Optimized Flow-Based Security Analytics Using Open Data Platforms

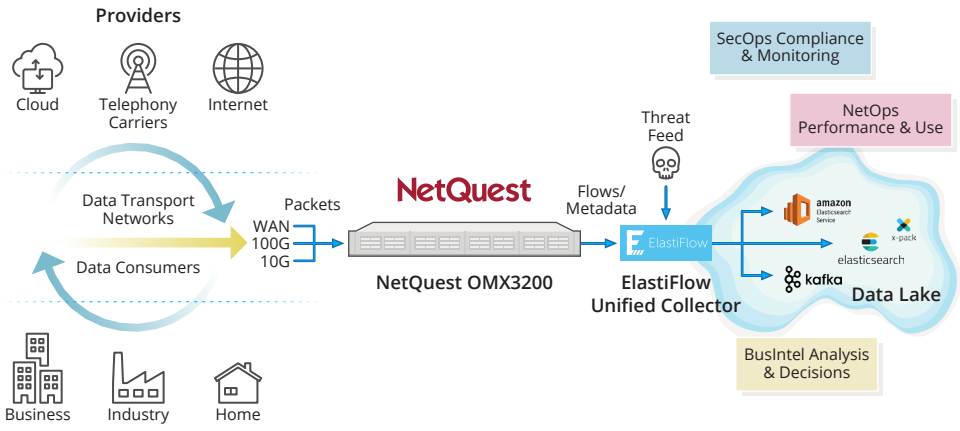
The challenge facing today's IT sector is how to scale real-time security monitoring on networks that are experiencing rapid data growth from a constantly rising number of bandwidth hungry connected devices. Security operations teams are required to handle increased bandwidth and maximize visibility despite ever-evolving network architectures. Internet service providers are building out 5G mobile networks and using edge data centers to move applications closer to the end-user; enterprises are transitioning their IT infrastructure to the cloud.

To eliminate network blind spots and overcome this big data dilemma, security teams are migrating from sampled flow data to full-fidelity network metadata for threat intelligence. At the same time, network traffic is migrating to 100 Gbps and beyond, placing a heavy processing burden on networking equipment, compute resources and budgets. Very few network security solutions can cost-effectively meet the monitoring demands of today's extreme scale networks.

Scalable Flow-Based Security Solution Overview

NetQuest and ElastiFlow offer a combined security analytics solution with a ***real-time*** methodology:

1. Process 100% of packets from congested 10G and 100G traffic links and track flow-based statistics
2. Convert real-time flow information into standards-based IPFIX data records
3. Collect, transform, and normalize data to enable use of common open data analysis platforms
4. Enrich network information for providing additional context to investigate and identify threat conditions
5. Provide a set of pre-loaded flow analysis modules for visualizing data and simplifying analysis



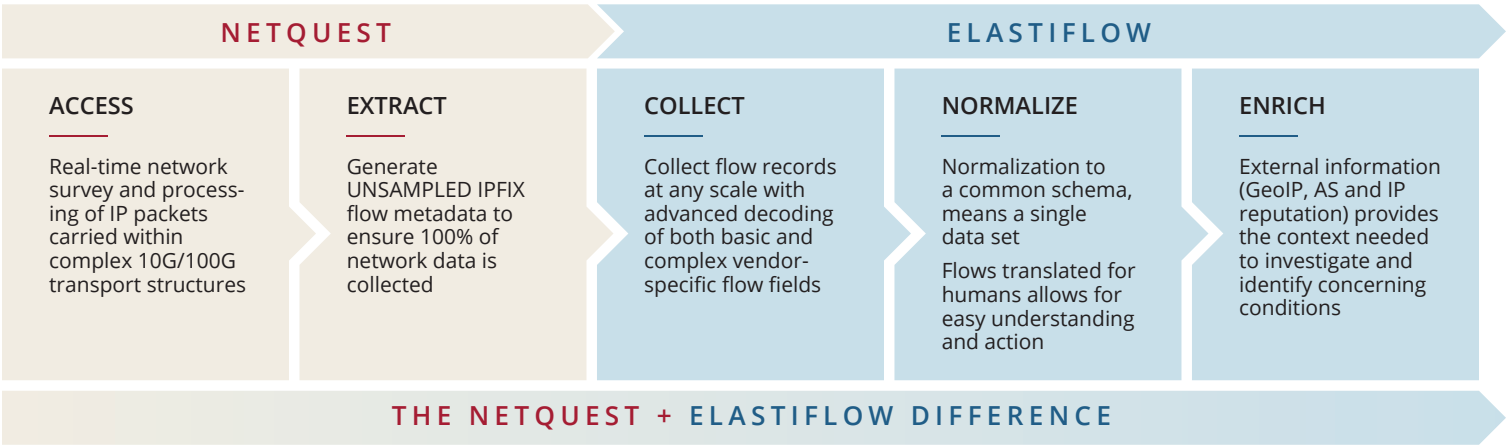
Who We Are

NetQuest is a trusted and longstanding supplier of high-performance Cyber Surveillance solutions to government agencies around the globe.

With the introduction of the OMX Optical Monitoring Exchange we have built upon our 30+ years of network monitoring experience and applied the indepth cyber knowledge we have gained to offer an optimized solution for complex network infrastructures, such as fixed line/mobile service providers and large-scale enterprise networks.

NetQuest
Monitoring Access Solutions

NetQuest OMX3200 and the ElastiFlow Unified Flow Collector



Analyze data further up the wire – Bad actors can cover their tracks by manipulating applications and compute devices within the network infrastructure. The scale of the NetQuest-ElastiFlow joint solution enables the analysis of real-time traffic from taps off large regional backbone networks and cloud uplinks to detect command and control messaging as well as callbacks from infection vectors.

Track network anomalies – When new applications, services, or devices come online, the analysis tools must have visibility to 100% of the traffic flows to detect irregular network behavior. The NetQuest-ElastiFlow joint solution provides complete visibility by processing unsampled IPFIX flow metadata. This allows security teams to view the complete network from a broader lens and analyze behavioral patterns across a wide range of endpoint variables optimizing the ability to detect anomalies and potential threats.

From fiber to analytics – NetQuest and ElastiFlow seamlessly integrate to eliminate the sizing, installation, and compatibility issues typically associated with bolting complementary technologies together. This optimized network flow analysis solution enables organizations to quickly convert real-time network traffic into actionable intelligence.

NetQuest OMX3200 High-Capacity Service Node

NetQuest's OMX3200 High-Capacity Service Node is a multi-terabit traffic flow visibility platform supporting unsampled IPFIX metadata generation and advanced packet processing in a modular 1RU hardware platform.

- Unsampled IPFIX metadata generation transforming packets to flow-based metadata for highly scalable n x 10/100G flow analysis
- Advanced packet processing providing optimized access to IP packets with line-rate header/tunnel stripping
- Automated network survey and WAN auto-discovery for identifying optical network signaling structures
- Compact modular chassis with pay-as-you-grow pluggable modules and field programmable FPGAs provides rapid deployment and flexible upgrades from 10G to 100G+ without rebuilding your visibility architecture

ElastiFlow Unified Flow Collector

ElastiFlow's Unified Flow Collector has grown from an open-source network flow collector with over 35,000 users to a company-supported, highly scalable, network collection/correlation/enrichment resource. The collector supports over 6,200 standard and vendor-specific data fields. After it collects, transforms, and normalizes the flow data, the Unified Flow Collector interoperates with open data platforms such as Elasticsearch, Amazon ElastiFlow Service, and Kafka to enable:

- Network, service and cloud performance analysis
- Security analysis for detailed risk metrics, threat determination and compliance metering
- Cost control of enterprise and outsourced resource utilization

ElastiFlow's Unified Flow Collector can scale to collect and analyze 100% of unsampled IPFIX flow records generated from typical large backbone network links running at 10G and 100G rates.

Technical White Paper

More detailed information on the NetQuest-ElastiFlow joint network visibility solution for real-time security analytics is available as a technical white paper. The white paper provides processing performance details for a specific deployment model monitoring a full-duplex ISP peering link. The solution leverages the OMX3200 and the Unified Flow Collector installed in a single dual-socket server including an Elasticsearch database and a Kibana analytical environment. Scaling options are also cited using a Docker deployment to expand the Unified Flow Collector across multiple nodes across multiple clusters. **Request a copy today!**

WWW.NETQUESTCORP.COM
NetQuest Corporation • 523 Fellowship Road • Mount Laurel, NJ 08054 USA • +1.856.866.0505 • Email: info@netquestcorp.com