Joint Solution Brief

From Packets to Intelligence: Collecting and Generating Network Intelligence at Massive Scale

Highlights

Garland Technology

- PacketMAX powers high-capacity network traffic collection across virtually any network architecture
- High-scale aggregation and replication supports 1:many, many:1, and many:many traffic distribution
- Wire-speed network traffic aggregation, filtering, and load balancing for reliable, sustained delivery of network traffic
- Flexible hardware platform choices support density and interface range for 1G, 10G, 40G, 100G and 400G network links

NetQuest

- Ultra-scale 1:1 network Flow metadata generation identifies end-points, protocols, and applications at scale
- Packet-to-metadata data reduction dramatically reduces data footprint by up to 99.5%
- Enriched Flow Intelligence reveals protocol-specific attributes and application classifications for clear and encrypted traffic
- Encrypted traffic analysis extracts fingerprints signatures, and heuristics to accelerate threat detection
- Intrinsic packet-flow optimizations and delivery for forensic investigations and reconstruction activities

The Problem

In today's hyperconnected world, virtually all communication traverses the network. Because the network interconnects everything, network traffic contains volumes of real-time intelligence that can be harnessed and mined for many important use cases ranging from network intelligence, security monitoring, threat hunting and forensics to lawful intelligence activities.

The challenge is with the proliferation of higher speed desktop, server and network interconnections the amount of traffic crossing networks has reached unprecedented levels and continues to grow exponentially. One hour of network traffic on a single 100G link can reach 45 terabytes. With the growing adoption of higher network speeds and the need to monitor more links to observe east-west traffic, monitoring and security tools are easily overwhelmed by the massive amounts of traffic to ingest and analyze. In addition to the unrelenting data explosion, the complexity of user and server network transactions and ever-changing threat landscape means more granular details must be extracted from network traffic to enable effective intelligence and analysis.

Flow-based metadata extracted from network packets overcomes these challenges to enable the efficient observation of all traffic in motion. Unsampled flow metadata is an abstraction of network traffic based upon full packet analysis of the wire data. It provides a rich, lower footprint, high-value data set with critical insights about who is connecting to the network and what is being accessed and shared without the burden of collecting, processing and storing high volumes of packets.

The Joint Solution

The joint Garland Technology-NetQuest solution empowers SecOps and NetOps teams to overcome these challenges by enabling efficient and high-scale monitoring to extract intelligence from virtually any network environment covering hundreds to thousands of network links and millions to billions of flows per second.

The Garland Technology PacketMAX™ Network Packet Broker acquires network traffic from across an organization's physical network and cloud footprint and aggregates and delivers network packets to the NetQuest Streaming Network Sensor™ for intelligent metadata creation at the speed of the network. The Streaming Network Sensor generates deep intelligent metadata that extends beyond basic NetFlow traffic statistics with rich insight into all activities traversing the network for clear and encrypted traffic.

Together the joint Garland and NetQuest Traffic Aggregation and Metadata solution is capable of collecting and translating petabytes of raw network packets into compact and highly efficient metadata containing detailed information about network activity to enable a wide range of operational missions for diverse intelligence activities at scale.

By combining the cost-effective PacketMAX platform with ultra-scale metadata creation, SecOps and NetOps teams can achieve higher capacities with richer metadata without compromising fidelity or service trade-offs empowering organizations to break-through the performance barriers, packet processing limitations and the high costs of smart packet broker systems.

Garland Technology PacketMAX

Garland Technology ensures complete 360-degree network visibility with a comprehensive family of network access solutions. Enabling complete network visibility, Garland's TAP-to-Tool™ architecture includes purpose-built Network Packet Brokers, Advanced Traffic Aggregators, Breakout TAPs, Regeneration TAPs, Advanced All-In-1 Filtering TAPs, Inline Edge Security Bypass TAPs, Hardware Data Diodes and Cloud Access Solutions.

The Garland PacketMAX enables high-scale acquisition of network traffic with wire-speed traffic replication that enables collecting, aggregating and distributing all network traffic to any monitoring tool, analytics system, or packet storage platform. The Garland PacketMAX platform delivers market-leading performance and scales packet-flow access to significantly lower the cost of network traffic acquisition while optimizing the ability to cost-effectively monitor more links across an increasingly complex network environment.

NetQuest Streaming Network Sensor

The NetQuest OMX™ deployed as a Streaming Network is a powerful intelligent ultra-scale network data source that enables organizations to keep up with fast-moving, high value network intelligence by extracting metadata and packet flows from network traffic. The Streaming Network Sensor delivers multi-terabit, wire-speed advanced packet processing and analysis services specifically tuned for security monitoring environments that rely on accurate and reliable network packet intelligence at scale.

The Streaming Network Sensor is purpose-built for deep network traffic analysis for 10G, 25G, 40G, 100G and 400G network monitoring environments. Leveraging the NetQuest OMX platform's powerful FPGA-based distributed pipeline processing architecture, the Streaming Network Sensor analyzes network traffic in a single pass without consuming multiple analysis ports for different services.

Deep Packet Inspection services and metadata creation are performed simultaneously at wire-speed to inspect Petabytes of network packets per hour for both clear and encrypted traffic enabling pervasive visibility of all traffic in motion and to extract the metrics that matter most with packet-like accuracy.

Seamless Interconnection and Integration

Garland's Network TAPs are strategically deployed to provide access to critical network links to acquire all network traffic in real-time. TAPs and SPAN/Mirror feeds are then sent to the packet broker to identify and aggregate the collected network traffic for delivery to the NetQuest Streaming Network Sensor. Based upon user-defined policies, traffic can be pre-filtered by the PacketMAX platform to deliver specific targeted traffic types or flows.

The PacketMAX supports many-to-many, one-to-many or many-to-one aggregation, so traffic can be collected from multiple slower links, such as 10G, 25G or 40G east-west traffic links, and aggregated for delivery to the NetQuest Streaming Network Sensor over a single 100G link for improved efficiency. To maintain packet-flow integrity, the PacketMAX can tag the acquired traffic to identify the source link/port and then aggregate and load balance the delivered traffic to assure that each monitored flow is consistently delivered to the correct Streaming Network Sensor.

For high-density, large-scale environments, multiple Garland PacketMAX platforms can be interconnected to the same physical Streaming Network Sensor, or to multiple systems, while maintaining the integrity of the source traffic. The number and speed of the interconnection uplinks between the PacketMAX and the Streaming Network Sensor are determined by the peak volume of traffic to be processed enabling cost-efficient, scale-out monitoring architectures.

Unmatched Ultra-Scale Metadata Capacity

To meet large-scale monitoring requirements, the Streaming Network Sensor ultra-scale capacity enables processing nearly one petabyte of network traffic per hour and up to 17 petabytes of network traffic per day, per system. As shown in the reference architecture on the next page (Figure 1), unlimited linear scale is achieved when multiple PacketMAX Packet Brokers and Streaming Network Sensors are deployed across the monitored environment. This scale-out architecture is capable of monitoring hundreds of exabytes of network traffic to support mega-capacity monitoring requirements.

Streaming Network Sensor appliances can be centrally clustered or distributed across the network. Multiple distributed monitored environments can feed streaming metadata to a single or multiple centralized analysis systems or data lakes to meet high-scale analysis capabilities.

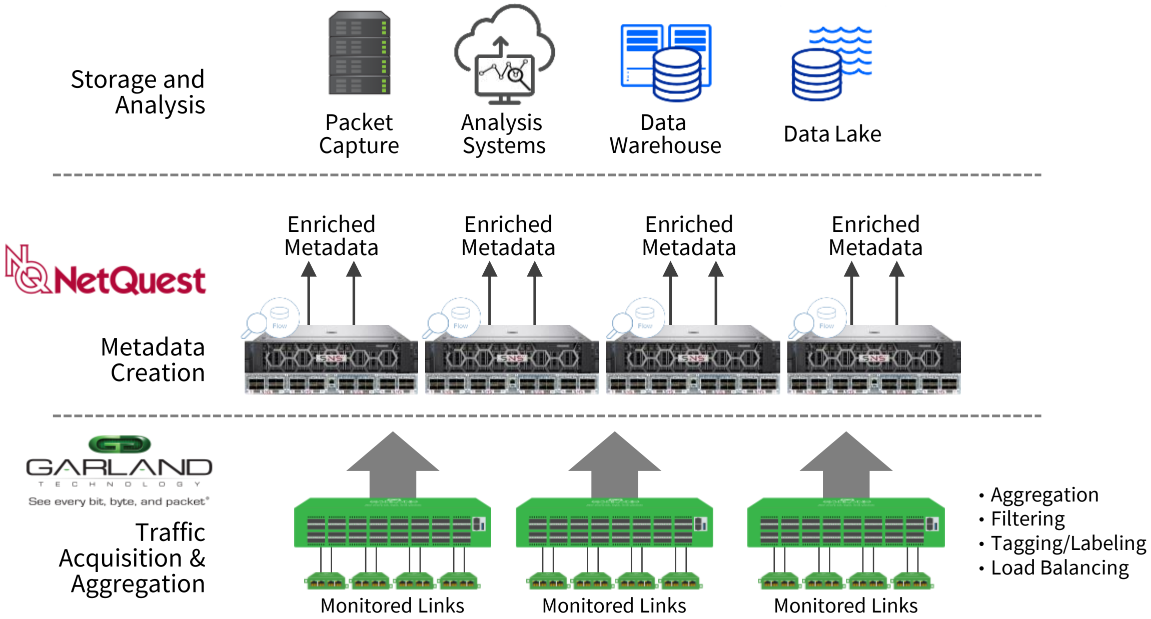

Figure 1: The Garland-NetQuest joint reference architecture shows a single monitored site leveraging the Garland comprehensive TAP-to-Tool™ solution acquiring traffic from hundreds of network links to enable real-time enriched metadata creation for all network traffic.

Rich Unsampled Flow Metadata at Scale

The NetQuest Streaming Network Sensor observes all traffic and analyzes every packet and flow in real-time as it crosses the wire. Analyzed traffic is translated 1:1 to highly efficient unsampled Flow metadata containing detailed information about network, application, and user activity with no dropped packets. Hardware-based wire-speed Deep Packet Inspection enables IPv4 and IPv6 traffic analysis inside tunnels and beyond packet headers to reveal the inner IP payload and headers exposing unobstructed Layer 2-7 network traffic insights.

A comprehensive range of metadata can be extracted from the network traffic providing deep contextual user activity and connection insights. Analysts can define the specific metadata fields to be extracted based upon flexible criteria and hundreds of available data fields such as:

- Network statistics and traffic patterns
- Specific protocols and services
- Encrypted traffic handshakes and headers
- Application-level metadata
- Subscriber/user information mobile devices

The metadata generated by the Streaming Network Sensor can be filtered to target specific metadata of interest to reduce noise, optimize upstream data collection and minimize the storage burden. Configurable output load balancing enables the Streaming Network Sensor to optimize and scale metadata delivery. Metadata can be delivered to 16 different collectors to support multiple monitoring platforms and/or segregate metadata into defined groups to optimize or isolate upstream collection to meet regulatory requirements.

Application-Layer Enriched Metadata

When application-layer metadata is required, the NetQuest Streaming Network Sensor can deliver metadata with Enriched Flow Intelligence™ to reveal protocol-specific attributes and application classifications for clear and encrypted traffic. Layer 4-7 enrichment provides contextual metadata with protocol and application-specific attributes for thousands of applications and services crossing the network.

Encrypted Traffic Analysis (ETA) automatically identifies encrypted flows and extracts fingerprints signatures, and heuristics to accelerate threat detection and identify potential indicators of compromise without the need for slow and expensive decryption. This enables identifying threats hiding in encrypted traffic such as command and control attacks, malware, and data exfiltration.

Application-level and encrypted traffic visibility automates and accelerates the detection of threats, anomalous activity, and evasive traffic powering deep network and user traffic intelligence. The Streaming Network Sensor Enriched Flow Intelligence capabilities include:

- Identifies 3800+ Layer 7 applications
- Protocol-specific metadata, such as DNS, HTTP, SIP, BGP, MPLS, SIP
- Mobile user end point details such as IMEI, IMSI, MSISDN
- Encrypted traffic analysis of TLS, IETF QUIC, GoogleQUIC, SSH
- Encrypted traffic fingerprints, such as JA3C, JA3S, HASSH

Joint Solution Brief

Efficient Traffic Optimization

The Streaming Network Sensor observes, analyzes, and processes raw network traffic at scale and efficiently generates relevant metadata in real-time without compromising packet traffic fidelity and granularity. The Metadata creation process reduces the upstream data footprint of network traffic up to 99.5 percent – with the metadata typically representing less than 1% of the monitored network traffic volume.

The metadata output record size delivered is defined by the network traffic characteristics and the number metadata fields required for analysis. Additional filtering and optimizations can be implemented to further reduce the actual metadata output to focus analysis on the data sets that matter. For distributed monitoring requirements, these optimizations help reduce the volume of data to be backhauled to centralized collection points, thus reducing WAN bandwidth consumption and lowering transport costs.

Packet Collection for Traffic Reconstruction

To meet diverse monitoring requirements, when packet-flow traffic is required for historical reconstruction and forensic activities, the Garland PacketMAX can replicate and direct the same acquired packets to other tools as-is or send the traffic to the Streaming Network Sensor platform for advanced packet processing and optimization services. The Streaming Network Sensor can return the conditioned packet traffic back to the PacketMAX for redistribution to targeted packet-based tools.

The Streaming Network Sensor can retain or drop any tagging added by the PacketMAX platform, and if needed, the Streaming Network Sensor can further tag, or retag, the conditioned packets to identify a source port or a specific tool destination.

The Value Realized

The threat landscape is ever changing, so when conducting investigations in today's hyperconnected world, access to uncompromised intelligence is essential to enabling rapid time to knowledge. Organizations must keep up with the speed of todays' networks, so the ability to seamlessly connect to the network to acquire traffic is more important than ever. As intelligence needs evolve and network traffic grows the joint Garland Technology-NetQuest solution can quickly adapt to extract network intelligence from new traffic types at faster speeds to scale without limits.

Together Garland Technology and NetQuest enable building an ultra-scale network traffic collection and metadata creation solution that empowers operators and agencies to collect and analyze network traffic at massive scale to quickly identify threats and uncover critical insights at unprecedented speed and performance. When compared to other well-known smart packet broker systems, the combined Garland-NetQuest solution delivers significantly higher density with more capacity, functionality, and greater performance at scale than alternative solutions in its class to meet the most demanding intelligence and monitoring requirements.

About Garland Technology

Garland Technology is an industry leader delivering network products and solutions for enterprises, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs), enabling data centers to address IT challenges and gain complete network visibility. For more information or learn more about the inventor of the first bypass TAP, visit: GarlandTechnology.com or @GarlandTech.

About NetQuest

NetQuest provides market-leading Ethernet and WAN Flow and Packet-Based traffic monitoring solutions that deliver the highest levels of accuracy, capacity, and performance at scale. Monitoring solutions from NetQuest are deployment-proven across thousands of network segments in enterprise, carrier, government, and defense agency networks across the globe, empowering security operations teams with high-scale visibility and actionable traffic intelligence.

This is a joint solution of NetQuest and Garland Technology and requires multiple products to enable the capabilities referenced. Functionality will vary by physical devices, operating modes, and licenses deployed. NetQuest and Garland Technology reserves the right to make changes to their respective technical information and specifications without notice at any time. The use of the word partner does not imply a partnership relationship between NetQuest and Garland Technology. NQ-GT-Metadata-JSB-11524

NetQuest Corporation
523 Fellowship Road, Suite 205
Mount Laurel, NJ 08054 USA
+1-856-866-0505 | sales@netquestcorp.com
www.netquestcorp.com