

Service Assurance – A Critical Telco Capability

Exploring Next-Gen Challenges and Opportunities

RESEARCH BRIEF

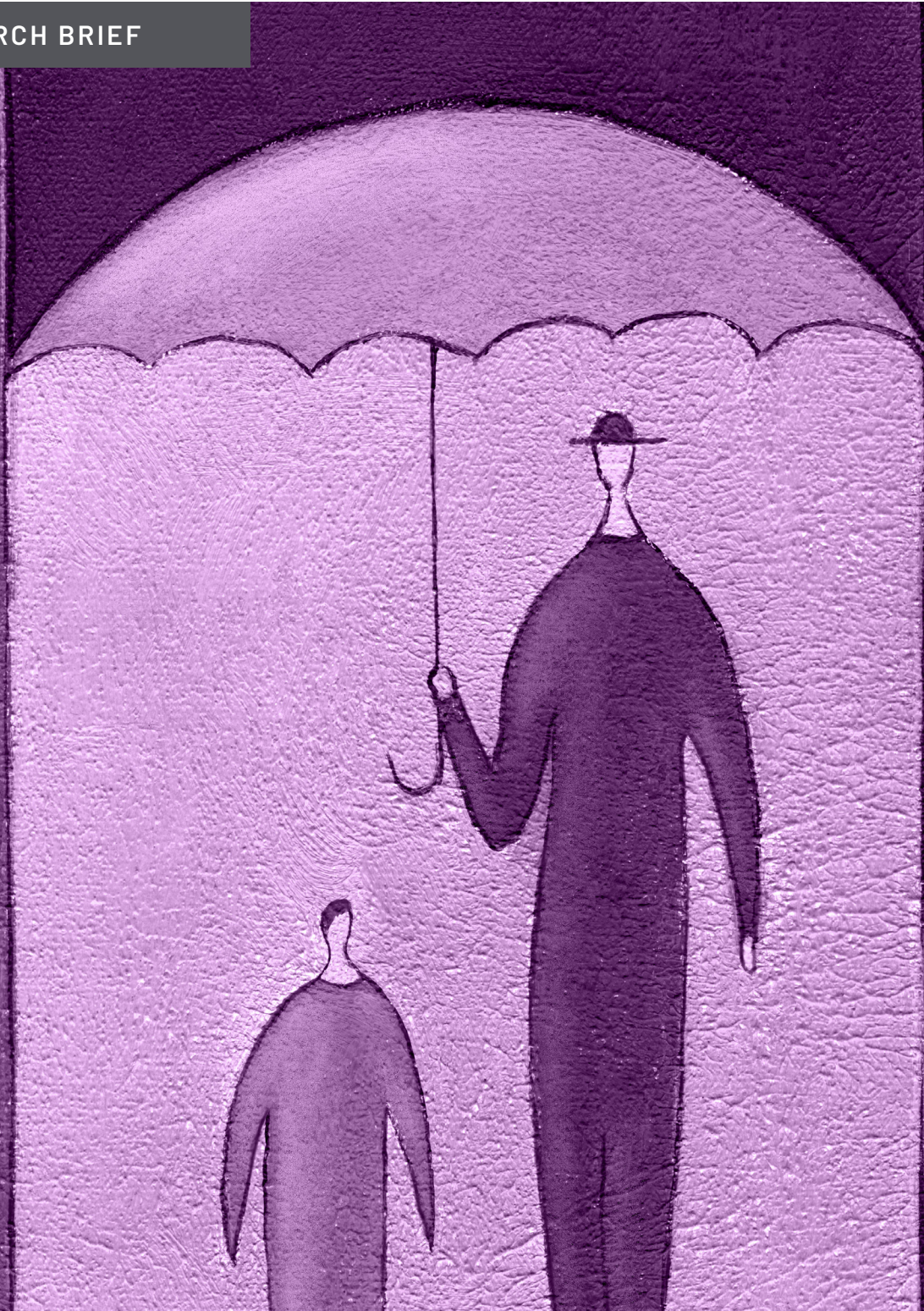


Table of Contents

Introduction	1
Key Telco Initiatives	1
5G Transition	2
Edge Build-Out	2
Complex Service Rollout	3
Fiber Densification	3
Virtualization and Cloud Transition	3
Disaggregation and Open Architecture	3
Increased Security Focus	4
Automation, AIOps, Zero-Touch, and OSS/BSS Modernization	4
Organization Transformation	4
Next-Generation Telco Service Assurance - Challenges and Opportunities	5
Complete Lifecycle Visibility	6
End-to-End – Multi-Domain, Multi-Silo Coverage	6
Multi-Layer – Networking and Application	6
Disaggregated and Open Architectures	6
Virtualization, including Containerization	7
Cloudification	7
Edge Diversity	8
Security and Assurance	8
Increased User Visibility and Involvement	8

Table of Contents (Cont.)

Strategies for Accelerating Next-Gen Service Assurance	9
Blending Active and Passive Approaches	9
Integrating Assurance into Design and Deployment	10
Embedded Assurance in Vendor Products	10
Investing in Automation	10
Developing a Cohesive Data Strategy	10
Demanding Rich and Relevant Telemetry from Vendors.	10
Complementing Analytics with a Model-Driven Approach	11
Leveraging Cloud-Based Analytics, AI/ML, and Solution-Wrapped AI	11
Adopting Cloud Culture	11
Conclusion - Towards a Zero-Touch and Closed-Loop Automated World.	12

Research Briefs are independent content created by analysts working for AvidThink LLC. These reports are made possible through the sponsorship of our commercial supporters. Sponsors do not have any editorial control over the report content, and the views represented herein are solely those of AvidThink LLC. For more information about report sponsorships, please reach out to us at research@avidthink.com.

About AvidThink™

AvidThink is a research and analysis firm focused on providing cutting edge insights into the latest in infrastructure technologies. Formerly SDxCentral’s research group, AvidThink launched as an independent company in October 2018. Over the last five years, over 110,000 copies of AvidThink’s research reports (under the SDxCentral brand) have been downloaded by 40,000 technology buyers and industry thought leaders. AvidThink’s expertise covers Edge and IoT, SD-WAN, cloud and containers, SDN, NFV, hyper-convergence and infrastructure applications for AI/ML and security. Visit AvidThink at www.avidthink.com.

REIMAGINE YOUR NETWORK OPERATIONS



With Ribbon's Advanced Analytics

Ribbon's 5G-ready Analytics portfolio leverages advanced automation with ML and root cause analysis, to monitor, isolate, and resolve operational and QoE issues as you build out your networks and services.

VISIBILITY → AGILITY → AUTOMATION

Ribbon's advanced service assurance and Analytics deliver:

- Automated Root Cause Analysis to monitor & troubleshoot

- ML to forecast network capacity & performance

- Improved end-user QoE & network Issues

- Reduced costs & risks to operators network



End-to-end
network visibility



Proactively
address issues



Security



Interactive
dashboards



Troubleshooting



Expedited issue
resolutions

INNOVATION YOU NEED
TECHNOLOGY YOU TRUST
PEOPLE YOU DEPEND ON



ribbon®

rbbn.com

How do you deliver the right QoS for your customers' mission critical 5G services?

The answer is Emblasoft.

Active monitoring, integrated with 5G nodes and NFs.

- Deploy in your production environment
- Measure QoS - latency, speed, errors and more
- Active integration for real-time automation
- Control and data plane protocols
- Scale to thousands of end-user agents

Trusted by Telenor, Swisscom, T Mobile and more, Emblasoft helps your 5G investments to pay off – and deliver the experience your customers and partners demand.

Is service assurance using device telemetry enough?

Here's why the shift to **Juniper Paragon Active Assurance** matters.

READ THE WHITE PAPER



Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Service Assurance – A Critical Telco Capability

Exploring Next-Gen Challenges and Opportunities

Introduction

Communication service providers (CSPs) today have numerous opportunities to evolve their services and transform their businesses. From 5G and edge computing to software-defined wide-area networking (SD-WAN) and secure access services edge (SASE), CSPs seek new ways to serve customers while leveraging unique assets.

These assets in the form of spectrum, connectivity infrastructure, valuable real estate (tower sites and switching offices), and decades of expertise in connecting consumers and companies while maintaining regulatory compliance can provide a barrier to competitors entering the space. CSPs may even have a chance to revive the IoT business as it experiences a 5G renaissance and grabs a slice of OTT (over-the-top) revenue by leveraging 5G build-out, fiber densification, and edge site expansion.

Whether 5G, or edge, or fiber, the essential capability critical to telco success in these initiatives is the promise of differentiated services and the ability to assure that quality of service. In this research report, we'll look at top CSP service initiatives and explore real-world strategies for assuring those services. The report is meant for a mixed audience of CSP business and technology leaders, networking vendors, integrators, and others in the telco ecosystem. Feedback is welcome, and you can reach us at research@avidthink.com.

Whether replacing 4G radios with 5G NR (new radio) across tower sites or upgrading wireless cores from 4G evolved packet core (EPC) to 5G core (5GC), many MNOs are on breakneck pace to upgrade their networks to the tunes of tens of billions of dollars per major carrier.

Key Telco Initiatives

CSPs are going through a new period of innovation. 5G and edge, and workplace mobility, along with realizing the importance of communication during the pandemic, have energized the telcos. Their goals and desire to remain relevant in the face of new competition from the OTTs and hyperscale cloud providers push them to be more creative in their efforts. The entire telco system has collectively taken on a faster transformation rate spurred by the early network functions virtualization (NFV) movement circa 2012. We'll discuss key telco initiatives, explain why assurance is critical, and then analyze key trends in service assurance today.

TODAY'S KEY TELECOM INITIATIVES





5G Transition



Edge Build-Out



Complex Services Rollouts



Fiber Densification



**Virtualization/
Cloud Transition**



**Disaggregation /
Open Architecture**



Increased Security Focus



**AIOps / Zero-touch
/ OSS-BSS
modernization**



**Organization and
Cultural Transformation**




5G Transition

5G represents the next generation of public mobile networks that offer faster speeds, better coverage, and new services like network slicing. The promise of 5G is compelling for mobile network operators (MNOs) looking to further monetize their investment and spectrum holdings. It's no surprise that over **100 5G networks went live worldwide in 2020** despite the pandemic. Further, 5G has ignited interest in private mobile networks for enterprises, opening the ecosystem to system integrators (SIs), cloud service providers, wireline providers, and startups.

MNOs are upgrading their network to 5G partially in search of marketing wins and adding capacity, improving throughput, and lowering latencies while enabling new differentiated services. Whether replacing 4G radios with 5G NR (new radio) across tower sites or upgrading wireless cores from 4G evolved packet core (EPC) to 5G core (5GC), many MNOs are on breakneck pace to upgrade their networks to the tunes of tens of billions of dollars per major carrier. The expectation is that carriers need this buildout to handle the increased needs of end-users consuming and generating more content, accommodating the tens of billions of IoT devices coming online, and providing the flexibility and agility to provide end-to-end differentiated services for business and consumer use.

Edge Build-Out

Related to 5G, edge computing has likewise risen to the forefront. As part of the 5G network build-out, MNOs are expanding the computing footprint to host parts of their 5G network at the edge. Similar efforts to have computing nearer end-users are underway with wireline providers, including the cable operators (multi-service operators or MSOs).

Edge computing is not a new idea. The edge exists in many mobile and wireline networks today, where edge-based content-delivery network (CDN) servers from sites like Netflix and YouTube help reduce latency and bandwidth. However, what's new is allowing end-users to run workloads on these edge computing servers as a shared resource pool. With a projected market size of **USD 250B in 2024 by IDC**, edge computing has piqued CSP interest and spurred early investment, even though

it's not clear that CSPs will capture a majority of that sizable market. Nonetheless, 5G with the edge and the hopeful resurgence of IoT should bring the CSPs a growing revenue source that they can tap into.

Complex Service Rollouts

To help combat declining average revenue per user (ARPU) in both wireline and mobile, CSPs have tried various strategies, including forays into cloud services and media and entertainment with mixed outcomes. CSPs have also tried to revitalize existing services like IoT, which have floundered, along with adding value-add services like unified communications and collaboration (UCC), software-defined wide-area networking (SD-WAN), and secure access services edge (SASE).

These offerings often span multiple domains of control and incorporate multi-layer network services. For example, analysts expect SD-WAN, a popular service being rolled out by CSPs globally, to grow at 24% over the next five years to **\$4 billion in 2025**. The SD-WAN offering combines a secure multi-point overlay orchestrated by a cloud controller, with numerous security and network services folded in. Carriers can package SD-WAN in combination with multiple underlay offerings, like MPLS, broadband internet, or fixed wireless access.

Given the need for revenue growth, CSPs will innovate in services that can help drive increased ARPU, mainly services that take advantage of new high-throughput fiber to the premises (FTTP) and 5G services.

Fiber Densification

Likewise, both MNOs and wireline operators are procuring and lighting up existing in-ground dark fiber and pushing new fiber build-outs. This fiber build-out will increase connectivity to hyperscaler clouds and other essential web locations, reduce latencies, and increase throughput for end-users, thereby improving the application experience. For wireline operators, some of the fiber will expand their last-mile footprint. For MNOs, a significant amount of the fiber will be used in their 5G densification, connecting 5G small cells based in dense urban areas.

Virtualization and Cloud Transition

The CSP move to network functions virtualization (NFV) starting in 2012 continues. However, the efforts are now multi-prong, with some network functions continuing to migrate to their VM versions (VNFs), while others are moving directly to cloud-native network functions (CNFs). Telco infrastructure or telco clouds comprise a mix of bare metal machines with Linux containers orchestrated by Kubernetes and hypervisor-powered VMs. Hybrid systems with containers in VMs, or even VMs in containers, are emerging, and the long-term expectation is that the latter will win.

Meanwhile, telcos are improving their operational capabilities as they build out and strengthen their networks. They view the hyperscale cloud providers as both partners and competitors in the offering of new services. Tier-1 CSPs, including AT&T, BT, Deutsche Telekom, Orange Business Services, Telstra, Telefónica, T-Mobile, Verizon, and Vodafone, have forged partnerships with the hyperscalers. Instead of building everything on an in-house telco cloud, many of them now depend on hyperscale clouds for their IT and back-office operations. Further, a subset of these CSPs is looking to run their mobile networks on CSP platforms. For instance, DISH is committing to using AWS to host their 5G mobile network, and Telefónica Germany uses an AWS platform to host a private 5G network for a large manufacturer.

Disaggregation and Open Architecture

Another CSP initiative that closely aligns with cloudification is disaggregation and the move to open architecture. Disaggregation and white box efforts span the core to transport to RAN. Open Compute Project (OCP), Telecom Infra Project (TIP), O-RAN Alliance (O-RAN), Open Networking Foundation (ONF), and the Linux Foundation are all hard at work in enabling an open ecosystem. The aim is to convert proprietary SW and HW stacks into open architectures with well-defined interfaces, expanding the number of ecosystem participants. The premise is this will lower costs, speed up time-to-market, and foster innovation. There are early efforts to replace core routers, edge cell-site routers, multiple network functions, and the RAN with their disaggregated counterparts. White box platforms, open RAN compliant with the O-RAN Alliance standards, are under

evaluation at CSPs globally. However, few telcos are running fully-disaggregated and open architectures, perhaps except for greenfield operator Rakuten Mobile in Japan and DISH in the US, which is in the process of starting their network rollouts.

Increased Security Focus

With an increased focus on cybersecurity, CSPs understand that they have a role and a stake in the security ecosystem. CSPs can offer customers security services in conjunction with networking offerings. However, they also need to ensure their infrastructure and processes are secure and resistant to attacks while maintaining a seamless user experience.

Automation, AIOps, Zero-touch, and OSS/BSS Modernization

With the complexity of new build-outs, infrastructure modernization, disaggregation, and increased scale, CSPs worldwide know that they cannot succeed without automation. Automation is so critical that Neil McRae, Group Chief Architect of BT, shared in a **recent event with the Network Media Group** that any CSP “who’s not making a significant investment in automation is really on a path to ruin.”

Many CSPs we speak with have early initiatives in AI/ML, but all are quick to point out that many of these efforts are nascent.

AvidThink has been in conversation and consultation with multiple tier-1 SPs globally, and it’s clear to us that automation is on the shortlist of operators’ top agenda items. The relationship between service assurance and automation is likewise undeniable – network automation is critical to enabling closed-loop systems that improve service reliability and CX. The goal of many carriers is zero-touch provisioning, to have services spin up and down without having a human involved in the entire process. While not fully achieved today, even across top-tier carriers, CSPs indicate that they are making progress. Automating actions on the network based on monitored metrics and rules-based AI and machine-learning (ML)-based decisions is essential to achieve the scale and reaction times that new 5G network services demand.

Many CSPs we speak with have early initiatives in AI/ML, but all are quick to point out that many of these efforts are nascent. However, in applying AIOps to assist their teams, a few CSPs are already seeing value in

customer service and network troubleshooting – improving customer retention, predicting equipment failures, and helping deal with historically hard-to-track brownouts.

In addition, CSPs recognize that many of the new services require a more intelligent operations support system (OSS) and a more flexible business support system (BSS). They have embarked in varying degrees on projects to migrate legacy systems to cloud-native systems, using a combination of networking software vendor commercial products and in-house custom coding, sometimes leveraging open-source orchestration projects.

Organization Transformation

Finally, CSPs recognize the importance of the cultural change necessary to move their organizations into a world of 5G, cloud, and edge. To compete against the hyperscalers and OTT players, CSPs have to adopt the same agile practices that have enabled OTT and hyperscale clouds to grow as rapidly as they have. CSPs will need a customer-focused approach, ensuring positive customer experiences (CX) by introducing novel services that better meet today’s customer needs.

Next-Generation Telco Service Assurance - Challenges and Opportunities

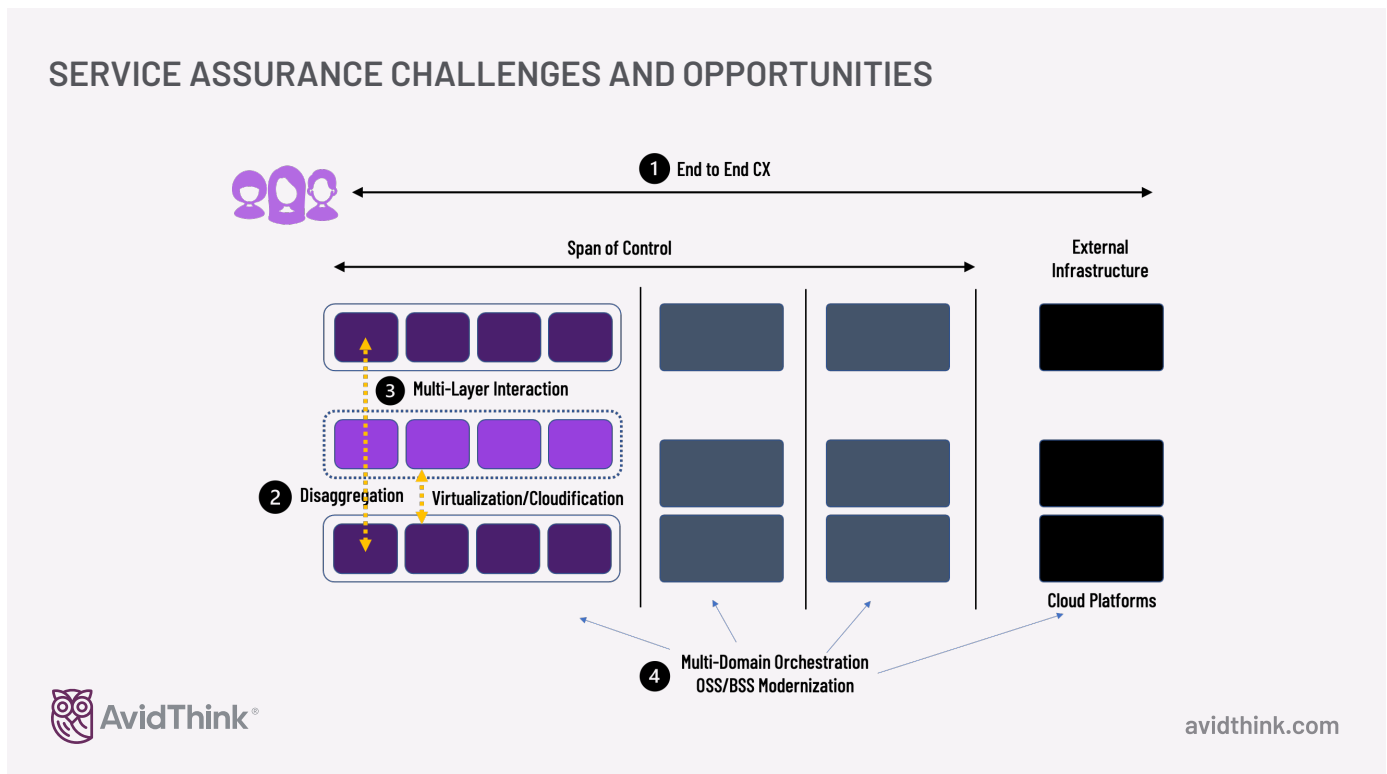
In the past, CSPs worldwide adopted the ISO telecommunications management network model, FCAPS. Fault, configuration, accounting, performance, security – these were the categories that defined network management. Today, those elements remain, but the scope of network management and assurance are broader and deeper.

As we examine the telco initiatives above, we see common elements that tie into the service assurance discussion. First, to remain competitive in the market with new services, there’s an increasing focus on ensuring that the end-to-end customer experience meets or exceeds expectations. To assure this level of CX requires cross-domain, cross-silo visibility, even in situations where the CSP doesn’t control the underlying infrastructure (like public clouds).

Second, there are architectural changes that mandate a different approach to assurance. They include virtualization, disaggregation, and cloudification. This pushes assurance to be more agile, flexible, and software-centric than in the past – telemetry gathering needs to be more comprehensive and cloud-friendly. It also means that assurance needs to understand the interplay between components that have been disaggregated.

Third, many new revenue services are multi-layer and composed of aggregate services (e.g., SD-WAN or SASE, or UCC). Assurance, therefore, needs a strong correlation capability with the ability to define dependencies. It also means that modeling is an integral part of assurance; likewise, active assurance methods will need to complement existing passive monitoring solutions.

Finally, there’s ongoing modernization and transformation of infrastructure and a cultural change towards a continuous integration/continuous deployment (CI/CD) mindset. Assurance will increasingly need to be built into the CI/CD pipeline as a critical step. CSPs will want to embrace reliability engineering practices from cloud companies within their processes. The diagram below summarizes the key pillars of change needed for a next-generation service assurance approach.



In an arena where the competition will drive improved customer experience and where monetization from enterprises will be based on offering end-to-end differentiated services, a focus on and investment in service assurance is critical.

We'll now dig into each of the critical elements that are challenges and opportunities for the new generation of service assurance at CSPs.

Complete Lifecycle Visibility

Today's scope for service assurance starts even before service is turned on during the discovery and purchase phase. This continues through provisioning and on-boarding, ongoing service use, any service upgrades or updates until decommissioning and off-boarding. All this is meant to improve the CX and help with customer acquisition and retention – vital goals for enterprise and consumer customers in a competitive communications market under attack from OTTs and where CSPs no longer hold sway.

End-to-End – Multi-Domain, Multi-Silo Coverage

As expressed earlier, today's CSP services go beyond physical connectivity like DSL lines, simple mobile connections, or an MPLS link. Enterprises and consumers purchase more complex services from CSPs, with end-users more concerned about the application experience than underlying connectivity. Simple 5-bar coverage is not always a helpful metric; the consumer is much more worried about how seamlessly Netflix streams, how robust their Apple FaceTime call is, and how quickly their TikTok video loads. The business customer is looking at whether employees can productively use popular SaaS applications like Salesforce, Box file sharing, Zoom conferencing and whether services like SD-WAN can improve the reliability and throughput of their wide-area networks.

There are more components that make up the total user experience – from the underlying network to computing elements that host user applications to the applications themselves. Even at the network level, there's complexity with overlays, not to mention the multiple domains that today's networks span. From public cloud data centers (where telemetry might be limited and insertion of 3rd-party instrumentation not possible), through backbone networks, tail circuits, and enterprise or home networks that serve the final stretch to the devices, there are many hops. When we add dynamic network slicing, tracking telemetry for applications and end-users can be highly complicated.

Multi-Layer – Networking and Application

Early assurance used to be about tying faults in the underlying physical connectivity to higher-level services. Even today, we continue to treat assurance and performance management of networks separate from applications (hence the categories of NPM - network performance management versus APM - application performance management).

For CSPs, though, the reality is that customer tickets will increasingly come within an application context: Netflix can't stream, Zoom video is intermittently displaying strange artifacts. Whether the source of failure or performance degradation was a high bit error rate on the physical link due to recent rains, an errant router, a DNS cluster with a single failing server, a misconfiguration in the in-memory database cache, or even a bug in the last night's application push, the customer is unhappy. That will require the next generation of service assurance to provide multi-layer integrative assurance and a deeper understanding of the application stack and dependencies.

Disaggregated and Open Architectures

Disaggregated and open architectures represent a collection of commercial off-the-shelf hardware (with hardware performance accelerators where needed) combined with software that runs on that hardware, either as bare metal, or containers, or virtual machines (in combination with virtualization). Disaggregation can also apply to software, where open interfaces between components are standardized, allowing multiple vendors to participate in the ecosystem. Whether O-RAN compliant or not, Open RAN is the latest wave of disaggregation for CSPs, especially the mobile operators.

While disaggregation can lower costs, increase flexibility, and foster innovation, it can create more interface combinations and variations of components, which need to be tested during integration and actively monitored in production. And if interfaces are not sufficiently well-defined or vendors not fully compliant, the benefits from disaggregation can be lost to the integration and troubleshooting overhead.

Disaggregation presents both a challenge and an opportunity for service assurance. Because there are more piece parts and interfaces to monitor, there's increased complexity. For disaggregation to be successful, strong service assurance is critical. Even after lab integration tests are run and vendor equipment certified, post-deployment testing and ongoing day 1+ assurance are vital to ensure the overall system exhibits KPIs that meet service-level agreements or objectives (SLAs, SLOs). Continuous monitoring of the different elements in a disaggregated architecture and integration and deployment tests during service rollouts and upgrades is essential.

Virtualization, Including Containerization

Service assurance today needs to seamlessly handle network functions and applications running in both VMs and containers. This means that telemetry gathering agents need to run in software as virtualized agents or probes and be deployable into VMs and container systems. Virtualization also means that the performance and behavior of the underlying virtualized infrastructure need to be assured. In the past, when network functions were wrapped in proprietary physical appliances, the entire system was the unit of test and monitoring. Many more elements need to be monitored and tested in a virtualized and containerized world, including the hypervisor managing VMs, the container run-time system, virtual switches, and software acceleration libraries like Data Plane Development Kit (DPDK), or SmartNICs handling the network traffic on behalf of the CPU. This drives increased complexity and sophistication required from the monitoring and assurance systems – just tracking the dependency graph of the various elements for subsequent correlation is no small feat.

Cloudification

Scaling up one level beyond virtualization and containerization is the use of cloud platforms. Both private clouds and public clouds provide the appeal of a scalable, on-demand infrastructure. In addition, cloud platforms represent a unifying abstraction that will host both applications and the new generation of software-based network functions. Multiple networking solution vendors have certified their platforms and software on public cloud solutions. Cisco, Juniper Networks, Nokia, Ericsson, Amdocs, Netcracker (NEC), and other major providers have indicated a willingness to treat the public cloud as a first-class platform.

However, in our work with CSPs, many of them have teams that are just making the transition to NFV and virtual network functions (VNFs) and aren't ready to take on the mantle of moving to Kubernetes and containers yet.

Regardless, moving to the cloud provides on-demand, scalable infrastructure but also adds service assurance challenges. There is limited visibility into the underlying infrastructure within a public cloud provider, so if a particular network link is slow, there are no easy ways to understand why (nor controls to ameliorate any issues). Likewise, service assurance strategies that follow the workload and can adapt to IP address changes, follow ephemeral container-based services, and can scale up and scale down operations, makes redeployment across distributed locations essential in understanding the performance envelope of the new breed of cloud-native network functions (CNFs). Tying into CI/CD pipelines as part of new deployments, running unit tests, mandating integration testing, and validating via active testing on service changes or turn-ups are all part of the next generation of service assurance workflows.

Tying into CI/CD pipelines as part of new deployments, running unit tests, mandating integration testing, and validating via active testing on service changes or turn-ups are all part of the next generation of service assurance workflows.

Edge Diversity

The edge will bring an additional set of locations where networking and computing can be deployed, adding to the number of sites to be monitored. Furthermore, because of space and power constraints, and potentially harsh conditions, there can be a different set of equipment typically found in a data center. The increased diversity of computing and networking equipment means more challenges for assurance and additional opportunities to add value.

Given the level of CSP interest in initiatives like open RAN and mobile edge and multi-access edge computing, service assurance solutions need to handle multiple hundreds or thousands of remote locations where computing and networking equipment are sequestered. Service assurance will need to provide aggregation capabilities to consolidate the information from these distributed locations and run in a disconnected mode and recover when these sites go down. We anticipate new models for local assurance in disconnected modes based on the different deployment models for edge (e.g., a private mobile edge in a factory, which is focused on assuring the local connectivity for manufacturing processes, may treat a WAN down event as important but not critical, versus a local small-cell down event, which is critical severity).

Security and Assurance

In some ways, security is part of service assurance – ensuring the continuity and uptime of critical business or consumer connectivity services. Likewise, protecting the integrity of communications and ensuring that no eavesdropping, corruption, or other compromises of the end-to-end service constitutes assurance.

A CSP confident enough to show ongoing measurements of service KPIs telegraphs competence and can attract new business through superior service assurance.

The other overlap between security and assurance is the use of telemetry information for both. The same analysis that a monitoring solution uses to determine service impact can also be mined for potential security breaches and anomalous information. CSPs (and networking vendors) must understand the types of data that can feed both service assurance processes and security systems and manage the data feeds to achieve both goals.

Increased User Visibility and Involvement

As part of improving the overall user experience, a few of the CSPs we spoke with are looking into extending the visibility of the service assurance process to end customers. Integrating convenient customer ticketing or just feedback gathering (mobile devices, single click, report problems buttons) can help smooth out the customer experience while gathering potentially valuable customer

input. Likewise, self-service status checks or aided troubleshooting (AI-powered) can reduce the time-to-resolution for customers.

Exposing elements of the service assurance process, like display KPIs or measuring those against SLOs/SLAs, can provide customer comfort and add to service differentiation. A CSP confident enough to show ongoing measurements of service KPIs telegraphs competence and can attract new business through superior service assurance.

Strategies for Accelerating Next-Gen Service Assurance

Given the above telco trends and the key challenges and opportunities in service assurance, what are CSPs today doing to move ahead in the journey to the next generation of service assurance? In recent conversations with several leading CSPs and other ecosystem thought leaders, we gathered the following concrete approaches:

NEXT-GEN SERVICE ASSURANCE - READY FOR THE FUTURE





Combine Active + Passive Methods



"Shift-Left" Assurance



Embedded Assurance



Rich Telemetry



Modeling + Analytics



Leverage Cloud-AI/ Prepackaged AI



Cohesive Data Strategy



Invest in Automation



Adopt Cloud Culture


avidthink.com

Blending Active and Passive Approaches

CSPs today are taking a blended approach to service assurance, combining both active and passive strategies. Active techniques include injecting synthetic transactions that mimic real-world interactions and measuring the outcomes to determine performance. Passive methods involve the placement of probes and gathering of telemetry information from the various network and computing elements (routers, switches, virtual agents hosted at critical locations) and using analytics to pull together a picture of network health, correlating performance events to the underlying traffic streams.

While there were debates in the past on the virtues of one approach versus the other, the networking industry today understands that both techniques are complementary and required for thorough performance assurance. Today, leading assurance vendors, including Accedian, Keysight/IXIA, Ribbon, Spirent, and Viavi, advocate a blended active and passive approach, settling the debate with finality.

Historically, there was a tendency to rely on monitoring (passive) to surface problems. However, with the complexity inherent in multi-layer and multi-domain services, CSPs are finding that active approaches that mimic a real-user transaction can provide immediate and relevant insights into performance. Active assurance techniques can also highlight issues during turn-up without waiting for monitoring data to come in. Further, active techniques can build baseline performance metrics that can be tracked and benchmarked over time (especially post-service changes).

Meanwhile, passive monitoring can be used to provide deeper insight (using AI/ML). The rich data set can power predictive maintenance, where CSPs take proactive measures to mitigate upcoming performance or reliability issues. That same data set can be fed into security systems to detect anomalous behavior in the network.

Integrating Assurance into Design and Deployment

In software development, “shifting left” means moving a process that previously happened downstream to earlier in the development pipeline – for instance, moving security validation and assessment of software to occur during the build phase instead of post-build. Likewise, for assurance, CSPs we speak with are looking to move assurance from a post-deployment process to a pre-deployment practice. Service assurance is being designed into service creation and baked into service turn-up. Likewise, from a change management standpoint, any service update or configuration change needs to be tested (automatically) as part of the redeployment.

This allows early detection of deviations of the service parameters from expected norms. It also shortens the time to resolution and troubleshooting for discovered issues. Most importantly, this practice detects problems before customers can encounter them, improving the customer experience.

Embedded Assurance in Vendor Products

Related to the “shift left” discussion, we’re seeing networking vendors baking assurance capabilities into their services. Major networking vendors like Cisco and Juniper Networks have made acquisitions in recent years that bring assurance technologies in-house – Cisco purchased ThousandEyes (adding to their AppDynamics application performance monitoring purchase from 2017), and Juniper Networks purchased active assurance startup Netrounds (now known as Juniper Paragon Active Assurance) as well as AI-powered WiFi provider Mist. We anticipate that networking vendors will be increasingly pushed to embed assurance into their products to help reduce the complexity of troubleshooting the increasing number of disparate components that are orchestrated to form a higher-level service (SD-WAN, private mobile 5G, etc.).

Investing in Automation

This particular item should be no surprise – we’ve covered multiple aspects earlier in the report. Automation is key to baking in service assurance as part of a deployment process and ongoing active assurance (periodic active testing to gather KPIs). Automation is also critical in creating zero-touch, closed-loop solutions that utilize the output of monitoring or active testing results to trigger appropriate workflows that can mitigate existing performance issues – for instance, turning up new circuits for additional capacity, allocating more cloud resources, and spinning up network functions to handle the increased load, or migrating traffic from failing hardware proactively.

Developing a Cohesive Data Strategy

Carriers we speak with understand the term “data lake,” which has replaced the dated data warehouse terminology. Regardless, the key to modern assurance is the management of crucial telemetry, metrics, and performance information that help build a picture of the customer experience. What data to gather, how to gather, where to store, when and how to process, and what to do with the results of processing the data are questions that need to be answered by a cogent data strategy.

With the move towards AIOps and AI/ML for other functions beyond assurance, like security, fraud detection, or even monetization, data management is a critical pillar in enabling next-gen service assurance.

Demanding Rich and Relevant Telemetry from Vendors

Essential to building the data that powers the next generation of assurance is having the data available in the first place. CSPs are working with networking and software vendors to ensure that the right metrics can be pulled from devices. For example, buffer utilization across devices and KPIs for software-implemented queuing or buffering mechanisms for network functions must be exposed to allow assurance systems visibility into that data. Especially with disaggregation and virtualization, new

software and hardware infrastructure components are introduced into the architecture, all of which need to expose appropriate telemetry to enable visibility.

Complementing Analytics with a Model-Driven Approach

Putting data into a large repository is a significant effort but translating that data into valuable and actionable information requires understanding how the data fits together. CSPs at the forefront of next-gen assurance are working towards a service model-based approach for their services, understanding how each part fits together and impacts a specific service (e.g., an underlying link failure may not impact the uptime of an SD-WAN service that utilizes multiple links, but may impact maximum bonded throughput).

We see leading CSPs (and vendors) working on incorporating the concept of assurance as part of service modeling and definition – trying to capture service intent and SLA attributes within the service definition. These CSPs believe that combining models with analytics will yield helpful insights faster than through a pure analytics approach.

In addition, because of the complexity of multi-layered and multi-domain services, CSPs are looking at modularizing sub-services. By creating useful and meaningful blocks of sub-services and assurance at each level, CSPs hope to stack them into aggregated top-level service metrics.

Leveraging Cloud-Based Analytics, AI/ML, and Solution-Wrapped AI

Leading CSPs we spoke with are embracing cloud platforms for their assurance initiatives. Public cloud services provide a rich set of big data analytics services, along with advanced AI and ML tools. Instead of recreating these analytics stacks in-house, CSPs are increasingly open to using public cloud services to collect, store and process telemetry data.

In addition, full AI/ML stacks are available in public clouds with services wrapped around them to make them easier to consume. By offloading the development and integration of these stacks in-house and leveraging best practices from the cloud providers, leading CSPs are finding themselves off to a faster start. Some CSPs are continuing to make in-house investments in AI/ML, both as a hedging strategy and hoping that they can plow new ground and find unique implementations specific to the telco market that the cloud providers might have missed.

For CSPs who might not have the capabilities or cycles to invest in building their own AI/ML capabilities, we have networking software vendors offering packaged solutions that utilize sophisticated AI learning models. These “solution-wrapped AI” packages allow CSPs to benefit from advanced technologies without necessarily having to learn the ins and outs of AI learning strategies like supervised and unsupervised learning. For example, Ribbon has wrapped machine learning in their network planning application and utilizes advanced analytics for their mobile and fixed assurance products.

Adopting Cloud Culture

With the virtualization and “softwarization” of networking and telecommunications services, telcos increasingly look like software delivery houses with new innovative services powered by software running on cloud platforms. Therefore, it makes sense to adopt and adapt the same assurance practices (e.g., site reliability engineering) developed and practiced by software and hyperscale cloud providers.

From continuous integration and continuous deployment (CI/CD) to test-driven development (where tests are written before the software is developed), the assurance process at CSPs should adopt these cloud-centric practices. Likewise, with automation and a cloud-native foundation for network services, innovative approaches like canary testing and blue/green deployments can be used. Canary testing involves rolling out

With automation and a cloud-native foundation for network services, innovative approaches like canary testing and blue/green deployments can be used.

upgraded services to a select subset of users, carefully monitoring the KPIs for that service, and validating user experiences. Only when verified is the change pushed to a larger population. These new approaches are starting to make their way into the market. A case in point is startup Emblasoftware, a provider of test and verification solutions that has 5G test solutions advocating CI/CD frameworks and canary testing for 5G network rollout.

In blue/green deployment, the CSP would have two production environments – the current and an upgraded set of services. The users would be migrated to the new services (green environment) while keeping the old (blue) services available for quick switchback if the new rollout doesn't go successfully.

Other practices that can help institute a next-gen assurance include NetDevOps, which adopts a DevOps model within the network. This leverages a strong automation foundation and scalable deployment and troubleshooting tools; it also creates a new role within the CSP that can help with new culture adoption and potentially recruitment (being viewed as a “cool” position).

Conclusion – Towards a Zero-touch and Closed-loop Automated World

We've attempted to capture our on-the-ground conversations with telcos, networking vendors, and other network operators in the sections above and distilled our findings into actionable steps for CSPs.

The pandemic in 2020 demonstrated the importance of a scalable and reliable communications infrastructure. 5G, edge computing, and new business services demand a higher level of assurance than before, at a faster deployment rate than any time in the past. To achieve success in new service rollouts, retain and attract customers through superior experiences, and monetize differentiated services enabled by 5G, CSPs will need next-gen service assurance capabilities. We hope the findings in this paper aids you in that journey.



AvidThink, LLC
1900 Camden Ave
San Jose, California 95124 USA
avidthink.com

© Copyright 2021 AvidThinkI, LLC, All Rights Reserved
This material may not be copied, reproduced, or modified in whole or in part for any purpose except with express written permission from an authorized representative of AvidThink, LLC. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced. All Rights Reserved.