Joint Solution Brief

Collecting, Storing, and Analyzing Network Intelligence at Massive Scale

Highlights

NetQuest

- Always-on ultra-scale network visibility across large-scale networks without performance limitations
- 1:1 Flow metadata generation identifies end-points, protocols, and applications
- Enriched Flow Intelligence reveals protocol-specific attributes and application classifications for clear and encrypted traffic
- Simultaneous packet-flow optimization and delivery for forensic investigations and reconstruction activities

Ocient

- Massively scalable data storage for multiple petabytes of data and trillions of records
- 10x-100x faster query time with 1/5 the storage footprint of copy-based systems
- Rapidly filter data fields of interest from comprehensive hyperscale datasets
- Enable long retention times of hyper scale datasets with optimized records and storage

The Problem

In today's hyperconnected world, virtually all communications traverse Communication Service Provider (CSP) networks. Because these networks interconnect everything, they contain volumes of untapped intelligence that can be harnessed and mined for many use cases ranging from network intelligence, security forensics and threat hunting to lawful intelligence activities.

Since the network sees everything, extracting intelligence from CSP networks is critically important. However, with the proliferation of fixed and wireless gigabit network speeds to users, the amount of traffic crossing CSP networks has reached unprecedented levels and continues to grow exponentially. In addition to the unrelenting data explosion, the complexity of users' network transactions and ever-changing threat landscape means more granular details must be extracted from network traffic to enable effective intelligence.

But collecting detailed network and communications data is only half the challenge. To harness the true power of extracting intelligence from network traffic, operators must also execute the difficult task of rapidly ingesting, storing, and analyzing these large datasets at scale to quickly extract accurate and meaningful insights.

The Joint Solution

The joint Ocient-NetQuest solution enables operators to overcome the inherent challenges of working with network traffic at massive scale. By combining real-time, ultra-scale network traffic collection, analysis, and metadata creation with hyperscale metadata ingest, transformation, processing, and storage, Ocient and NetQuest deliver unparalleled network monitoring and analytics capabilities. Together, joint NetQuest and Ocient solutions empower organizations to intelligently monitor virtually any operating environment passing billions of flows per second. Our joint solutions are uniquely able to analyze trillions of data records at multi-petabyte scale to deliver mission-critical insights with unmatched analytics speed for diverse intelligence activities at scale.

Ocient Hyperscale Platform

The Ocient hyperscale platform enables the ingest, storage, and analysis of massive sets of network traffic metadata, rapidly extracting insights from datasets spanning weeks, months, and years of activity. Ocient seamlessly joins multiple hyperscale datasets, interconnecting and correlating data from multiple sources to enrich them further. Operators can then analyze and filter fields of interest in near real-time for diverse intelligence activities.

Ocient's flexible SQL engine can ingest, store, transform, and analyze agnostic metadata at 100% resolution, returning complex query results in seconds versus hours or days. Ocient's simple and efficient data warehouse architecture rapidly accelerates query speed by placing compute adjacent to storage on NVMe SSDs. As a result, Ocient's highly parallelized system is the most cost-effective, highest performance solution for hyperscale network metadata analysis.

NetQuest OMX Platform

The NetQuest OMX™ deployed as a Streaming Network Sensor™, is uniquely capable of keeping up with Ocient's ability to ingest fast-moving network intelligence through the delivery of massive volumes of network metadata. The ultra-scale OMX acquires traffic data from across an organization's entire physical network and translates petabytes of network traffic into compact and highly efficient metadata containing detailed information about network activity for both clear and encrypted traffic. For targeted communication reconstruction requirements, network packets can also be collected and forwarded to packet-based tools for full contextual visibility into traffic payloads when deep historical forensic investigations are required.

OMX is an FPGA-based appliance purpose-built to deliver multi-terabit-scale wire-speed metadata creation and advanced packet processing services. Its software-defined architecture enables feature flexibility with multiple operational modes on the same hardware with high-density 10G, 40G, 100G and 400G ports. The OMX platform's unique distributed pipeline processing architecture allows metadata creation activities and packet optimization services to be performed simultaneously at wire-speed – delivering uncompromising sustained performance at scale. As a Streaming Network Sensor, the NetQuest OMX delivers more than 2-3x higher density, throughput, and packet processing power per rack unit (RU) than alternative smart service brokers at a significantly lower cost with measurably lower power consumption.

Rich Metadata Intelligence

The NetQuest OMX observes and processes 100% of all network traffic and provides 1:1 unsampled Flow metadata at scale to generate uncompromised network intelligence. 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 monitored network traffic to provide deep contextual connection and user activity 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
- Specific protocols and services
- Encrypted traffic handshakes and headers
- Application-level metadata
- Subscriber information for fixed and mobile

The metadata to be delivered to Ocient can be prioritized and filtered to target only the specific metadata of interest to reduce noise, optimize upstream data collection, minimize the storage burden, and accelerate time-to-analysis. Configurable output load balancing enables OMX to manage, optimize, and scale metadata delivery. OMX can deliver metadata to 16 different collectors and support multiple monitoring platforms and/or segregate metadata into pre-defined groups to optimize or isolate upstream collection and analysis to meet regulatory requirements.

Enriched Metadata

OMX Streaming Network Sensor can deliver metadata with Enriched Flow Intelligence™ to reveal protocol-specific attributes and application classifications for clear and encrypted traffic. Application layer analysis of encrypted traffic identifies encrypted connections and extracts fingerprints, signatures, and heuristics to accelerate threat detection and identify potential indicators of compromise without the need for slow and expensive decryption. OMX enriched metadata 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

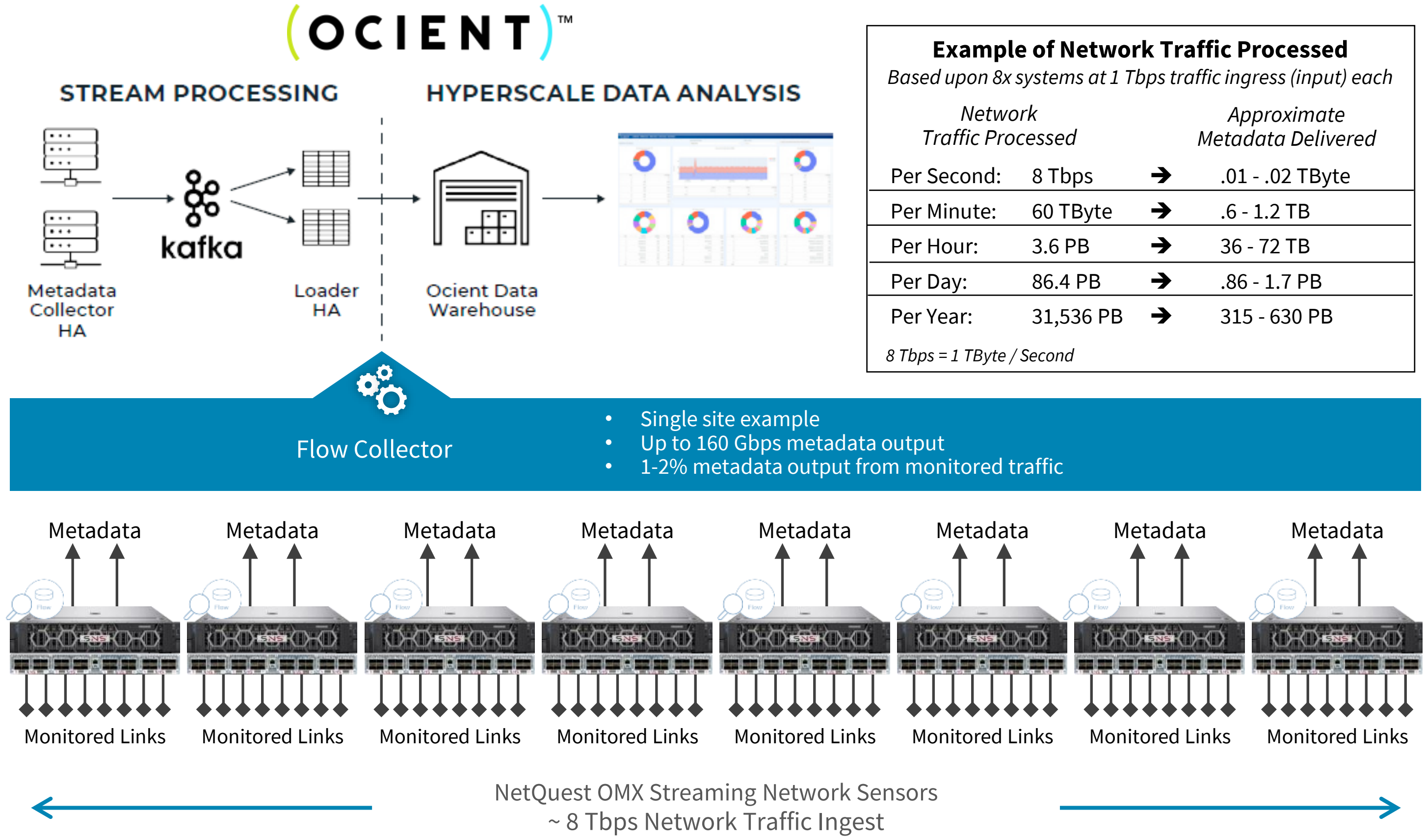
Unmatched Ultra-Scale Capacity

To meet the challenges of mega-bandwidth network environments, each OMX system is capable of processing up to 1.6 Terabits of network traffic per second for metadata creation depending on traffic volumes, characteristics and the depth of intelligence to be extracted. The OMX Streaming Network Sensor operating mode's ultra-scale metadata capacity enables the capture and processing of almost 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 below (Figure 1), virtually unlimited linear scale is achieved when multiple OMXs are deployed side-by-side across the monitored environment, capable of analyzing hundreds of exabytes of network traffic per year, to support mega-capacity monitoring requirements. OMX Appliances can be centrally clustered or distributed across the monitored network and multiple distributed monitored environments can feed streaming metadata to a single Ocient instance to enable massively scalable analysis for all network traffic.

Efficient Traffic Optimization

OMX observes, analyzes and processes raw network traffic at scale, and efficiently generates relevant metadata in real-time for upstream consumption by the Ocient Hyperscale Data Warehouse™ without compromising the fidelity and granularity needed for critical intelligence analysis activities. The generated metadata typically represents only 1-2% of the monitored network traffic. The record size for the output metadata delivered to Ocient is dependent on the monitored network traffic characteristics and the number and size of the metadata fields delivered to Ocient for analysis. In addition, OMX enables intelligent metadata and packet optimization to reduce the volume of data to be backhauled to centralized collection points, helping lower WAN bandwidth requirements and control transport costs.



Example of Network Traffic Processed

Based upon 8x systems at 1 Tbps traffic ingress (input) each

	Network Traffic Processed		*Approximate Metadata Delivered*
Per Second:	8 Tbps	→	.01 - .02 TByte
Per Minute:	60 TByte	→	.6 - 1.2 TB
Per Hour:	3.6 PB	→	36 - 72 TB
Per Day:	86.4 PB	→	.86 - 1.7 PB
Per Year:	31,536 PB	→	315 - 630 PB

8 Tbps = 1 TByte / Second

Figure 1: The joint Ocient-NetQuest reference architecture shows a single monitored telco site covering hundreds of network links to observe all network traffic generating 3.6 Petabytes of peak traffic per hour which equates to more than 31 exabytes of network traffic per year.

Joint Solution Brief

Blazing Fast Query and Analysis

The Ocient Hyperscale Data Warehouse is a highly scalable analytics platform and visualization engine that is capable of ingesting billions of records per second from one or more OMX platforms, minimizing time-to-queryability and returning query results within seconds. Ocient's solutions execute real-time analytics, complex OLAP-style queries, geospatial analytics, and machine learning on hyperscale data sets 10x-100x faster than other solutions while reducing the storage footprint by 80% when compared to copy-based systems. The speed, simplicity and efficiency of the Ocient Hyperscale Data Warehouse enables operators to analyze data at terabits per second upon ingest, consolidate multiple workloads on a single, unified platform, and support thousands of concurrent users across the organization without impacting performance. As the data stores for CSPs continue to scale, Ocient can retain and query full resolution data in a relational format, enabling users to retrieve valuable "needle-in-the-haystack" records, and to detect anomalous behavior across the network.

Packet Collection for Traffic Reconstruction

To meet diverse operational and monitoring requirements, when packets are required for historical reconstruction and forensics OMX can deliver optimized packet-flow traffic to dedicated packet analysis tools from the same ingress network traffic processed for metadata creation. Packet-flow traffic can be filtered and optimized to deliver the targeted and relevant packet-flows as required by various upstream tools. Metadata creation and packet optimization services are applied to monitored network traffic simultaneously, in one pass, without impacting metadata creation performance. The software-defined functional flexibility of OMX can eliminate the need for an additional expensive layer of Network Packet Brokers – reducing TCO and removing the operational complexities associated with managing multiple probes, sensors, and Network Packet Brokers.

High-Scale Optical WAN Monitoring

OMX can be leveraged to monitor high-density fiber optic cables and high-speed WAN links, such as OTN or SONET/SDH, by connecting to the optical fiber pairs. OMX auto-discovers and identifies all traffic traversing the fiber and converts the WAN traffic to IP Ethernet Packets or metadata suitable for traditional monitoring tools – eliminating the need for expensive specialized WAN monitoring systems.

The WAN traffic, now converted to standards-based IP packets or metadata, can be conditioned in the same manner as native IP packet traffic and delivered to Ocient or other upstream monitoring tools.

Example Use Cases

Context-rich Metadata extracted from network traffic can serve a number of important operational missions and use cases ranging from network performance monitoring to security monitoring and threat hunting, to deep user connection and network activity intelligence for law enforcement and national security investigations. Some example use cases addressed by the joint Ocient and NetQuest solution include:

- Network traffic monitoring
- Cybersecurity behavioral analysis
- Threat hunting and detection
- Incident response and remediation
- Fraud detection and investigation
- Internet Connection Record collection
- Lawful Disclosure of data for compliance

The Value Realized

The threat landscape is ever changing, so with today's hyperconnected world when conducting investigations rapid time to knowledge is essential. Together NetQuest and Ocient deliver the highest scale network traffic collection, analysis, and storage capacity to empower operators and agencies to more efficiently collect and analyze network traffic at massive scale to quickly identify threats and uncover critical insights at unprecedented levels of performance. As intelligence needs evolve and network traffic grows the joint Ocient-NetQuest solution can quickly adapt to address new traffic types, faster speeds and consolidate analysis on a single platform to scale without limits. When compared to other disparate approaches, the combined Ocient and NetQuest solution delivers significantly greater capacity, functionality, and performance at scale than alternative solutions in its class to meet the most demanding intelligence requirements.

Copyright © 2023 NetQuest Corporation. All Rights Reserved. NetQuest, the NetQuest logo, OMX, Streaming Network Sensor and Enriched Traffic Intelligence are trademarks of NetQuest Corporation. Ocient and the Ocient Logo and Ocient Hyperscale Data Warehouse are trademarks of Ocient. All other brands and product names are trademarks of their respective owners. This is a joint solution of NetQuest and Ocient and requires multiple products to enable the capabilities referenced. Functionality will vary by physical devices and/or licenses deployed. NetQuest and Ocient both reserve the right to make changes to its technical information and specifications without notice at any time. The use of the word partner does not imply a partnership relationship between NetQuest and Ocient. NQ-OCT-JSB-0523-R1

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