NEOX NETWORKS
NEXT GENERATION NETWORK VISIBILITY

Feature Brief

Ensuring Data Privacy with Data Masking

In today's interconnected digital landscape, protecting sensitive data is not just a compliance requirement—it's a critical security imperative. As networks handle vast amounts of confidential information, the ability to selectively obscure sensitive data while maintaining visibility for monitoring and security tools is essential. At NEOX, we understand that Data Masking isn't just about compliance—it's about enabling secure, intelligent network monitoring without exposing critical information to unnecessary risks.

What is Data Masking

Data Masking is the process of dynamically obscuring sensitive or regulated data within network traffic packets, ensuring that only authorized systems and personnel can access the original information. Unlike static redaction, NEOX's Data Masking leverages real-time processing to selectively hide sensitive fields in the packets while preserving the integrity of network monitoring, threat detection, and forensic analysis.

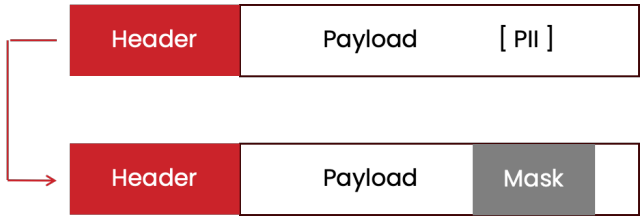
Why Data Masking Matters

NEOX's Data Masking ensures that security and monitoring tools operate effectively without compromising sensitive information. Here's why it's indispensable:

1. **Enhanced Security & Privacy Compliance**
   To protect sensitive data and comply with regulations like GDPR, CCPA, and HIPAA, organizations must prevent unauthorized exposure in logs, SIEMs, PCAP and monitoring tools by masking Personal Identifiable Information (PII), financial data, and healthcare records. This reduces compliance risks and safeguards privacy.

2. **Secure Sharing of Network Traffic for Analysis**
   Organizations can securely forward network traffic to third-party analysts, managed security service providers (MSSPs), or threat intelligence platforms by implementing data sanitization measures to prevent the exposure of confidential information. This approach enables effective forensic investigations and threat analysis while significantly reducing the risk of data breaches, ensuring both security and operational efficiency.

3. **Optimized Monitoring & Threat Detection**
   To enhance security without compromising privacy, organizations should configure monitoring tools like NDR, SIEM, and DLP to prioritize detecting behavioral anomalies rather than processing raw sensitive data. This approach maintains critical visibility into attack patterns and threat activity while safeguarding customer and corporate information from unnecessary exposure. By focusing on metadata and behavioral analytics, businesses can strengthen their security posture while minimizing data privacy risks.



How NEOX Delivers Advanced Data Masking

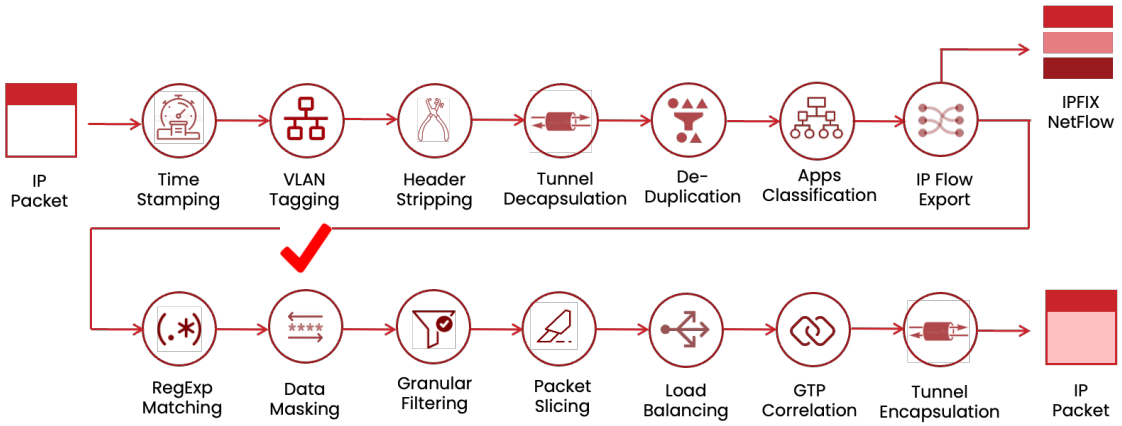
NEOX's PacketWolf and PacketTiger series of Packet Brokers & Processors integrate real-time Data Masking to secure sensitive data without disrupting network monitoring workflows.

1. **Real-Time, Inline Data Masking**
   NEOX Packet Brokers provide real-time, inline data masking for TAP/SPAN and inline deployments, instantly securing sensitive structured (JSON/XML) and unstructured data in transit. This enables continuous network monitoring while automatically protecting confidential information without workflow disruption.

2. **Deep Packet Inspection (DPI) for Precision Masking**
   NEOX uses Deep Packet Inspection (DPI) to precisely identify and mask sensitive data in decrypted TLS/SSL traffic, with context-aware protection customized for healthcare, finance, and e-commerce applications. This enables compliant, secure network monitoring without disrupting operations.

3. **Security-Optimized Slicing**
   NEOX solution enables intelligent traffic filtering that preserves critical threat indicators—including malware signatures, C2 beaconing patterns, and data exfiltration attempts—while automatically discarding non-essential payload data. The system forwards optimized, sliced packets to security tools like IDS/IPS, NDR, and SIEM systems, ensuring high-speed threat analysis without the noise of unnecessary data. This targeted approach enhances detection capabilities while reducing the processing burden on security infrastructure.

4. **Cloud & Hybrid Network Support**
   NEOX's PacketTigerVirtual brings consistent security to multi-cloud environments (AWS/Azure/GCP), applying the same filtering and masking policies across hybrid infrastructures. This ensures uniform protection and monitoring for both cloud workloads and on-premises systems.



Feature	PacketWolf	PacketLion	PacketTiger	PacketTigerVirtual
Data Masking	✓		✓	✓

Best Practices for Data Masking with NEOX

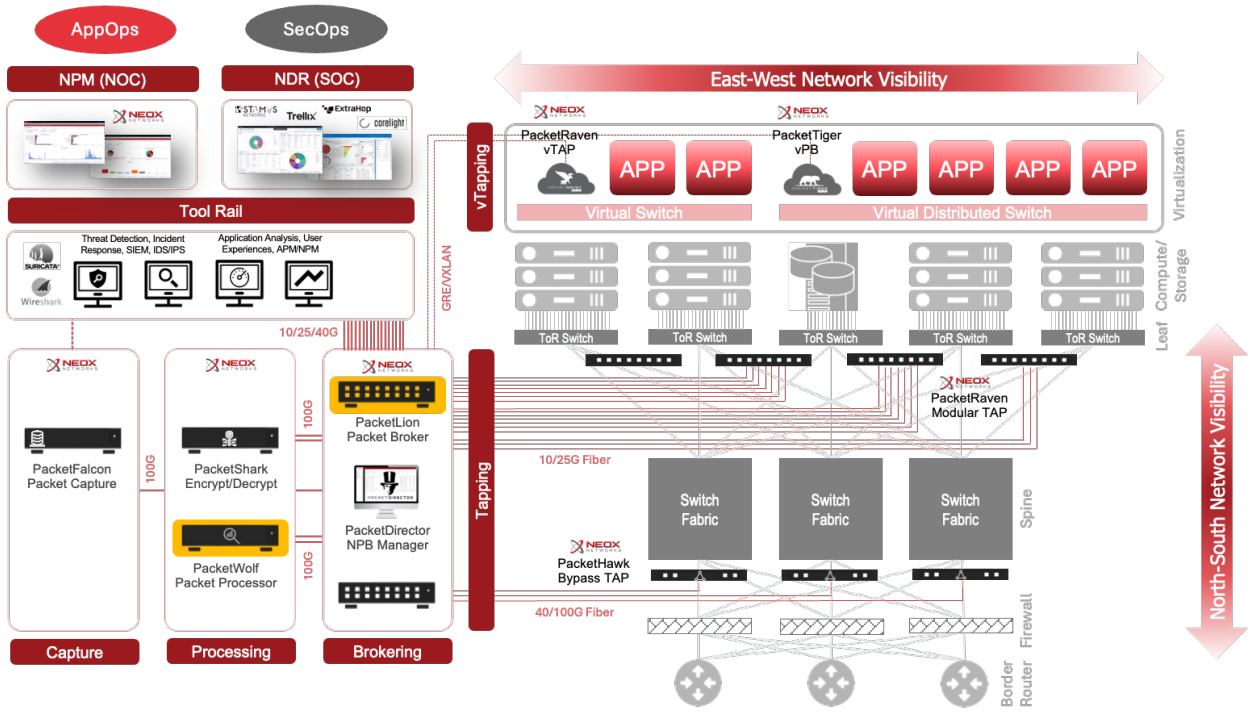
To maximize security and compliance while maintaining network visibility, we recommend:

- ✓ Deploy NEOX Packet Brokers inline or via TAP/SPAN to mask sensitive data before it reaches monitoring tools.
- ✓ Combine Data Masking with Advanced Filtering to reduce unnecessary processing of non-critical traffic.
- ✓ Regularly update masking policies based on evolving compliance and threat intelligence requirements.
- ✓ Use format-preserving masking for analytics tools that require realistic but anonymized data making it easier to handle increasing volumes of data and growing numbers of connected devices or links being monitored in a network.

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 PacketWolf Packet Broker for faster Data Masking 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 Data Masking 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 Data Masking 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.
NEOX – Precision. Performance. Perfected.

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