Solution Brief

Cloud-native Service Assurance
# Contents

Cloud-Native Service Assurance.......................................................................................................................... 1
Executive Summary.................................................................................................................................................... 3
Challenges in Service Assurance .......................................................................................................................... 3
Reimagining End-to-End Service Assurance ......................................................................................................... 4
Symops Service Assurance...................................................................................................................................... 5
  Fault Management.............................................................................................................................................. 5
  Performance Management................................................................................................................................ 6
  Configuration Management................................................................................................................................. 6
Symworld Platform: A Strategic Foundation for Intelligent Operations........................................................................... 6
Observability at the Core......................................................................................................................................... 7
Observability Framework........................................................................................................................................ 7
Key Differentiators................................................................................................................................................ 9
  Out-of-the-Box Observability Framework........................................................................................................ 9
  Bridging IT observability and Telco domain ....................................................................................................... 9
  Modern Architecture....................................................................................................................................... 9
  Proven at Scale and Future-Proof...................................................................................................................... 9
  Fast, Flexible Deployment............................................................................................................................... 9
  Rapid Integration............................................................................................................................................ 9
  Beyond day 1 operations............................................................................................................................... 10
  Partnership Delivery Model............................................................................................................................ 10
Conclusion........................................................................................................................................................... 10
Executive Summary

Service Assurance is the part of telecom operations dedicated to ensuring the network delivers to the required service levels. Faults on the network, or problems reported with services, must be identified, diagnosed, and resolved as quickly and effectively as possible.

The knowledge required to understand networks and any operator’s specific network means that Service Assurance is a highly-skilled and costly function. In addition, the typical working environment – of a live Network Operations Center (NOC) – is high-pressure, requiring constant vigilance and responsiveness.

The service infrastructures of Communication Service Providers (CSPs) are becoming increasingly complex, and reactive monitoring is not enough to resolve issues because of application failures. Cloud-native computing has accelerated the adoption of micro-services architecture, and future software must be agile, resilient, disaggregated, and language and technology agnostic. The Symops suite of products Fault Monitor (FM), Performance Monitor (PM), and Configuration Manager (CM) delivered with service assurance are designed with a micro-service architecture that allows the CSPs to move forward confidently.

Cloud-based networks are disaggregated and distributed in nature and networks have a higher number of interconnected parts, so the number and types of failures that can occur are higher. In a distributed environment, understanding a current problem is an enormous challenge, primarily because it produces more “unknown unknowns” than simpler systems. Furthermore, growing traffic and introducing advanced monitoring techniques urgently need to process large amounts of data in near real-time poses an enormous challenge. With many operators often still working in silos, using different tools to monitor network health, which leads to disconnected networks and redundant data with even a single issue, is creating multiple network problems.

After manually filtering and correlating this influx of outage data and when operators eventually understand the cause of the service issue, they often cannot establish an automated solution to remediate it. This further causes lengthy service outages and escalates the costs, increasing competitive and financial damage.

Cloud-based technologies are agile, necessitating agile architecture and processes for software to stay relevant and in tune with time, adopting the best in technology and practice.

Automated, end-to-end Service Assurance has become critical for CSPs seeking to improve their quality of service and experience and drive down operating expenses.

A new approach is required in the era of cloud, 5G, and dynamic on-demand services. We must integrate and utilize software-centric micro-services and fully adopt cloud-native architecture. This must be combined with data & analytics-based analysis for better capacity planning and AI/ML-based models to detect issues and fix them before they even happen.

Challenges in Service Assurance

Networks and services are only becoming more complex. Cloud-based networks, 5G, and Open RAN drive a new real-time performance requirement for Service Assurance that cannot be met by existing solutions which rely on network polling and averaged non-real-time KPI measurement from EMS.

Operators are facing significant obstacles with the current generation of service assurance solutions, such as:

- **Lack of “end-to-end” visibility and cloud specific insights**- With more services being delivered by OTT providers, operators can struggle to identify, diagnose, and size the resources to better address the service-impacting problems – adding to cost and impacting end customer experience.

- **Demand for more real-time responsiveness**- With consumers and businesses even more reliant on connectivity and cloud services, they demand faster response to and resolution of faults.

- **Limited capability to assure cloud and software-based networks**- These change the dynamics and nature of the network and what it means to assure it. Software configurations can be the cause of major outages
The Symphony approach to Service Assurance is built on four foundational elements required for significantly lower cost, more effective, and future-proof end-to-end service assurance:

- **Observability** – visualization and analysis of real-time telemetry from a more complex, software-defined infrastructure.
Intelligent Operations – Cloud-native Service Assurance

- **Automation** – the ability to rapidly create and operationalize automatic analysis and completion of tasks. The use of AI is an integral part of automation.
- **Scalability** – a cloud-native design that scales gracefully as data volume and variety inevitably increases.
- **Cloud Platform** – a common foundation that will support the transition from today’s networks and operations to the more autonomous networks of the future.

The Symphony approach addresses the underlying causes of labor-intensive, and high-cost service assurance. In Service Assurance as it is practiced today, costs are kept high by labor on tasks that could be automated - or eliminated altogether.

**Symops Service Assurance**

Symops Service Assurance offers a new yet proven approach to automated, end-to-end service assurance. It gives operators a way to reduce operations costs today, but also a future-proof solution able to support the journey from today’s 2G/3G/4G mobile networks through to cloud-native networks of 5G SA and beyond.

Developed together to support modern networks and an automation-first objective, this solution provides:

- “Single Pane of Glass” visibility
- End-to-end view of network and services
- Scalability – due to engineering as cloud-native applications
- Deployment on any public or private cloud
- Fast, incremental deployment with DevOps

The automated, end-to-end service assurance solution includes the standard capabilities that operators would expect but with flexibility and scale to give CSPs a solution that will help them overcome their challenges and reduce costs.

**Fault Management**

- **Real-time network visualization** provides real-time network visibility and continuous monitoring to identify outages and faults.
- **Rapid access to alarm information** offers real-time tracking and visualization of alarms based on geography and category.
- **Quick issue identification** provides rapid fault identification within a site.
- **Displays and tracks alarms efficiently**, allowing users with the complete status of alarms, comprehensive alarm monitoring, alarm library, and a list of discarded alarms.
Intelligent Operations – Cloud-native Service Assurance

- **Rapidly detect faults and outages**, providing fast correlation and resolution by locating the sources of complex network problems and speeding up their repair.
- **Improves Quality of Experience (QoE)** through outage detection that eliminates avoidable alarms and prioritizes high-impact faults.
- **Real-time alarm tracking** facilitates users to track alarms in real-time, which reduces maintenance costs and helps to gain real-time insights.

### Performance Management

- **Unified Monitoring Solution** allows businesses to collect, process, store, and analyze data from multiple sources and create performance dashboards.
- **Generic KPIs** facilitate the grouping of multiple vendor KPIs of the same domain and technology to display comprehensive performance.
- **Anomaly Detection** provides an automatic diagnosis of the performance and availability problems across the technology stack.
- **Root-cause Analysis** facilitates the creation of closed-loop automation of various performance related issues in the network.
- **Data Integrity** provides adaptive network traffic analysis by providing real-time insights into network performance.
- **Performance Threshold Correlation** allows users to define corresponding threshold correlation rules for daily and weekly busy hour calculations.
- **Customizable Dashboards** provide users with the ability to create dashboards using predefined widgets to get an at-a-glance network view.

### Configuration Management

- **Configuration Manager Dashboard** provides an analytical view of the non-compliant golden parameters, which shows detailed information through different widgets and at different geographic levels.
- **Network Tree** provides a hierarchical representation of network devices with configuration parameters to track changes.
- **e-SON** supports the self-optimization of the radio network via the SON algorithm and performs the required configuration change suggested by the algorithm.
- **Parameter Library** for central hosting and managing parameters for all devices for different software versions, which acts as a central repository to perform various configuration management tasks.
- **Impact Change** provides insights into the number of gains and losses realized within the network related to the changes implemented through CM.
- **Audit Templates** provide a central repository where the templates are saved. The templates facilitate the user to conduct an audit; based on that, Configuration Manager dashboards are generated. It enables users to create and manage audit templates to define baseline parameters and perform device configuration checks to detect violations.
- **Audit Report** generates network audits, allowing the operators to understand the status of their networks and take appropriate actions to fix faults.
- **Planned Event** allows users to implement day two-parameter change in the network as part of the change management workflow.
- **Query Builder** allows users to implement user-defined criteria to search and filter the specific configuration parameter objects value on network devices and view results.

### Symworld Platform: A Strategic Foundation for Intelligent Operations

The Symworld Platform is explicitly designed for the telecom industry delivering cloud-native microservices across many different applications, such as databases, analytics, workflow, and automation. This reduces costs by removing duplicated technologies across the service assurance estate (such as expensive third-party database licenses).
By deploying the end-to-end Service Assurance solution, operators put in place the foundational capabilities that support other initiatives targeting intelligent, automated, and autonomous operations.

**Observability at the Core**

Key to the new approach is the use of an observability framework at the heart of the solution.

Symops Observability Framework is a carrier-grade platform that enables end-to-end visibility into the fault, log, performance, and traces for Applications, Network Functions, Network Elements, Clusters, and Bare-Metal Systems. It further contributes to the effective deduction, improved mean-time to repair, proactive monitoring and building of closed-loop scenarios.

It is an integrated framework created using curated open-source software (Kafka, OpenSearch, Spark, Prometheus, etc.), which is quality-assured, scale-tested, and packaged for cloud-native deployments. It helps to monitor and troubleshoot issues to meet customer experience demands and business requirements effectively.

**Observability Framework**

The service infrastructures of Telco companies are becoming increasingly complex. Reactive monitoring is not enough for resolving issues because of application failures, software is no longer monolithic and is advancing to cloud architectures. Operators are migrating their network to the cloud in multitudes to reduce the amount of infrastructure they must create and maintain. The benefits of using the cloud over traditional server-based infrastructures and computing capabilities are innumerable. However, in a cloud-native environment, due to diversified services across multiple containers, and monitoring service-specific and system-level metrics, traditional systems cannot ingest the metrics on a large scale. In addition, cloud infrastructure enables new data streams (events, logs, traces, application metrics) for enhanced observability. Consuming these varied set of data across vendors and devices in real-time, processing, deriving, and correlating observations across the data streams and network layers to provide relevant and quick insights, and next best action is essential.

Cloud-based networks are disaggregated and distributed in nature and such networks have a higher number of interconnected parts, so the number and types of failures that can occur are higher, too. In a distributed environment, understanding a current problem is an enormous challenge, largely because it produces more “unknown unknowns” than simpler systems. Also, the cloud-native platform causes proactive perceptiveness, which allows businesses to spot potential flaws or breakdowns before they become a disaster. Particularly when microservices or containerized applications are involved, cloud environments create significantly more telemetry data. The rapidity with which they generate this data makes it much more difficult to keep up with the flow of data, let alone effectively understand it in time to resolve a performance issue. To manage these situations, manual monitoring is insufficient.

With today’s complex service architectures, legacy systems face many challenges:

- **Lack of Visibility:** Businesses are not able to provide continuous monitoring of application and service instances’ dynamic behaviour. Due to their transient and dynamic nature, monitoring cloud systems without adequate change detection and modern technologies are unmanageable and challenging. The difficulty is to balance granular functionalities that provide impressive performance without becoming unmanageable in the long run, leading to a lack of visibility.
- **Inept Traditional Monitoring Approach:** It is impossible to get real-time metrics from every key component of a system without a good framework, especially when those components include thousands of microservices running on numerous physical servers across multiple clouds. However, the bigger problem with more obsolete monitoring models is that they only capture the specific metrics they track. Traditional monitoring systems are not proactive and cannot spot potential flaws or failures before they become a disaster.
- **Penalties of Deferred Observability:** Without a detailed understanding of potential performance bottlenecks or failure scenarios, it is hard to forecast production system behaviour. When failures occur, the cause and effects of alternative solutions are unknown. Usually, teams attempt to guess the primary cause of problems and try making sense of telemetry to come up with solutions. They go from one hypothesis to
the next and one change to the next without fully comprehending the system’s impact wastes time and effort.

The platform extends its support by providing and generating alerts in exceptional and critical scenarios, assisting in both proactive and reactive use-cases. It is an extensible solution that provides log analytics using multiple dashboards and alerting systems. The platform also aims to simplify the process of managing logs and improving the durability and reliability of the system. It extracts actionable insights to boost productivity, improve application performance, and enhance user experience.

Symops Observability Framework augments telecom monitoring management and automation by contextualizing large volumes of operational data. It also provides a comprehensive understanding of the system behaviours that makes it easy for businesses to navigate from problem identification to assisting in resolution within minutes. The overall health can be tracked through monitoring as it builds the context regarding systems, clusters, network functions, and services.

Overall, with end-to-end visibility into the system, cluster, application, and network through performance, faults, logs, and traces collection, the issues can be easily narrowed down to the right pain points. Whether the issue is at the
Application Layer or Network Layer, or between the stack or at functions, such can now be determined with ease through the platform. Symops Cloud Observability does not replace monitoring, it enhances it.

Key Differentiators
In terms of features and functions, Symops Service Assurance provides a comparable capability to traditional assurance vendor solutions. But as a platform capable of supporting operators through the next decade of radical change, Symops Service Assurance is uniquely equipped:

Out-of-the-Box Observability Framework
Access to real-time telemetry is not part of the conventional service assurance offerings, but real-time telemetry is key to achieving faster, more responsive service assurance. The Symphony Observability Framework provides the ability to integrate and process telemetry from any source – cloud-native platform and applications, Infrastructure, legacy Telecom Network Functions, PNFs, Transport elements, and even via vendor EMSs.

By providing an off-the-shelf, ready-made, proven observability framework, the Symphony solution significantly reduces integration costs and effort.

Bridging IT observability and Telco domain
Symphony is unique in having not just an IT cloud perspective but an IT and telco perspective. Many aspects of assurance analytics are common across enterprises. However, the telco is particularly unique in the wide distribution of its network and capabilities.

Modern Architecture
Cloud—native, open-source software and open interface driven architecture from ground-up. Even the UI is micro-frontend framework enabling isolation and rapid development and deployment of features.

Modular architecture and open interfaces make it easier to introduce the solution into a brownfield operation by selectively enabling functions and integrations, and handshake with existing OSS systems to maintain operational continuity.

Proven at Scale and Future-Proof
The Symops Service Assurance solution is already supporting record-breaking levels of automation at the world’s largest, most advanced, cloud-native network: Rakuten Mobile.

With the backing of one of the world’s most successful digital services companies, parent Rakuten, the Symphony solution is being funded in line with its ambition to become the de facto industry standard for a new generation of telecom providers.

Agile architecture and process means the software stays relevant and is in tune with the time, adopting best in technology and practice.

Fast, Flexible Deployment
Symops End-to-End Service Assurance can be deployed and operational in a public cloud environment in as little as two weeks. The deployment process can be incremental, adding in data sources, service models, automation, and analysis incrementally.

Additionally, individual solution components (Performance Management, Fault Manager, and Configuration Manager) can be deployed alongside existing complementary tools, with a gradual cutover/consolidation.

Rapid Integration
Integration framework – that supports cloud native and custom integrations – avoids vendor lock-in and enables faster integrations. API-based handshaking between all other modules in the Rakuten suite, including Kafka real-time integration, provides a standardized integration framework for the integration of Rakuten Symphony components into an existing brownfield.
Beyond day 1 operations
Symworld has been built with a microservices, cloud-native architecture from the beginning utilizing an agile CI/CD delivery approach. This enables Symworld to rapidly deploy new functionality to address new technology, specific CSP or enterprise business context rapidly, rather than waiting for slow waterfall deliveries of products.

Many of the challenges of large-scale OSS system integration projects can be minimized with this CI/CD approach. It prevents the tangled mess of short-term fixes and workarounds that characterize OSS integration, where products with six-monthly waterfall roadmaps, integrated with closed proprietary networks cannot address immediate CSP needs.

Partnership Delivery Model
Drawn from practical experiences, the delivery model for service assurance solution offers rapid, incremental benefits. Symphony knows the challenges that can derail service assurance automation projects; our engagement model identifies clear responsibilities and technical checks to avoid them.

Conclusion
The Symops Service Assurance solution combines the ability to transform existing service assurance operations with equivalent capability to existing solutions, but with a platform for fundamental operational change and large scale automation, AI-led processes ready for the cloud-based network of the future:

- A completely cloud-native architecture that is delivered at a faster pace with a DevOps approach.
- Designed to easily evolve with time, to quickly adopt to the latest and greatest technology and open-source solutions, and de-facto standards in the community.
- Modular architecture and open interfaces make it easier to introduce the solution in brownfield, selectively enabling functions and integrations, handshake with existing OSS systems to maintain operational continuity.
- Modern and state of the art micro-frontend based UI/UX, enabling isolation, and rapid development and deployment of features.
- North-Bound Interface (NBI) and South-Bound Interface (SBI) framework that supports cloud-native and custom integrations, avoids vendor lock-in and enables faster integrations.
- Automated, end-to-end service assurance that includes the standard capabilities that operators expect, enhanced with smart applications for auto-RCA, anomaly detection, and focused use of AI/ML.