Solution Overview

The volume of data is exploding and outpacing existing analysis tools. Together Ocient, and Cubro address the issue of large scale data retention for Lawful Intercept applications.

Components

- Omnia120 Advanced Network Packet Broker
- NetFlow Optimizer
- Ocient Data Warehouse

Benefits

- 1:1 Netflow generation on dedicated hardware
- DPI-enhanced IPFIX identifies protocols and applications
- Aggregate flow records to significantly reduce the volume of data exported and stored without losing data accuracy
- Enrich flow data with geolocation information, host names, VM names, user identity, and threat intelligence
- Hyperscale data storage; trillions of records / multiple petabytes of data and trillions of records
- Using ANSI SQL, Ocient can provide 10x-50x faster query analysis than other solutions with 1/5 the storage footprint of copy-based systems

Unrivaled large scale Lawful Intercept applications

Introduction

The volume of structured data is exploding and outpacing the ability of existing analysis tools to rapidly capture, store and perform effective analysis. To adapt, many organizations either down sample data, losing fidelity, or spend significant time (sometimes days) waiting for query results and losing efficiency. Others dump their data into an HDFS to deal with later (at a higher cost) or simply dispose of data they are unable to properly manage.

For enterprise businesses and government institutions who want to leverage full resolution datasets, consolidate data silos, find needle-in-the-haystack insights in interactive time, innovate and gain a competitive advantage from previously under-utilized data, Ocient, leveraging rich network data created by Cubro, enables rapid transformation and analysis of hyperscale datasets in “interactive time” – seconds not hours – via accelerated solutions that deliver a lower total cost of ownership (TCO).

The Challenge

The volume and availability of structured and semi-structured data has outpaced the ability of today’s solutions to quickly explore and analyze fast-moving data to deliver mission-critical insights at scale. Ocient offers an unparalleled ability to deliver fast, accurate and detailed network monitoring and analytic capabilities on trillions of data records and multi-petabyte scale.

With enterprise networks generating billions of metadata records per day, Ocient’s data warehouse and analytics platform can transform, ingest, and store format agnostic metadata at 100% resolution with a flexible SQL engine that returns complex query results in interactive time (seconds versus days). The efficiency and simplicity of Ocient’s novel data warehouse architecture places compute adjacent to storage on NVMe SSDs to rapidly accelerate data query and analytics. As a result, Ocient’s highly parallelized system is the most cost-effective, high-performance solution for hyperscale network metadata analysis.

Joint Solution

Cubro provides the tapping, aggregation, and flow generation layer by obtaining an out-of-band, packet for packet copy of the network traffic to generate one-to-one IPFIX records based on individual sessions. These records contain all information traditionally found in NetFlow as well as protocol and application detection from Cubro's Deep Packet Inspection engine. This data is then forwarded to NetFlow Optimizer for further processing and data enrichment.

NetFlow Optimizer (NFO) uses patented streaming technology to aggregate flow records from multiple sources, such as virtual or physical network devices and public cloud flow logs, eliminating redundant data. Simultaneously, the data is augmented with valuable information, including GeoIP data, domain names, VM names, user identity, and threat detection, adding further layers of data enrichment. The output is also standardized to JSON format for forwarding to the Ocient Data Warehouse.

Ocient deploys the data transformation and analytics engine from ingest (ETL) to insights, enabling rapid analytics on 5x-10x more data for higher fidelity insights on trillions of records. The foundation for intelligent analysis, correlation, and forensic applications, Ocient enables complex queries within seconds of ingest and can scale without limits to provide longer retention or "lookback windows" on network metadata.

Joint Solution Components

The Cubro Omnia120 Advanced Network Packet Broker

The Omnia120 is an advanced network packet broker designed from the ground up to address the needs of evolving networks and demanding throughput requirements. Omnia provides purpose-built hardware capable of handling network links from 1 Gbps to several 100 Gbps and a feature-set derived from years of experience and engineering. Omnia combines features included in Advanced Network Packet Brokers with high-performance multi-core CPUs to enable numerous network monitoring, security and analytics uses cases and applications, including those from partners and the open-source community.

Cubro NetFlow Optimizer

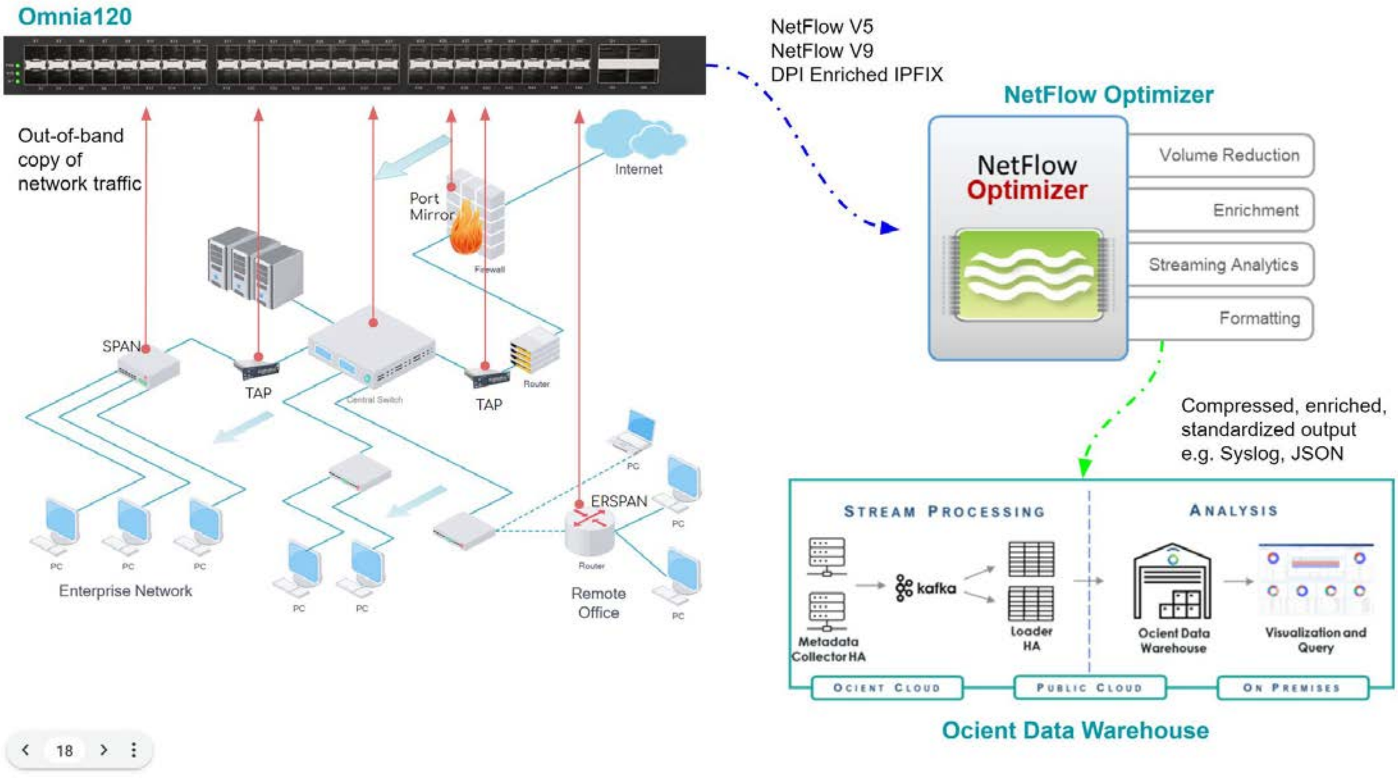
NetFlow Optimizer (NFO) uses patented streaming technology which allows the processing of flow data up to 10 times faster than competitive products. It is complementary to traditional network monitoring and security solutions. NFO provides aggregation of records from multiple flow data sources, converts it into standard Syslog or JSON format, filters to eliminate redundant data and enriches with useful additional information delivering a critical component for complete network visibility.

Ocient Data Warehouse Platform

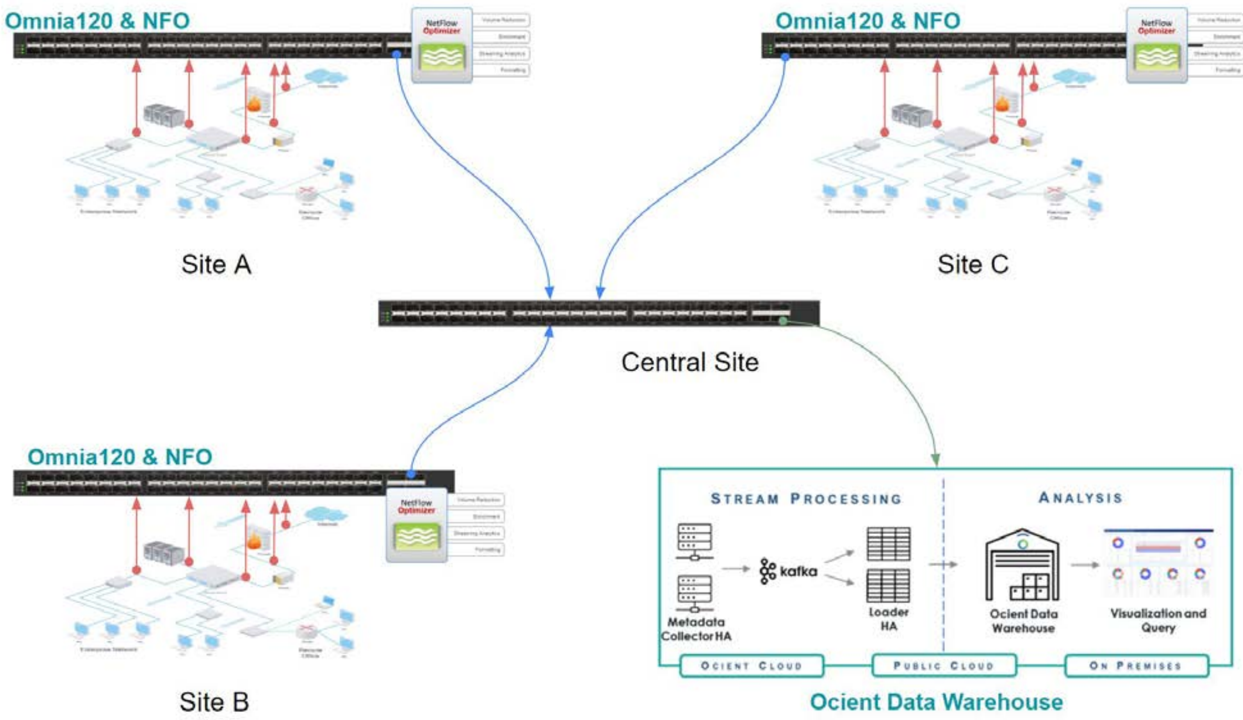
Built to scale to quadrillions of data records, Ocient's Data Warehouse Platform executes complex OLAP-style queries and machine learning on hyperscale data sets 10x-50x faster than other solutions while reducing the storage footprint by 80% when compared to copy-based systems. The speed, simplicity and efficiency of the Ocient Data Warehouse enables customers to transform 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. Ocient's modern technology architecture accelerates the speed by which organizations can process and analyze complex data types across a diverse set of users.

Use Cases

A combination of Cubro TAPs and mirror ports (such as SPAN and ERSPAN feeds) provide a copy of all network traffic to an Omnia120. The Omnia120 generates DPI enriched IPFIX records from all traffic sessions. These records are sent to an instance of NetFlow Optimizer for processing, compression, and further data enrichment. The output is standardized and forwarded to the Ocient Data Warehouse for retention and analysis. Additionally, the Omnia120 can aggregate, filter, and distribute traffic to out-of-band security and monitoring tools (such as an IDS) and NetFlow Optimizer can ingest other structured data, such as public cloud flow logs (AWS/Google VPC Flow logs, Azure NSG Flow logs), for processing and forwarding to the Ocient platform.



As in the example above combination of Cubro TAPs and mirror ports (such as SPAN and ERSPAN feeds) provide a copy of all network traffic to an Omnia120. The Omnia120 generates DPI enriched IPFIX records from all traffic sessions. These records are sent to a local instance of NetFlow Optimizer for processing, aggregation, and further data enrichment. The output is standardized and sent to a remote centralized installation of Ocient Data Warehouse for retention and analysis.



About Ocient

Ocient is a leading hyperscale data analytics solutions company that enables organizations to unlock value from trillions of data records at performance levels and costs previously unattainable. Leading organizations around the world trust Ocient's team of industry experts to design and deploy complex solutions that fast-track new revenue opportunities, streamline operations, and improve security on 5-10x more data while reducing their storage footprint by roughly 80%. Ocient's pilot-to-production solutions are rapidly deployed on-prem or in the cloud with little to no resource-intensive integration. Ocient is a carbon-neutral company, headquartered in Chicago, and backed by leading investors including Greycroft, In-Q-Tel and OCA Ventures. For more information, please visit www.ocient.com.

About Cubro

Cubro is a leading vendor of network visibility solutions that include network TAPs, Advanced Network Packet Brokers, Bypass Switches and Network Probes, for Service Providers and private and public sector Enterprises worldwide. Our solutions improve security posture while reducing costs by increasing the effectiveness and lifecycle of network security devices, improving business continuity, and reducing the total cost of ownership (TCO) while increasing the ROI of network security. Cubro's products remove network blind-spots to ensure all relevant network traffic is available for security analysis, filter out unnecessary network traffic for analysis, and provide high-availability capabilities for security solutions. For more information, please visit www.cubro.com.

Cubro Network Visibility
Ghegastraße 3
1030 Vienna, Austria

Tel.: +43 1 29826660
Fax: +43 1 2982666399
Email: support@cubro.com

Cubro Asia Pacific
8, Ubi Road 2 #04-12
Zervex
Singapore 408538

Tel.: +65-97255386
Email: jl@cubro.com

Cubro North America
Cubro Network Visibility Inc.
225 Peachtree Street NE,
Suite 1100, Atlanta, GA, 30303, USA

Email: americas@cubro.com

Cubro Japan
6-7-22, Shinjuku,
Shinjuku,
Tokyo, 160-0022 Japan

Tel: +81(0)50-3708-5839
Email: japan@cubro.com