csg

TOGETHER, YOU WIN.

OSS MEDIATION

RESOURCE DATA COLLECTION FOR OSS EVOLUTION

A WHITE PAPER

INTRODUCTION

In the transition from communication service providers (CSPs) to digital service providers (DSPs), operators are deploying agile, next-generation networks based on network function virtualization (NFV). They are rolling out virtual IMS networks to support services like VoLTE and VoWiFi, virtual Evolved Packet Core (EPC) and virtual network functions like CGSNs and SCEFs to support NB-IoT rollouts.

Such virtual networks create new challenges for the OSS ecosystem and particularly for service assurance functions like fault management and performance management.

Consequently, operators are transforming service assurance in order to increase automation in operations, provide a clearer view of services (across domains and topologies) and reduce the time to restore services (by determining root causes more quickly).

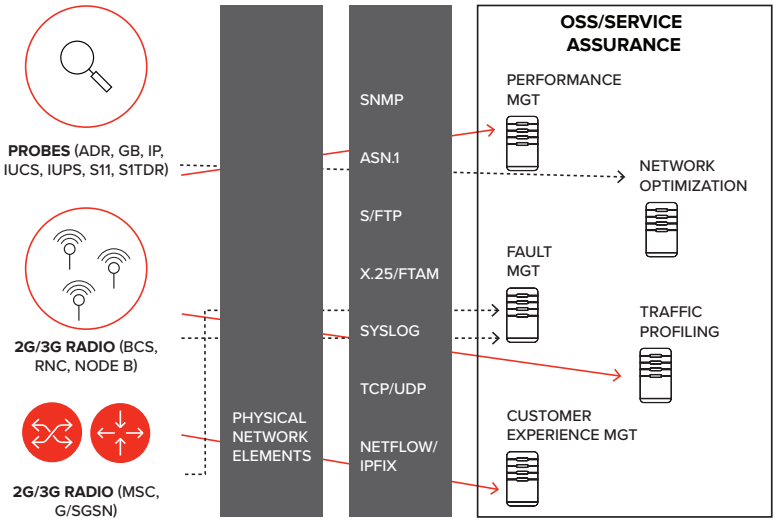
And in this transformation, they are deploying a common resource data collection layer to provide a single source of network data to service the needs of all data consumers across networks/engineering, OSS, analytics and business functions. This approach simplifies the integration with the network, which reduces integration and operations costs and improves time-to-market, while reducing the load of OSS polling on network functions.

ROLE OF NETWORK DATA ORCHESTRATION

CHALLENGES OF LEGACY OSS

Today's legacy OSS architectures involve tightly coupled interfaces between network elements and OSS applications. Network functions are mostly physical network elements (e.g., 3/4/5G radio and core) and have limited separation of software and underlying hardware. Each service assurance application is directly integrated to the network elements.

Figure 1
Current OSS architectures



There are several challenges with this architecture:

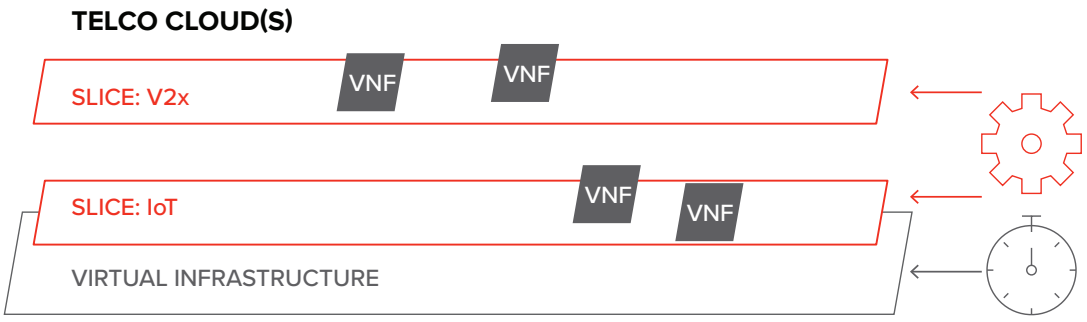
- **Replicated network interfaces:** there are replicated OSS functions for each function/domain, often due to rollouts of new OSS stacks for new network evolutions (e.g., different fault management systems for 3G and 4G). In many cases, this adds complexity due to legacy interfaces from mergers and acquisitions. This results in many direct interfaces between network elements and OSS
- **Many interface protocols:** equipment vendor implementations of standards-based interfaces vary, resulting in complex multi-vendor network integration
- **Excessive network load:** due to point-to-point OSS integration
- **Costs for interface evolutions:** the cost and time of managing change (switch build upgrades, changing KPI definitions, etc.) is high
- **Limited view of services:** it is difficult to manage an end-to-end service for customers and determining quality of experience is challenging
- **Response to alarms is simple, siloed and slow:** often relating to a single network element rather than end-to-end service

NEXT-GENERATION OSS FOR NFV

Operators around the world are fast deploying NFV for new services such as 5G and VoWiFi, into the Evolved Packet Core and into the radio network. This will continue with deployments of NB-IoT and 5G.

The principal concepts of 5G are based on NFV to enable network slicing, including the dynamic instantiation and management of network services. The goals are for virtual network functions (VNFs in the diagram on the next page) to support auto-scaling (up/down, in/out) and auto-healing, with minimal manual intervention and “assisted operations.” A further goal of 5G telco clouds is tenancy and offering NFV-as-a-Service to other operator customers, in addition to enterprise and retail customers.

Figure 2
5G Network Slices



Next-generation service assurance aims to increase the automation in operations, have a clearer view of services (via cross-domain and topology correlation), and reduce the time to restore services (by determining root causes more quickly). A further goal is a single source of network data, which can be made available immediately to internal and external users.

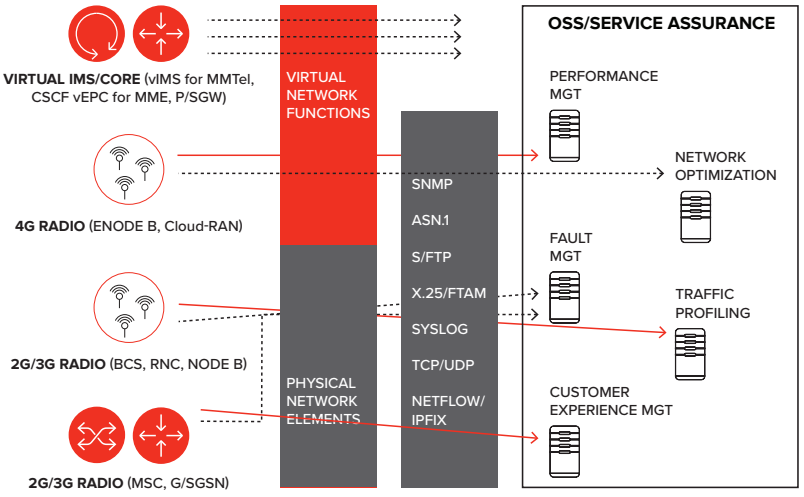
Within NFV networks, it is necessary to understand the interactions of each element in the NFV management and orchestration (MANO) stack in managing faults and performance. This means collecting network data from a wide range of NFV functions, such as NFV orchestrators (NFVOs), VNF managers and virtual infrastructure managers (VIMs).

CHALLENGES OF NFV AND LEGACY NETWORKS

In addition to enabling virtual network functions that are dynamically instantiated and auto-scale, next-generation service assurance must support legacy networks and OSS systems that will not be decommissioned for many years. OSS needs integration with physical, virtual and hybrid networks.

From a network data collection perspective, not only is there a gap for integrating new virtual networks into OSS applications, but challenges to overcome in overall OSS transformation. These challenges include minimizing the replicated collection of network data from overlapping OSS applications, providing a single, common view of network service data, and reducing the load on network resources (only polling network elements and functions once for each dataset).

Figure 3
Data Collection from Physical, Virtual and Hybrid Networks



NETWORK DATA ORCHESTRATION

To address these challenges, operators are deploying a common network data orchestration layer for resource collection and mediation of network data. It is a single data collection layer to service the needs of all data consumers across networks/engineering, OSS, analytics and business functions.

This Network Data Orchestration function is being deployed to integrate a wide range of data sources and deployment architectures, including virtual **resource collection functions** that run in the network fabric on the network function virtualization infrastructure (NFVI).

Network Data Orchestration performs remote and centralized data collection via a wide range of network protocols, from real-time data feeds like SNMP, Syslog/UDP and Kafka, to batch data processing (e.g. from element management systems for 3/4/5G Radio).

At a macro level, data sources can include usage from traditional IT cloud infrastructure and NFVI/telco clouds, backhaul and transmission networks (optical, IP and Metro Ethernet), radio access and core networks and fixed access networks.

In supporting a scalable and fault-tolerant data processing for OSS, the Network Data Orchestration solution facilitates data brokerage between the different layers of a Lambda architecture.

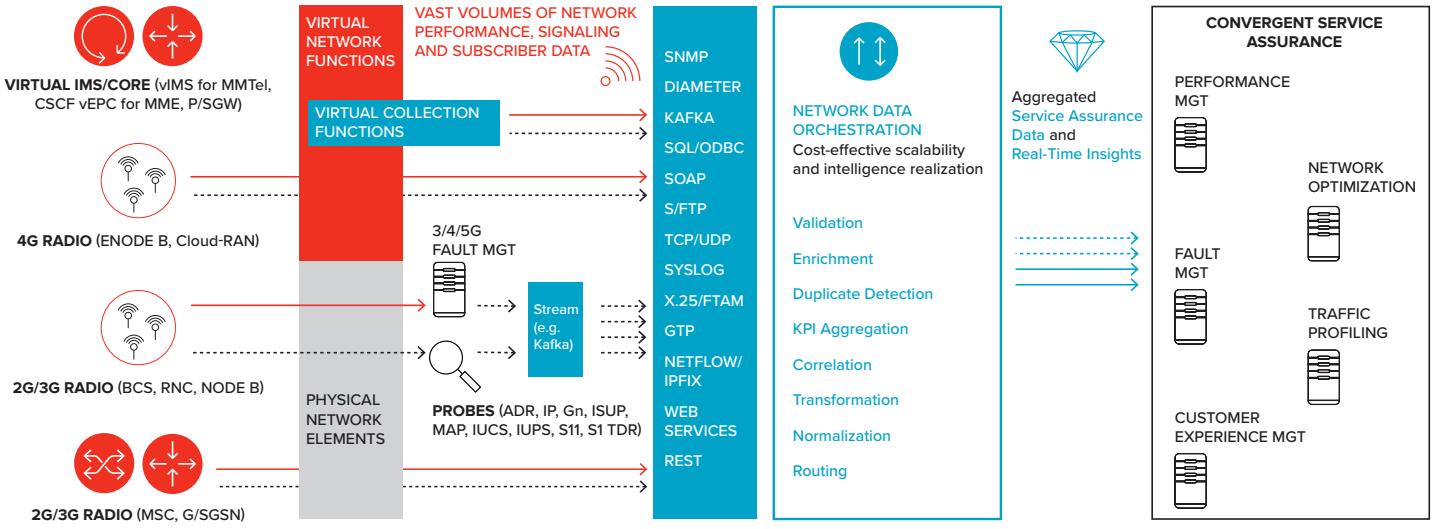


Figure 4
Role of Network Data Orchestration

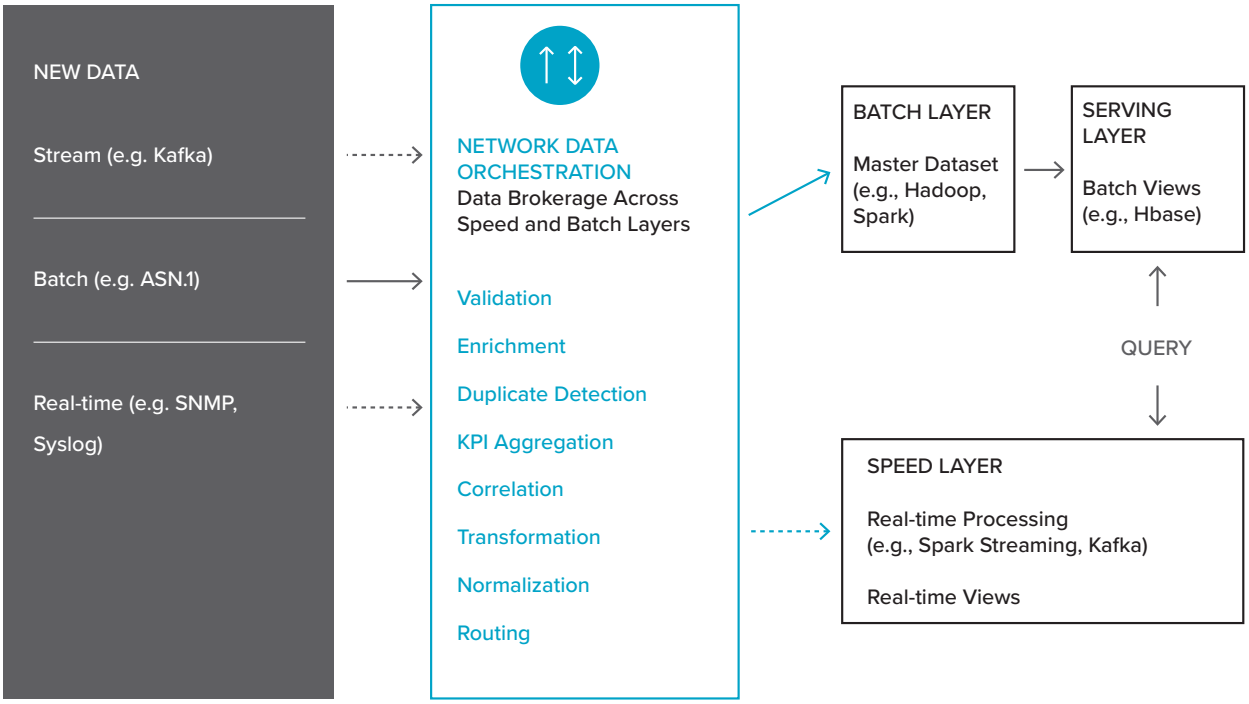


Figure 5
Network Data Orchestration enables brokering across layers of Lambda Architecture

As illustrated above, Network Data Orchestration provides both "fast data" and "slow data" processing streams. It sends immediate insights to the Speed Layer for real-time processing, for example, via Kafka or to Spark Streaming, while completing batch operations (like correlation) to provide more complete data to the Batch Layer which manages the immutable master dataset and pre-computed views (e.g. Hadoop, Spark).

BENEFITS OF NETWORK DATA ORCHESTRATION

Operators are standardizing on a single, enterprise-wide platform for network data collection and mediation to realize various benefits, which include:

- A single funnel of user data to OSS systems; no doubt where to go for data
- Deliver significant cost savings and operational efficiencies
- Service velocity; faster time to market
- Enable network and OSS evolution
- Simplified service assurance
- Eliminate costs and dependencies on multiple vendors
- Workforce productivity improvement; fewer systems to learn and operate

RESOURCE DATA COLLECTION SOLUTION

CSG Security Data Orchestrator meets all the requirements for OSS resource data collection (RDC).

CSG NETWORK SECURITY DATA ORCHESTRATOR OVERVIEW

CSG Security Data Orchestrator enables you to streamline the handling of network event, alert and log information and strengthen your network operations. The solution helps ingest, filter, cleanse, and correlate massive amounts of data at machine speed. Security Data Orchestrator easily handles the tasks of high-volume data normalization and transmission to the monitoring layer, thereby reducing the impact on large existing investments (see figure below). The result? Greatly improved harmonization and performance from network monitoring—and significantly reduced storage costs and bandwidth utilization.

Security Data Orchestrator allow you to support both "fast data" and "slow data" processing streams to meet the different requirements of OSS applications for real-time insights and more complete data aggregated over time via batch. The platform is deployed to support analytics and visualization solutions such as CSG Digital Mediation Insights.

The solution provides access to an extensive library of pre-existing collection and transfer protocols and file and record format definitions. Consequently, the solution easily adapts to accommodate both standard and non-standard data formats and transmission methods/protocols, ensuring any variation in the format and transmit protocol of inbound data is never an issue for collection.

Security Data Orchestrator is comprised of two main components: Security Data Orchestrator Collector and Security Data Orchestrator Aggregator.

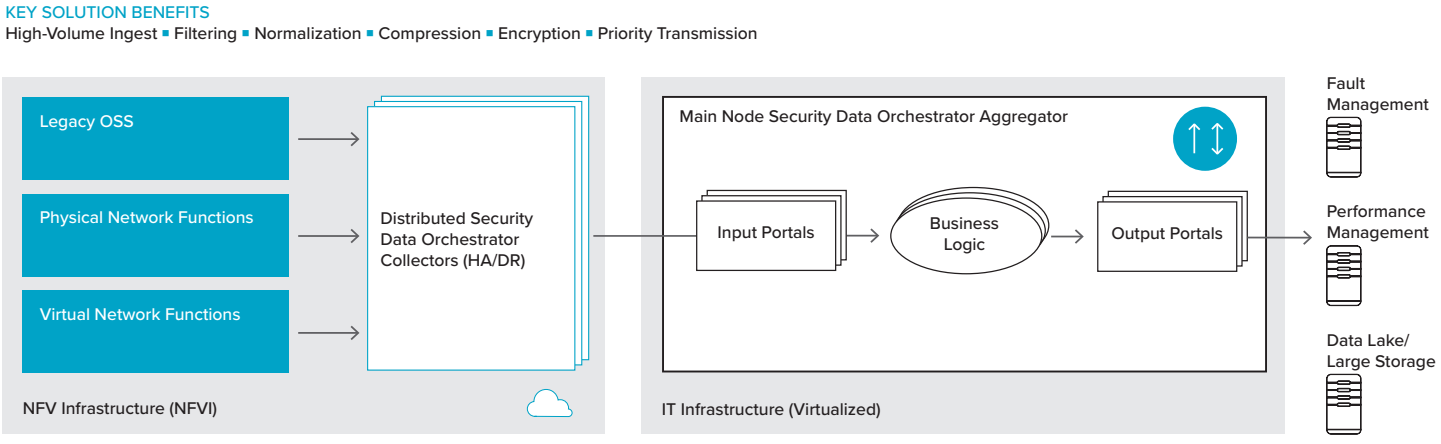


Figure 6
CSG Security Data Orchestrator components

THE COLLECTORS

The Security Data Orchestrator Collector software is co-located with the data sources in a distributed enterprise network to capture event and log data from disparate technologies. By introducing single points of collection from network sources, this eliminates the need for the network sources to support multiple system connections and reduces usage of network bandwidth. The Collector can be configured to automatically filter unwanted data records; enrich useful records; resolve and augment records with local origin information; and apply priority designations to the records. The enriched records are then transmitted to one of more defined destinations in priority order.

- Transmission options permit different (or the same) subsets of the records to be transmitted to each destination, on different schedules, with data packaging optimized for the destination
- Data records are safely stored on the Collector until they have been delivered to all configured destinations
- The Collector performs encryption and compression prior to transmission to the destination, ensuring the security of the data and minimizing the amount of data being transmitted

Device connectors are software modules residing in the Security Data Orchestrator Collectors that interface to the devices where data is sourced. The Connectors transfer the data and monitor all data acquisition processes, register the data files with the data management subsystem and automatically restart any failed input sessions, when possible.

The device connectors also connect to the systems receiving data distribution. Custom connectors can be created for new devices or proprietary data formats.

THE AGGREGATOR

The Security Data Orchestrator Aggregator is a carrier-grade software application designed to reliably and efficiently ingest large volumes of data, typically from a distributed network of Security Data Orchestrator Collectors. The Aggregator performs advanced data operations, to complement the initial Collector processing, including correlation of records across multiple record streams, further elimination of unwanted records, detection and elimination of duplicate event reports, and enrichment of the data with enterprise information such as:

- User credentials
- Event success/failure
- Usage
- IP geospatial information
- QoS

Higher levels of error checking can be configured for the data at this time, along with other data normalization, for example:

- Upper/lower case normalization
- Date/time stamp normalization
- Identifier normalization, e.g. MSISDN, IP address, IMSI, etc.

Data deemed to be in error may be sidelined within the Aggregator for inspection by skilled data flow analysts. The Aggregator solution permits such data to be recovered and corrected in bulk.

SUPPORT FOR RESOURCE DATA COLLECTION REQUIREMENTS

The table below outlines how the CSG solution supports the high level requirements for RDC:

REQUIREMENT	KEY CAPACITY
Near real-time messaging from network elements, OSS systems and service platforms	→ Security Data Orchestrator provides a huge library of plug-in Connectors for collecting data from source systems. This includes real-time and streaming protocols such as SNMP, log monitoring, Netflow/IPFIX and Kafka, besides proprietary equipment vendor application protocols
Streaming telemetry via Kafka to OSS applications (FM, PM, SQM and relevant dashboards)	→ Security Data Orchestrator provides plug-in Kafka Consumer and Publisher Connectors. It scales cost-effectively and has been benchmarked to support half a billion messages a day per core and 4MB RAM
Possibilities to utilize open source-based solutions in OSS space	→ Security Data Orchestrator integrates seamlessly with many open source tools to deliver OSS solutions, including with big data frameworks such as Hadoop and Spark, and to NoSQL databases like Couchbase
Storage for common data outside RDC (dimensioning currently several terabytes-petabytes)	→ Security Data Orchestrator optimizes the storage of huge data volumes using aggregation and compression algorithms and formats to reduce space by up to 95 percent
Long-term history data forward to data lake	→ Security Data Orchestrator has unique tools to optimize the ingest of data to data lakes, like the use of its PTP plug-in. The Parallel Transport and Post-Transfer plug-in eliminates the latency associated with HDFS ingest processing scripts, automates the management of restart jobs and load balancing ingest failures. It has also been proven faster than open source tools like Flume
Measurement data handling	→ Security Data Orchestrator has been deployed in a hub and spoke architecture, with remote virtual collection functions and aggregation to ingest raw network data from a huge range of sources, and deliver both aggregated management information and real-time insights to service assurance tools

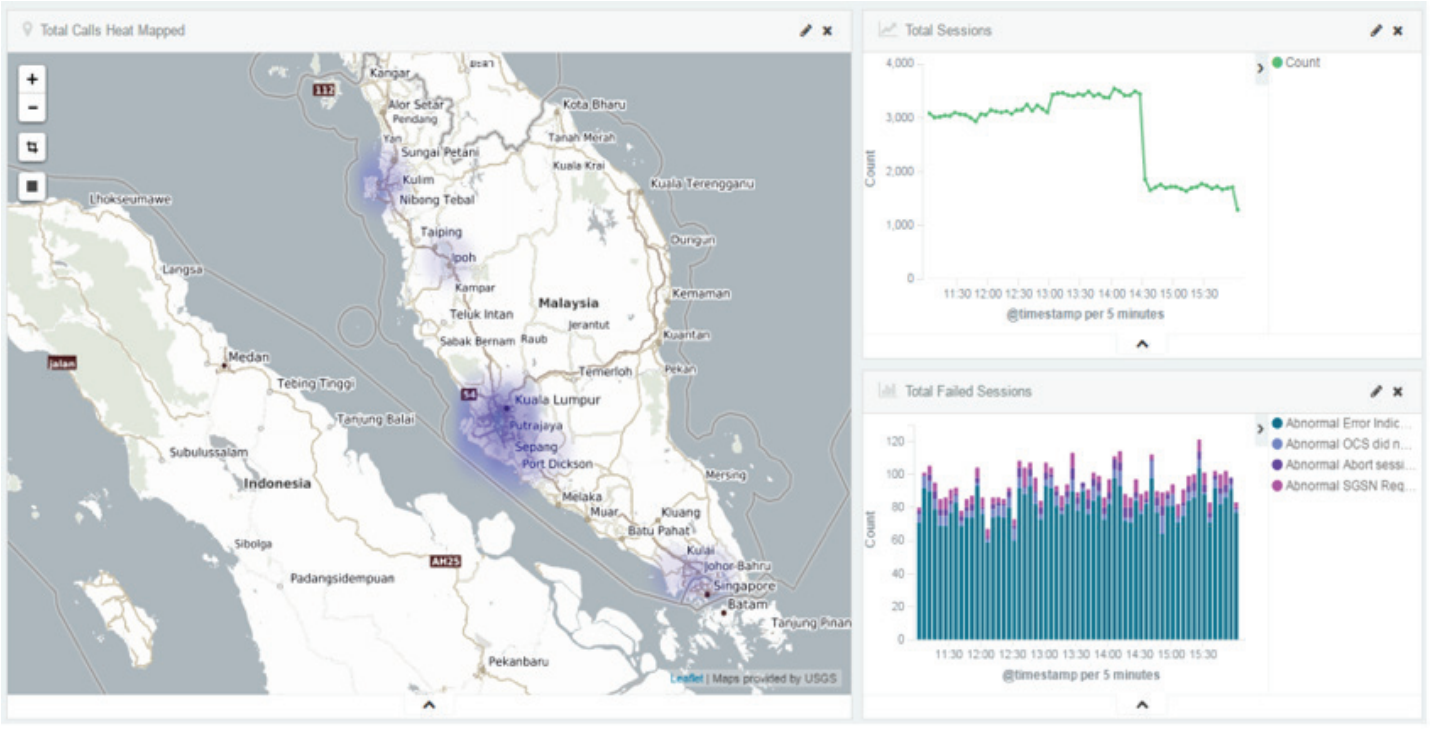
DIGITAL MEDIATION INSIGHTS

The Digital Mediation Insights solution seamlessly integrates with CSG Security Data Orchestrator, enabling service providers to collect, transform and visualize data from any source in real-time. The resulting analytical dashboards enable operators to gain insights and make proactive decisions much quicker in comparison to the traditional large data warehouse (DWH) platforms that are typically used to drive business intelligence.

Dashboards can be quickly created and populated with real-time data, rather than having to wait days or weeks for a large DWH to be queried and reports generated. With Digital Mediation Insights, it is possible to bring new data sources online, process, store and analyze them extremely quickly and cost effectively, ensuring the CSP has access to timely information and insights that enable them to be proactive, maintain competitive advantage and enhance customer satisfaction.

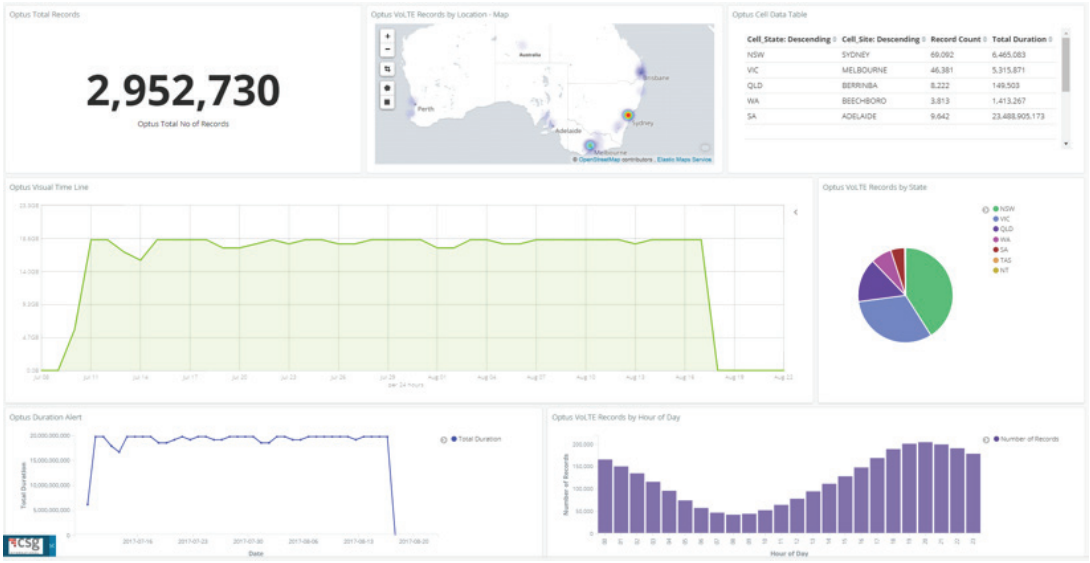
The flexibility of the solution enables it to be used across the business for many different use cases, some examples of which are shown below and on the next page. For more information, please refer to the Digital Mediation Insights Solution Spotlight.

TRAFFIC ANALYSIS (E.G., DROPPED CALLS/SESSIONS BY CELL SITE)



REAL-TIME TRAFFIC DETECTION

NETWORK PERFORMANCE OPTIMIZATION (E.G., VOLTE OPS DASHBOARD)



CONCLUSION

Next-generation OSS and service assurance is critical for CSPs' digital transformations and the deployment of NFV. Resource data collection is a foundation for providing a single layer of harmonized data to all OSS management functions.

CSG Security Data Orchestrator technology is proven and delivers unique capabilities for data collection scalability and flexibility. Talk to CSG today and learn how you can increase automation in operations and simplify network integration with CSG Security Data Orchestrator.

ABOUT CSG

For more than 35 years, CSG has simplified the complexity of business, delivering innovative customer engagement solutions that help companies acquire, monetize, engage and retain customers. Operating across more than 120 countries worldwide, CSG manages billions of critical customer interactions annually, and its award-winning suite of software and services allow companies across dozens of industries to tackle their biggest business challenges and thrive in an ever-changing marketplace. CSG is the trusted partner for driving digital innovation for hundreds of leading global brands, including AT&T, Charter Communications, Comcast, DISH, Eastlink, Formula One, Maximus, MTN and Telstra. To learn more, visit our website at csgi.com and connect with us on LinkedIn and Twitter.