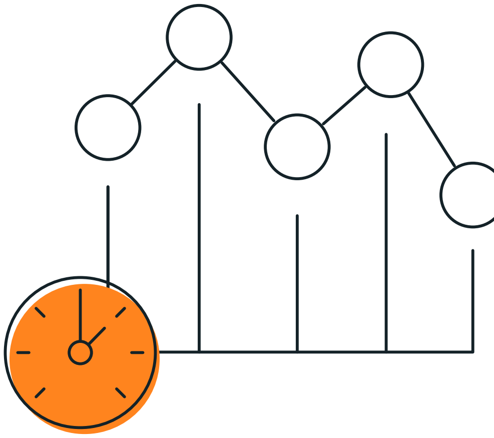
Gigamon® | OCIENT®

Monitor and Analyze Metadata Rapidly With Gigamon and Ocient



THE CHALLENGE

With the proliferation of household gigabit connections and 5G networks, the amount of data being transmitted has reached unprecedented scale. New requirements for BYOD and IoT add additional complexity and make gaining insight into network transactions more difficult than ever.

While network traffic solves half the problem, it must be ingested, transformed, and stored effectively to provide meaningful insight, which can be expensive and require extensive resources.

THE SOLUTION

Ocient's Data Analytics Platform, coupled with Gigamon Hawk, provides a highly scalable, high-performance, and cost-effective network metadata monitoring and analysis solution.

JOINT SOLUTION BENEFITS

- Provides pervasive network visibility across physical, virtual, and cloud infrastructures
- Stores petabytes of traffic as metadata without compromising query performance
- Offers fast interactive analytics and insights within seconds for months and years of data
- Enables easy filtering for fields of interest from joined hyperscale datasets

Introduction

Ocient enables the management, storage, and analysis of Petabyte Scale and Quadrillion row datasets. Gigamon Hawk acquires traffic from across an organization's entire physical and virtual network, and its extended network metadata approach provides detailed information about activity on the network. Together they can handle billions of flows per second, enabling real-time metadata analysis.

The Gigamon + Ocient Joint Solution

Key features of Gigamon Hawk, the Hybrid Cloud Visibility and Analytics Fabric, that enhance Ocient include:

- **Easy access to traffic from a physical network:** Gigamon Hawk enables traffic from across the network to be managed and delivered to tools efficiently and in the format they need.
- **Easy access to traffic from a virtual network:** East-West datacenter traffic is growing increasingly fast. Gigamon Hawk can tap this traffic and incorporate it into the rest of the Hawk fabric for delivery to the tools you are using physically on-prem as well as in the cloud. That ensures all traffic can be monitored and analyzed together, preventing blind spots, increasing the likelihood of spotting suspicious behavior, and eliminating the need to learn a new set of tooling for virtual environments.
- **Traffic filtering:** There's no point in loading a tool with traffic it will just drop after identifying it, such as database traffic going to a web application firewall (WAF). Gigamon Hawk can be configured to only send relevant traffic — or relevant sessions — to the connected tools.

- **Aggregation to cover asymmetric routing and LAG:** Gigamon Hawk can aggregate the two before sending them to the tool, to minimize the number of ports that need to be used on the tool. More importantly, most security devices require all the packets in a session be inspected by the same device and incomplete sessions risk getting blocked or uninspected. Hawk provides an intelligent and efficient way to ensure inspection happens in most architectures. By tagging the traffic, it also ensures the source of traffic can be identified.
- **De-duplication:** Pervasive visibility means that you will be tapping or copying traffic from multiple points in the network, so you will see the same packet more than once. To avoid the unnecessary overhead of traffic backhaul, load on tools' processing, or tools providing false network indicators, Gigamon Hawk has a highly effective de-duplication engine to remove duplicates before they consume resources.
- **Header stripping for efficiency:** If the connected tool doesn't need to see the body information within the packet, Gigamon Hawk can remove it before sending the packet header to the tool for processing. This reduces load on the device and increases its efficacy.
- **Flow and meta-data (NetFlow/IPFIX/CEF) generation:** Gigamon Hawk can generate unsampled NetFlow/IPFIX flow data and/or IPFIX/CEF metadata for any traffic flow. This includes generating extended metadata records for things like HTTP response codes and DNS queries selected from over 5,000 attributes. This extended metadata can be used to provide far more detailed contextual analysis when looking at network and security events.

While Gigamon Hawk generates a steady stream of IPFIX data, Ocient's high performance, hyper-scale enterprise data warehouse platform enables organizations to find needle-in-the-haystack insights from full resolution network traffic data in interactive time. Ocient can transform, ingest, and store format-agnostic metadata at 100% resolution with a flexible SQL engine that returns complex query results in interactive time (in seconds versus days). Key features that enable Ocient to achieve unprecedented speed at limitless scale include:

- **Compute Adjacent Storage on NVMe:** Ocient maximizes compute at the NVMe IO tier, lowering the number of context switches and memory copies in the data path and freeing up memory bandwidth and CPU for other tasks
- **Built-In Streaming and Transformation:** Ocient transforms complex data types at terabits per second during ingest and makes it available for ad hoc analysis using SQL semantics and machine learning in near real-time
- **Dynamic Workload Management in a Multi-Tenant Environment:** Ocient enables customers to co-locate mixed OLAP-style workloads on a single unified platform, re-use data across silos, and serve thousands of concurrent users while maintaining performance
- **Enterprise-Grade Reliability with a Minimal Storage Footprint:** Ocient leverages efficient compression and erasure coding to achieve high availability and reliability while reducing the storage footprint by 80% or more compared to copy-based systems
- **SQL Filtering:** Ocient utilizes standard SQL semantics to build queries that enable fast filtering on millions of rows of data
- **Data Enrichment:** Ocient can scale to meet the demands of multi-dimensional data types, ensuring the system remains flexible as data requirements grow and evolve

By eliminating disparate systems and streamlining the data path from network capture to analysis, Gigamon Hawk and Ocient customers can dramatically reduce time-to-market for new and innovative workloads. Together, Gigamon and Ocient enable customers to:

- **Realize super-scale network visibility** for performance monitoring, threat hunting, malware attacks, and lawful interception across physical and virtual environments
- **Simplify the generation of network metadata**, remove the traditional complexities of managing extract/load/transform (ELT), and execute low-latency queries in interactive time
- **Leverage standard SQL for flexible ad hoc queries** and dynamic schema changes
- **Increase the volume of data transformed, stored and analyzed** while tackling previously infeasible workloads and use cases

For customers looking to save on operational costs and deploy quickly, Ocient's team of highly experienced data engineers and solutions architects can work with Gigamon-Ocient customers to design a schema and index, craft SQL queries and deploy cost-effective data analytics solutions on-prem, in the OcientCloud or in the public cloud. This pilot-to-production service saves Gigamon-Ocient customers precious months in development and engineering resources while drastically reducing operational overhead to get the solution up and running.

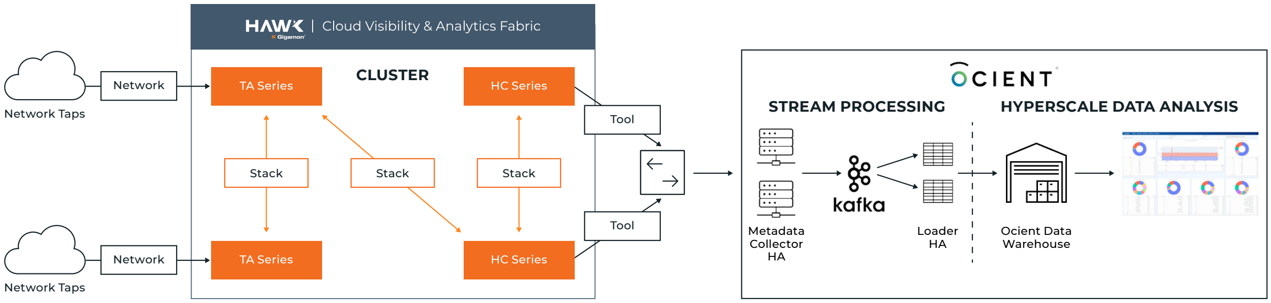


Figure 1. Gigamon Hawk and Ocient together

Together, Gigamon and Ocient provide a powerful combination that enables super-scale visibility, analytics, and threat detection.

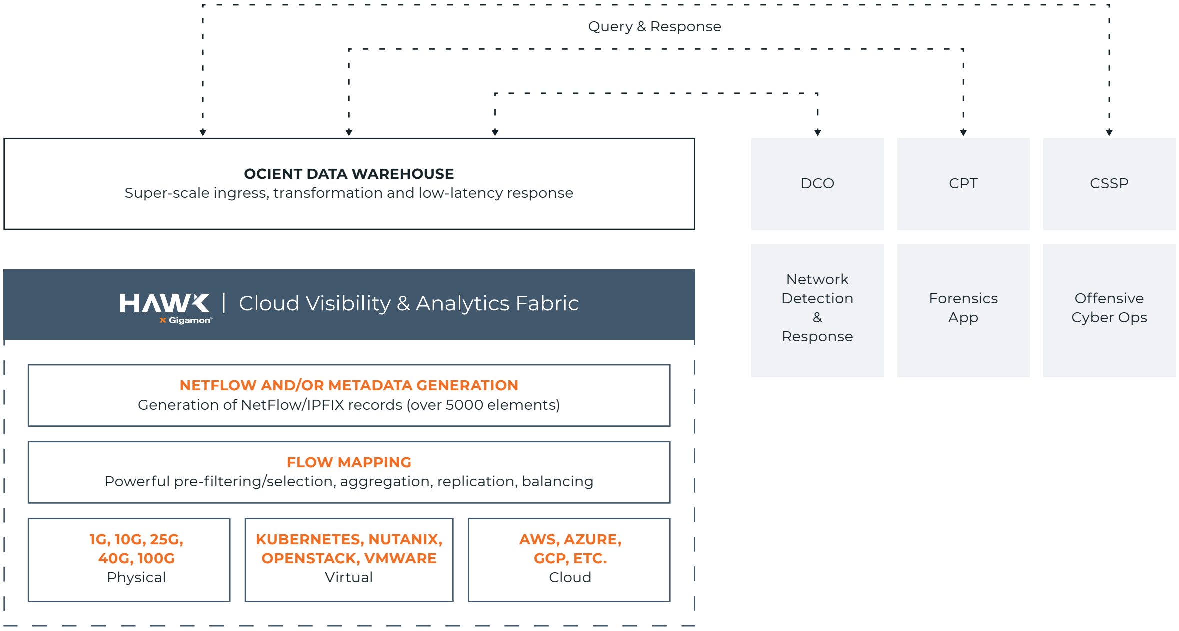

Query & Response
OCIENT DATA WAREHOUSE
Super-scale ingress, transformation and low-latency response
DCO
CPT
CSSP
Network Detection & Response
Forensics App
Offensive Cyber Ops
HAWK × Gigamon | Cloud Visibility & Analytics Fabric
NETFLOW AND/OR METADATA GENERATION
Generation of NetFlow/IPFIX records (over 5000 elements)
FLOW MAPPING
Powerful pre-filtering/selection, aggregation, replication, balancing
1G, 10G, 25G, 40G, 100G
Physical
KUBERNETES, NUTANIX, OPENSTACK, VMWARE
Virtual
AWS, AZURE, GCP, ETC.
Cloud

Figure 2. Gigamon–Ocient representative reference architecture

For more information on Gigamon and Ocient, visit: gigamon.com and ocient.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com