NEOX NETWORKS
UNIFIED NETWORK VISIBILITY

BLUECAT™

Solution Brief

AI-Powered Application Observability with

NEOX PacketOps and BlueCat LiveNX Performance Intelligence

Challenge

Enterprise networks now span campuses, WAN and SD-WAN, data centers, branch locations, remote users and public clouds. When businesses applications go down or performance deteriorates, network operations (NetOps) teams must correlate device health, application behavior, traffic paths and packet evidence across multiple vendors and domains, as business bleeds revenue. Flow-only monitoring can reveal where traffic is going, but it may not expose the underlying packet-level cause. Packet-only analysis, without network context, can slow prioritization and troubleshooting. You need a balance of both. Fragmented visibility leads to longer outages, slower root-cause isolation and higher operational costs.

NEOX & BlueCat Observability Solution

NEOX Networks and BlueCat Networks bring together a high-fidelity Network Visibility foundation and context-rich Network Observability solution. NEOX's PacketOps™ components such as Network TAPs and Network Packet Brokers provide consistent access to critical north–south and east–west network traffic, selectively aggregating, filtering and distributing rich packet data to BlueCat. Where deployed and licensed, NEOX PacketLion, PacketWolf or PacketTiger packet brokers can generate NetFlow/IPFIX records from the packet data and optimize monitored traffic. BlueCat LiveNX correlates flow, device and application telemetry, maps paths, and identifies performance anomalies; LiveWire adds packet capture and detailed packet analysis; and the optional LiveAssist add-on provides AI-assisted investigation and guided operational insights for an early AIOps flavor.

Together, the solution enables a practical progression from network-wide visibility to application context, flow-level diagnosis and historical packet repository for troubleshooting — helping NetOps resolve problems faster and protect user experiences.

Business Benefits

- Improved service availability and digital experience through faster fault isolation.
- Reduced troubleshooting time (MTTR) and unnecessary infrastructure upgrades.
- Improved monitoring ROI by reusing a scalable visibility layer across tools.

Technical Benefits

- Correlated topology, interface/device telemetry, application flows and PCAP evidence.
- Feed monitoring tools with policy-controlled, filtered and deduplicated traffic where supported.
- Combined LiveNX analytics with LiveWire packet investigation and optional LiveAssist.

Solution Construct

The joint architecture separates traffic acquisition and optimization from performance analytics. This creates a scalable monitoring foundation while preserving each product's distinct responsibilities.

NEOX Network Visibility Foundation

Deploy NEOX PacketRaven and/or PacketHawk network TAPs at selected physical links and use PacketRaven Virtual vTAPs or provider-native mirroring for relevant cloud environments to extract the wire data. PacketLion packet broker provides TAP and SPAN high-density aggregation and packet data distribution. In highly scalable data center applications, it is recommended to deploy PacketWolf to handle advanced packet processing such as deduplication and slicing, and to generate the packet to flow data for BlueCat consumption. In smaller applications, PacketTiger may supply the advanced brokering and optional packet/flow services. Product selection depends on throughput, topology, license and monitoring requirements.

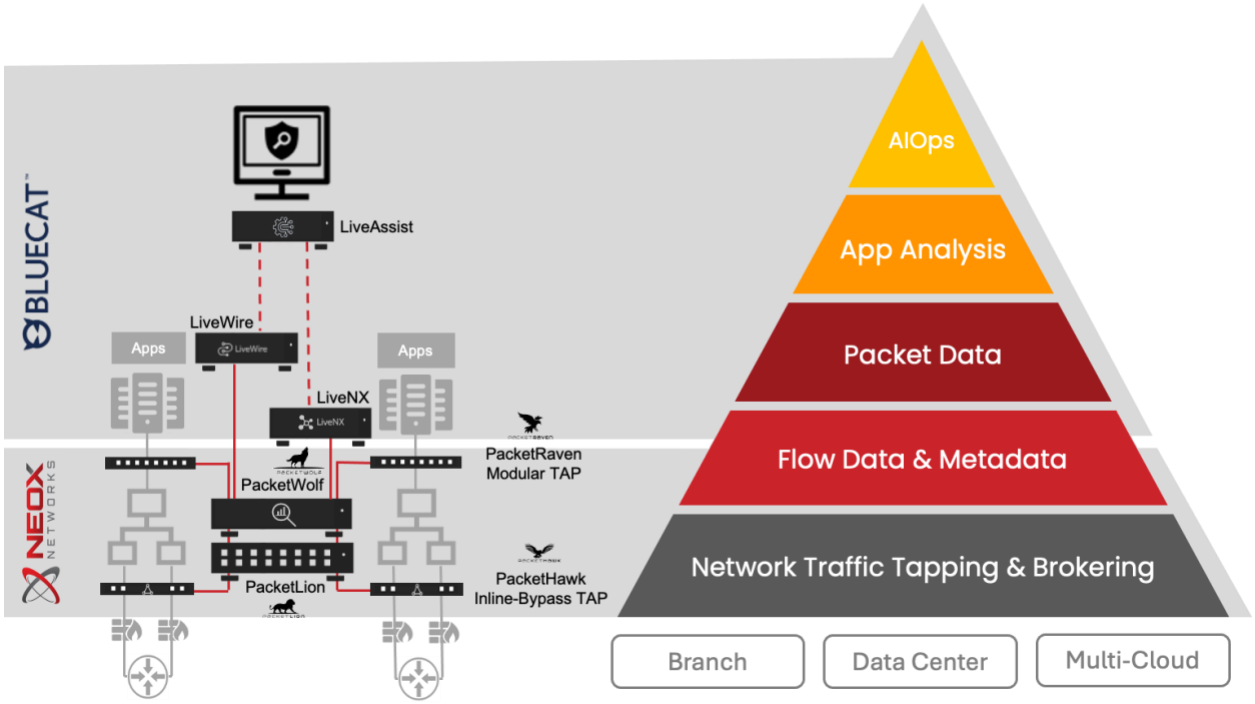


Diagram-1: NEOX and BlueCat Application Observability Solution

BlueCat Network & Application Observability

Deploy BlueCat LiveNX to collect and correlate network flow records, device metrics, topology and application context for service health, QoS, path analysis and troubleshooting. LiveNX delivers comprehensive observability for network and application performance across your entire infrastructure—all through a single, intuitive interface. By collecting, correlating, and analyzing vast volumes of complex network and application data, LiveNX transforms insights into actionable intelligence, empowering NetOps teams to quickly identify issues, optimize performance, and drive better business outcomes. Gain a real-time, end-to-end view of your network health and seamlessly drill down from the entire network to a specific site, individual hop, or even a single packet—all in just a few clicks.

Deploy BlueCat LiveWire to provide packet capture (PCAP) data and granular packet analysis at selected points. LiveWire empowers NetOps and SecOps teams with advanced network forensics and deep packet-level drill-down to strengthen network performance, security, and operational resilience. By capturing, analyzing, and correlating network packet data in real time and at scale, LiveWire delivers actionable insights into network and application behavior, enabling teams to rapidly pinpoint issues, accelerate troubleshooting, optimize performance, and minimize business disruptions.

Flow records may come from network devices or from appropriately configured NEOX flow-generation capabilities on its packet brokers; raw packet feeds are separately distributed to LiveWire or other packet-analysis tools. NEOX TAPs and packet brokers do not themselves replace LiveNX infrastructure telemetry, while LiveNX does not replace the physical traffic acquisition layer. The precise integration should be validated for supported export formats, transport, capacity and deployment licensing.

BlueCat AIOps-Assisted Insights

Reduce your workload and deploy BlueCat LiveAssist as an optional add-on for natural-language investigations and guided root-cause assistance; it is not the packet-capture engine or packet broker. LiveAssist delivers AI-powered network intelligence by continuously analyzing network telemetry, alerts, and configuration data across your infrastructure. Through an intuitive, natural-language interface, LiveAssist empowers network engineers to ask questions, uncover actionable insights, and gain real-time visibility into network issues. By accelerating root cause analysis and providing guided remediation steps, LiveAssist simplifies troubleshooting, reduces resolution times, and improves overall network performance and operational efficiency.

Application Troubleshooting Workflow Example

- BlueCat LiveNX alerts about increased application latency or degraded voice quality at a site.
- The engineer reviews topology, path, interface and flow data to isolate the segment and affected traffic.
- Relevant packets from NEOX PacketOps device feeds such as packet brokers are captured and analyzed with LiveWire to examine the underlying cause, if that integration and capture path are deployed.
- LiveAssist can summarize related evidence and suggest follow-up checks; the operator validates the diagnosis and remediates the fault.

Key Benefits

1. **End-to-End Visibility Across Hybrid Networks:** Gain consistent visibility into selected traffic paths across campus, data center, WAN/SD-WAN, branch and cloud environments. NEOX TAPs and packet brokers acquire, aggregate and deliver relevant network traffic, while BlueCat LiveNX correlates flow records, topology, device metrics and application context. Teams can follow application behavior across network domains, recognize emerging performance anomalies and identify where deeper packet investigation is needed. LiveWire provides packet-level evidence at instrumented locations, helping bridge the gap between broad operational visibility and detailed diagnosis.
2. **Faster Root-Cause Isolation:** Accelerate investigations by moving from LiveNX service-health dashboards and application views to the specific paths, devices, interfaces and flows associated with an incident. Where LiveWire capture is deployed, engineers can examine relevant packet evidence to validate suspected causes such as retransmissions, loss or application response delays. NEOX traffic filtering and distribution help deliver the appropriate traffic to each analysis tool. This coordinated workflow reduces manual correlation across disconnected consoles, supports more confident troubleshooting and helps lower mean time to resolution (MTTR).
3. **High-Fidelity, Tool-Ready Network Data:** Establish a reliable traffic visibility foundation using NEOX PacketRaven and PacketHawk TAPs together with PacketLion, PacketWolf or PacketTiger packet brokering as appropriate. Aggregate traffic from multiple observation points and apply selective filtering, packet slicing and supported deduplication to reduce unnecessary tool load. Where configured and licensed, supported NEOX platforms can also generate NetFlow/IPFIX for flow analytics. Distributing fit-for-purpose packet and flow feeds helps protect monitoring capacity, improve data relevance and extend the value of existing observability and security investments.
4. **AI-Assisted Network Operations:** Extend the LiveNX and LiveWire investigation workflow with the optional BlueCat LiveAssist capability. Engineers can ask natural-language questions about network telemetry, alerts and configuration context instead of manually navigating every data source. LiveAssist can surface related evidence, suggest likely causes and recommend guided follow-up checks to support faster triage. These AI-assisted insights help standardize troubleshooting across teams and reduce repetitive investigation effort. Operators remain responsible for verifying conclusions, approving changes and confirming successful remediation.
5. **Better Application Experience and Capacity Decisions:** Connect network conditions to application and user experience by correlating traffic flows, QoS metrics, route changes, interface utilization and device health. Identify congestion, latency, packet loss and abnormal traffic patterns before they become prolonged service disruptions. Use historical trends to distinguish persistent capacity constraints from transient faults and to prioritize targeted remediation. Better evidence supports bandwidth planning, service-level discussions and more efficient infrastructure investment, while helping NetOps maintain dependable performance for business-critical applications.

Solution Deployment Best Practices

- **On-Premises Data Center and Campus**
  Deploy passive NEOX TAPs at critical aggregation, core, interconnect and service links to capture the north–south and east–west traffic relevant to key applications. Use PacketLion for high-density TAP/SPAN aggregation and traffic distribution, with PacketWolf for advanced processing such as supported deduplication, slicing and flow generation where required; PacketTiger can provide a consolidated option for smaller deployments. Feed appropriately selected packets to LiveWire and export supported NetFlow/IPFIX records to LiveNX when configured. Confirm link speeds, redundancy, oversubscription limits and capture placement before rollout, and test representative application paths under peak traffic conditions.

- **WAN, SD-WAN and Branch Edge**

  Use router and switch flow exports, SNMP/device metrics and available SD-WAN telemetry in LiveNX to understand path selection, transport health, QoS, tunnels and application behavior across distributed sites. Prioritize business-critical branches and links where poor experience or intermittent faults warrant deeper investigation. Where packet evidence is needed, deploy suitable NEOX traffic access and brokering at the branch, hub or data-center edge and deliver selected feeds to LiveWire. Minimize backhaul of raw packets over constrained WAN links; evaluate local capture, selective filtering, transport security and retention requirements. Validate visibility across primary and failover paths.

- **Hybrid and Public Cloud**

  Capture relevant cloud traffic through provider-native mirroring or supported virtual TAPs and, where appropriate, aggregate and filter it through virtual packet brokering. Combine these packet feeds with available cloud, virtual-network and device flow telemetry in LiveNX to maintain application context across on-premises and cloud boundaries. Identify east–west paths, ephemeral workloads and encrypted traffic limitations early in the design. Size mirrored traffic and packet capture for expected peaks, and assess egress and mirroring charges before deployment. Establish data residency, access control and PCAP retention policies, and verify compatibility with each cloud provider and target tool.

- **Design and Operational Safeguard**

  Begin with an application-centric visibility map identifying critical services, traffic sources, network paths, blind spots and intended tool destinations. Size TAPs, brokers, processing resources and flow-export capacity using measured peak throughput, packet rates and realistic oversubscription assumptions. Apply least-privilege access, secure management, time synchronization and explicit retention controls for packet captures and telemetry. Validate supported NEOX export formats, LiveNX/LiveWire ingestion interfaces, optional LiveAssist licensing and feature availability for the target releases. Test failover and the complete workflow—from anomaly detection and flow investigation to packet analysis, guided diagnosis and verified remediation—before production acceptance.

NEOX Networks
NEOX Networks provides unified network visibility solutions for IT and OT observability and security. Its TAP, packet brokering and processing portfolio helps customers obtain and distribute high-fidelity network traffic for monitoring and analytics. neoxnetworks.com

BlueCat Networks
BlueCat's LiveNX delivers network and application performance observability across complex, multi-vendor environments. LiveWire adds packet-level analysis, while optional LiveAssist supports AI-guided NetOps investigations. bluecatnetworks.com