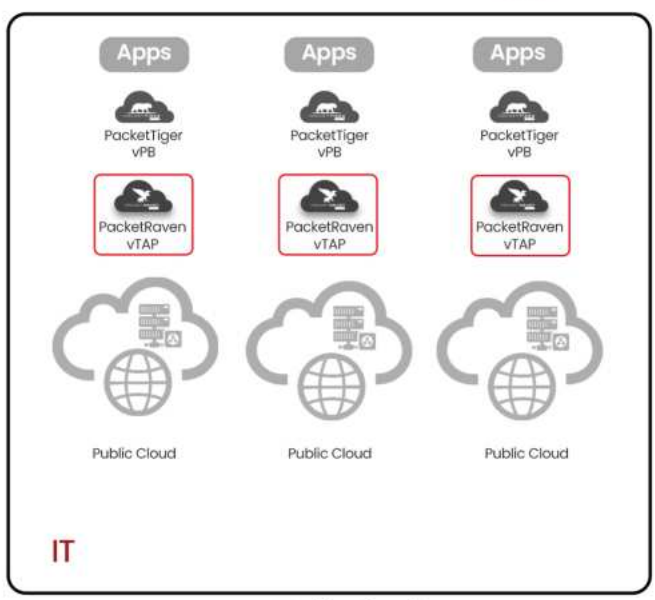
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

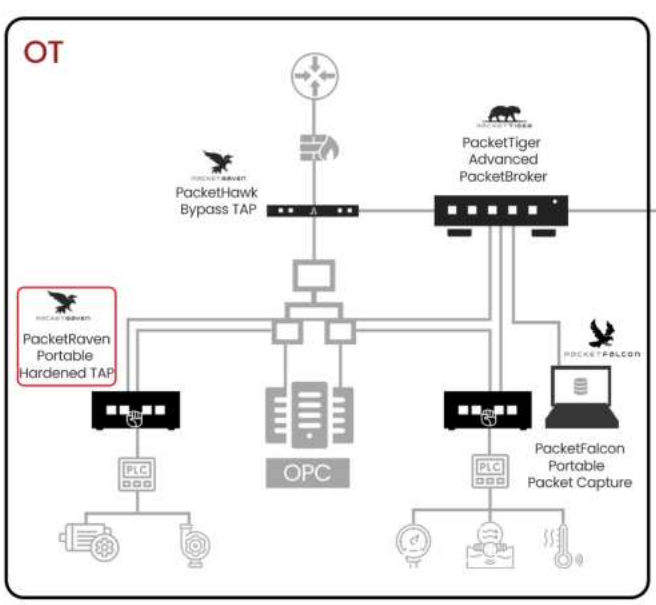
Application Issues, User Experiences, APM/NPM



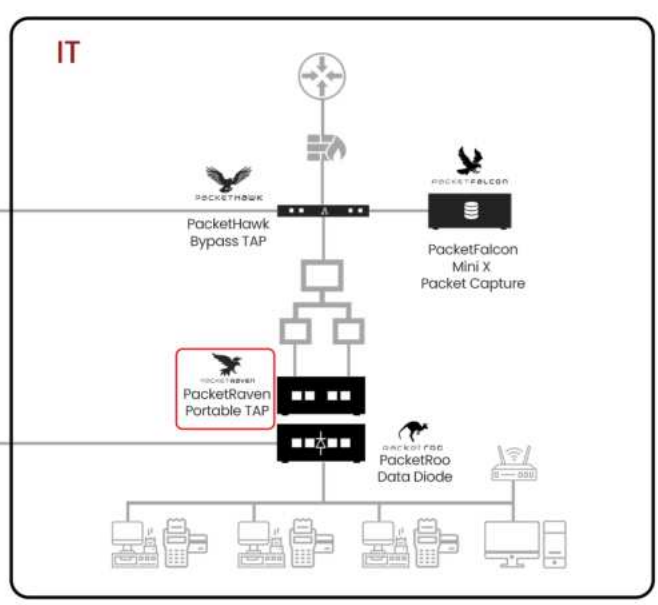
Data Center



Multi-Cloud



Industrial Site



Branch

NEOX NETWORKS

packetroo

NEOXPacketRoo Data Diode

Strengthening Cybersecurity and Application Observability, by Integrating the Real-Time Network Wire-Data Intelligence

NEOX NETWORKS

Network Diode

NEOXPacketRoo Data Diode

Secure File Transfer | Air Gap Assurance | Galvanic Isolation

- Unidirectional Data Flow
- Galvanic Isolation
- Vendor Agnostic
- Air Gap Assurance
- For Harsh Environments
- Automatic Speed Sync
- Link Loss Detection
- Error Prevention through Fixed Configuration
- Windows & Linux Support

packetroo

neoxnetworks.com/
packetroo-data-diode

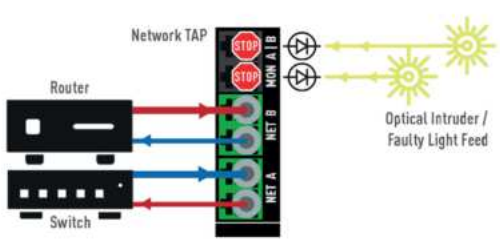
Cybersecurity | NDR Feed | Incident Response

Compliance | Remote Site | Industrial Facility

A Data Diode is a specialized solution that enforces full galvanic isolation between networks while allowing unidirectional signal transmission, preserving the critical air gap. To eliminate any attack surface on the physical layer, operators can either use data transfer methods leveraging the NEOXPacketRoo Data Diode functionality or utilize the NEOXSecureFileTransmitter software, which provides secure, granular, and one-way file transfer from OT to IT.

- The PacketRoo, combined with the NEOXSecureFileTransmitter, offers a scalable and high-performance solution for both Windows and Linux hosts, enabling seamless unidirectional data transmission. Each component of the bundle is also available separately, and if an existing data diode is already in place to bridge the air gap between networks, the NEOXSecureFileTransmitter remains fully vendor-agnostic. This flexibility also applies to the PacketRoo itself.
- In critical sectors like energy supply, transportation, defense, and industrial manufacturing, protecting IT/OT networks from cyberattacks is essential, especially in applications demanding Safety Integrity Levels (SIL) 3 and 4. Implementing an air gap between OT and IT environments strengthens security by physically separating operational technology systems from external IT networks, significantly reducing the risk of cyber threats.
- To reduce the risk of configuration errors, the PacketRoo is available only in fixed configurations, with no option to modify port settings after deployment. As a fully sealed system, it is designed for both civilian and military use cases, ensuring robust and secure

Data Diode functionality:



NEOX NETWORKS

NEOX PacketRoo Data Diode

Strengthening Cybersecurity and Application Observability, by Integrating the Real-Time Network Wire-Data Intelligence

IT NetSecOps | Critical Infra | Data Center | Multi-Cloud

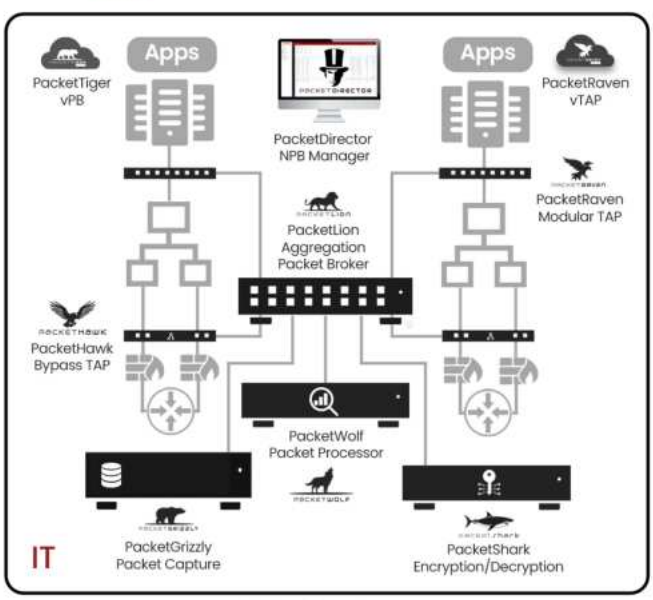
Deployment

SOC

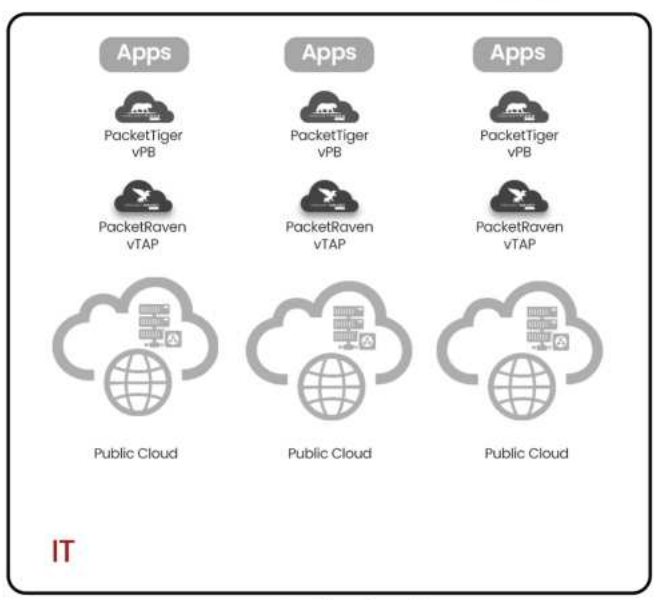
Threat Detection, Incident Response, SIEM, NIDS, NIPS

NOC

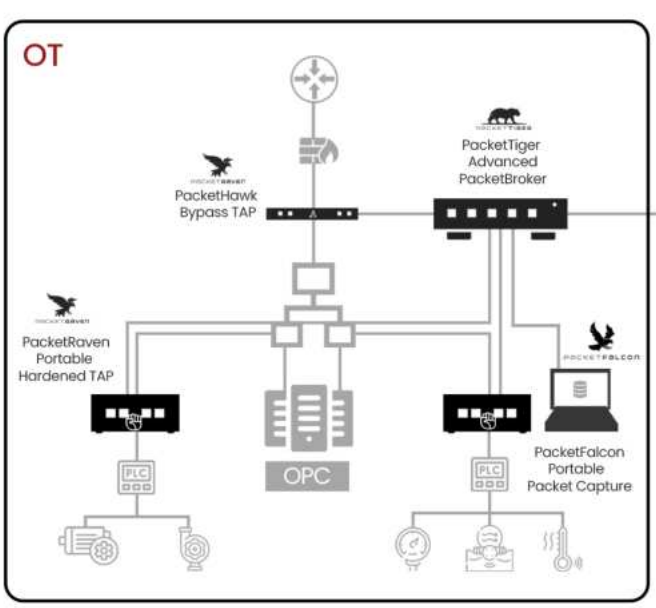
Application Issues, User Experiences, APM/NPM



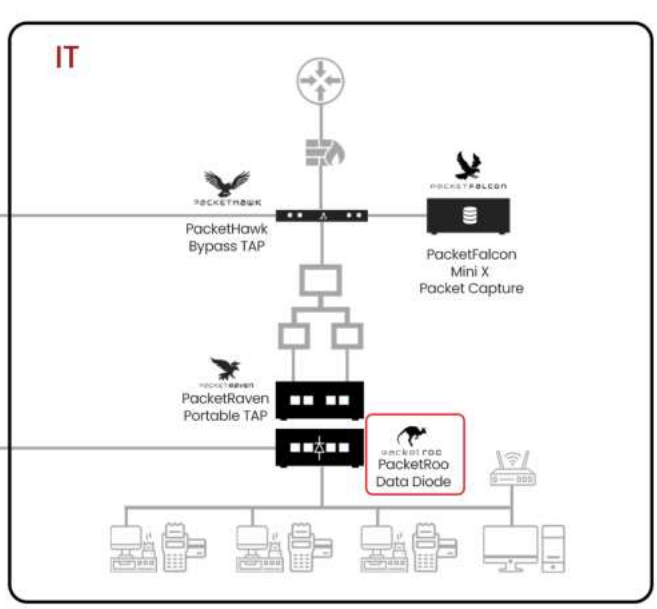
Data Center



Multi-Cloud



Industrial Site



Branch

NEOX NETWORKS

Optical Transceivers and Cables

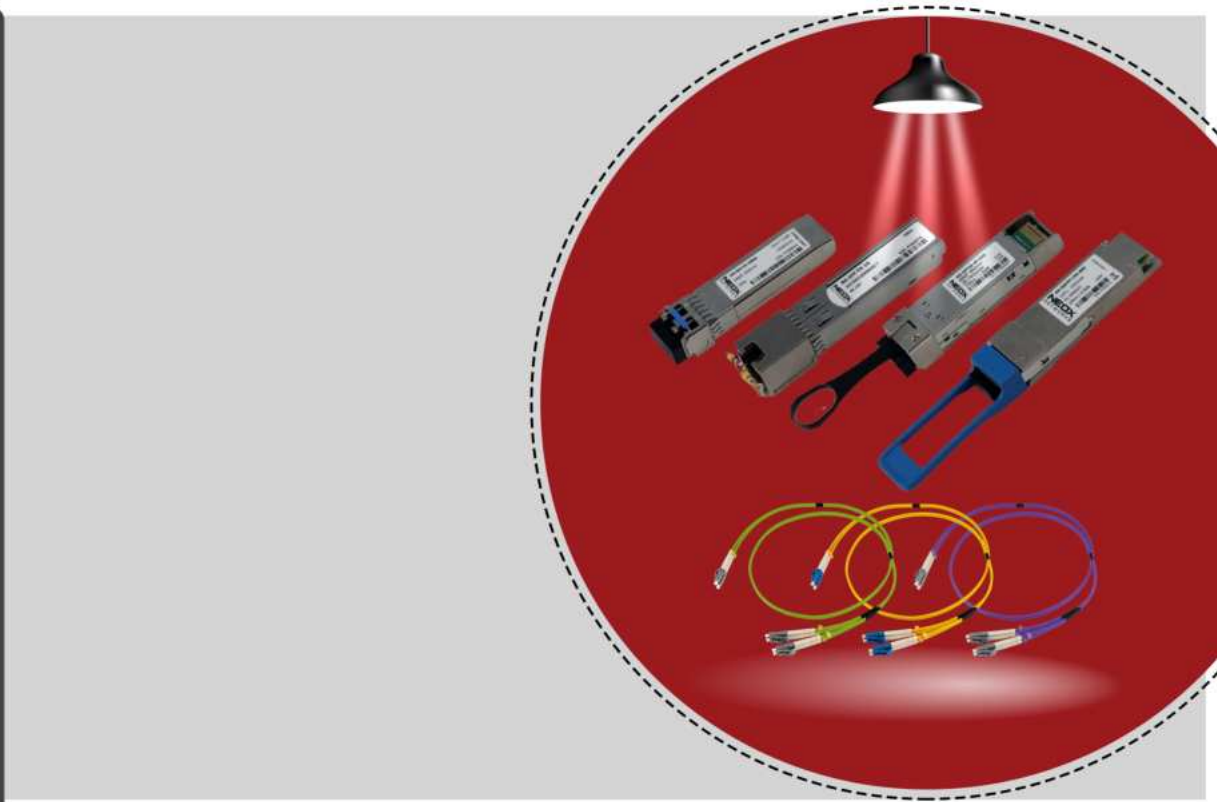
Strengthening Cybersecurity and Application Observability by Integrating Faster and Reliable Connectivity

NEOX NETWORKS

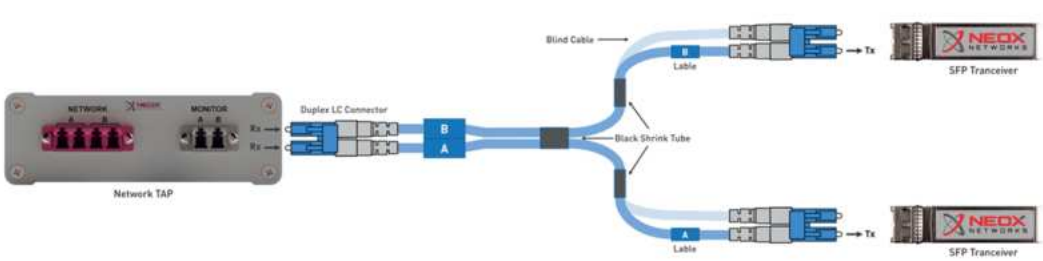
Connectivity

Optical Transceivers and Cables

Pre-Qualified Faster and Reliable Connectivity



- 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.

NEXT GENERATION NETWORK VISIBILITY

NEOX NETWORKS

Techmart Center 5201 Great America Parkway Suite 320
Santa Clara, CA 95054

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