NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

Feature Brief

Rapid Visibility with Intelligent Application Classification

In today's complex and dynamic networks, identifying and categorizing application traffic quickly is essential for effective visibility, monitoring, security, and policy enforcement. Without proper Application Classification, networks suffer from blind spots, inefficient resource allocation, shadow IT, and increased vulnerability to threats. NEOX's Application Classification feature on its Packet Brokers delivers deep application recognition, enabling precise traffic steering, optimized tool performance, and enhanced security posture.

What is Application Classification

Application Classification with Packet Brokering refers to the advanced identification and categorization of network traffic based on application, protocol, and service types. Unlike traditional port-based methods, NEOX's deep packet inspection (DPI) and machine learning-powered technology ensure accurate application recognition — even for encrypted or evasive applications — enabling granular traffic control and policy enforcement.

Why Application Classification Matters

NEOX's Application Classification feature enhances network observability and security by:

1. **Improving Security & Threat Detection**
   By classifying encrypted and obfuscated traffic, NEOX exposes hidden threats, malicious apps, and unauthorized services. Security tools like NGFW, IDS/IPS, and SWG receive enriched metadata, enabling deeper inspection and reducing false negatives.

2. **Optimizing Network Performance & Efficiency**
   NEOX's Application Classification intelligently prioritizes business-critical applications while limiting bandwidth-hungry or non-essential traffic. This ensures optimal resource allocation, reduces network congestion, and improves user experience—without compromising security or visibility. IT teams gain granular control to enforce QoS policies and align network usage with organizational priorities.

3. **Optimizing Tool Efficiency & Reducing Noise**
   NEOX filters and forwards only relevant application traffic to monitoring and security tools, eliminating unnecessary processing overhead. This extends tool lifespan, reduces costs, and improves detection accuracy by eliminating irrelevant noise.

How NEOX Delivers Advanced Application Classification

NEOX's PacketTiger series of Packet Brokers integrate hardware-accelerated Application Classification to ensure zero-latency traffic classification and forwarding.

1. **Deep Packet Inspection (DPI) & Behavioral Analysis**

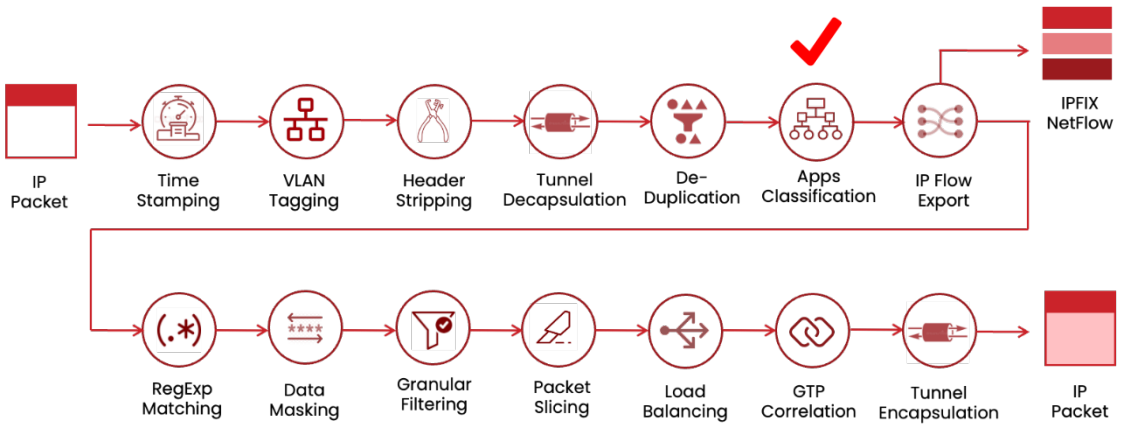
   NEOX goes beyond basic port/protocol detection, using signature-based and behavioral analysis to identify applications—even over encrypted channels (TLS/SSL). Machine learning continuously refines classification accuracy, adapting to new and evolving apps.

2. **Weighted & Adaptive Traffic Routing**

By classifying encrypted and obfuscated traffic, NEOX exposes hidden threats, malicious apps, and unauthorized services. Security tools like NGFW, IDS/IPS, and SWG receive enriched metadata, enabling deeper inspection and reducing false negatives.

3. **Optimizing Tool Efficiency & Reducing Noise**

   NEOX filters and forwards only relevant application traffic to monitoring and security tools, eliminating unnecessary processing overhead. This extends tool lifespan, reduces costs, and improves detection accuracy by eliminating irrelevant noise.



Feature	PacketWolf	PacketLion	PacketTiger	PacketTigerVirtual
App Classification			✓	✓

Best Practices for Application Classification with NEOX

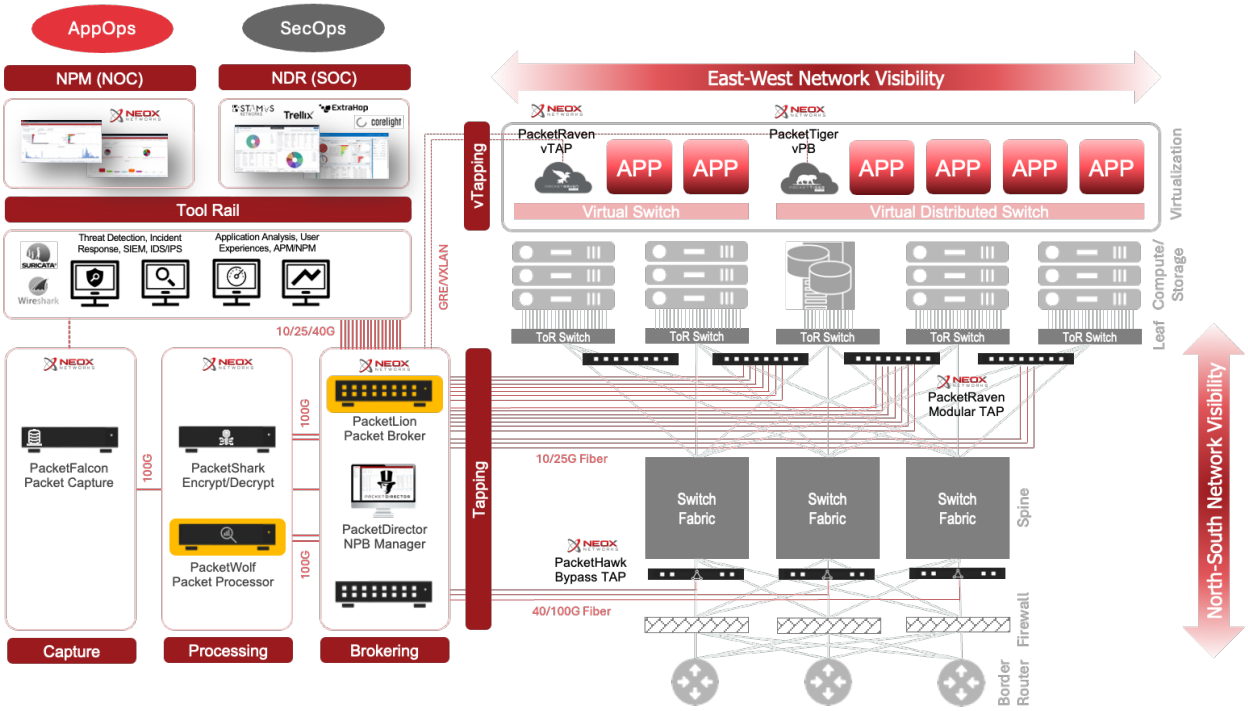
To maximize efficiency, we recommend:

- ✓ Deploy NEOX at network choke points (gateways, data centers, cloud edges) for full visibility.
- ✓ Combine with Advanced Filtering to reduce irrelevant traffic before classification.
- ✓ Update signature databases regularly to detect emerging applications.
- ✓ Integrate with SIEM/SOAR for automated threat response based on application behavior.

To help you get the most out of your network, we recommend the following best practices to funnel, consolidate, and process all network traffic to be monitored through one of the two NEOX Packet Broker approaches:

- For better hardware performance, lower latency network, or for a future-proofed scalable visibility approach, deploy a **two-tier visibility architecture**. Use NEOX PacketLion Packet Broker for high-density TAP and tool aggregation, and use NEOX PacketTiger, Packet Broker for Application Classification and other packet services operations.

- For a lighter or software-driven approach, consolidate all network traffic to be monitored through a NEOX PacketTiger, and then from there to the tool rail. Same can be achieved in the cloud with PacketTigerVirtual before forwarding traffic to cloud-native monitoring or security tools.



The Future of Network Traffic Brokering Starts Here

As networks grow in complexity and speed, the importance of Application Classification will only continue to rise. At NEOX we're committed to helping you stay ahead of the curve with innovative solutions that deliver precision, reliability, and performance

Ready to Transform Your Network?

Discover how NEOX can elevate your Network Traffic Brokering with advanced Application Classification technology. Contact Us today or Request a Demo to learn more about our solutions and take the first step toward a smarter, faster, and more secure network.

About NEOX Networks

NEOX Networks provides Next Generation Network Visibility for IT & OT Observability and Security. The result is strengthened cybersecurity, hybrid-cloud application observability, and business continuity, by integrating the network intelligence and real-time data-in-motion. Learn more at neoxnetworks.com