RESEARCH

analysys mason

WHITE PAPER FOR NETSCOUT SYSTEMS

ASSURING APPLICATION AGILITY IN MULTI-CLOUD ENVIRONMENTS: CSPS MUST LOOK BEYOND NETWORK PERFORMANCE

Anil Rao

OCTOBER 2018

analysysmason.com

Contents

List of figures

1. Executive summary

Enterprises worldwide are undergoing some form of digital transformation or have a digital strategy in place. At the heart of these transformations is an intent to provide consistent and superior real-time customer experience to their end customers, rapidly deliver new services, and significantly reduce the cost of operations. To achieve some of these goals, enterprises are moving to multi-cloud environments; research shows that enterprises now use multiple public cloud platforms alongside their own private clouds.[1]

Multi-cloud environments enable application agility, allowing enterprises to dynamically place the applications and workloads in the most suitable cloud environment, and access public cloud and SaaS-based cloud services to deliver the best application performance, latency, and customer experience at lower cost points. However, to deliver application agility, enterprises must overcome the networking bottlenecks – rigid appliance-based branch networks and static wide-area network (WAN) connections. The focus is on communications service providers (CSPs), which supply wide-ranging managed services to enterprises, including branch networks and WAN services, to deliver agile branch networks and agile WAN.

Reacting to market demand, CSPs are launching managed software-defined WAN (SD-WAN) solutions, which enable enterprises to dynamically select a WAN path (e.g. IP/MPLS or internet) based on factors such as the destination (e.g. public cloud, private cloud, data center, or another branch) and the criticality of the traffic (e.g. critical or recreational). An appliance-based SD-WAN would increase the rigidity of the branch networks, so CSPs are offering universal CPE (uCPE)-based SD-WAN solutions. Taking advantage of the maturing software-defined networking (SDN) and network function virtualization (NFV) technologies, the uCPE platform obviates the need for proprietary appliances for WAN services such as SD-WAN, firewall, and WAN optimizers, and replaces them with equivalent software-based VNFs. Combined with orchestration capabilities, the uCPE platforms provide software-based dynamic control, allowing CSPs to deliver on-demand WAN services.

Service assurance will play a crucial role in the success of CSPs delivering the agile connectivity and branch services for application agility. CSPs, however, need a new assurance approach; one that is based on the ability to monitor and assure a highly dynamic application and WAN environment. The traditional WAN assurance solutions, designed for static branch and WAN environments, consist of a disparate set of tools, focusing primarily on performing service test and turn-up testing, monitoring the network appliances and the physical WAN links for performance degradation, and used separate tools for application performance monitoring.

Assurance for multi-cloud environments must take into consideration the new dynamic networking environment with SD-WAN, uCPE, and agile applications and workloads that will be distributed and moved across cloud environments. CSPs need to take an application performance-led end-to-end assurance approach providing a granular, near real-time view of how network performance is affecting application performance. The assurance solution must rapidly adapt to the dynamic network traffic paths and application locations to present an accurate view of the end-to-end service performance. It should incorporate dynamic active testing to validate the SD-WAN service and the VNFs instantiated in the uCPE environment, as well as the applications in the multi-cloud environment. And finally, the unified assurance solution should also provide the capability to monitor the health of the underpinning uCPE infrastructure and the VNFs and offer a fully correlated performance view across the

[1] According to the "RightScale State of the Cloud Report" (2018), enterprises are using an average of 4.8 public and private clouds.

service chain, network, and the infrastructure layers. As part of the technology evaluation process for monitoring multi-cloud environments, CSPs should consider a unified assurance approach based on virtual passive and active probes, which can provide an independent and vendor-neutral view of the end-to-end service performance.

2. CSPs are helping enterprises move to multi-cloud environments through SD-WAN and uCPE propositions

Rapidly shifting business goals and the increasing proliferation and maturity of public cloud services are leading many enterprises to embrace multi-cloud strategies. There are many business reasons why enterprises are embracing a multi-cloud approach, prime among these are:

- *Application agility*: quest for application agility and performance – enterprises want to place the applications, and run workloads, on cloud environments that are most suited for those applications and want to move them around based on various requirements such as latency, security, regulation, and costs.
- *Cloud vendor independence*: multi-cloud strategy allows enterprises to avoid cloud vendor lock-in and choose cloud platforms based on the needs of application and workload performance.
- *Access to SaaS clouds*: most enterprises now access applications such as Microsoft Office365, Oracle, SAP, and Salesforce hosted on the respective SaaS vendor clouds.
- *Disaster management*: cloud platforms provide a level of native redundancy but distributing the critical workloads across multiple cloud environments prepares the enterprises to mitigate the risks of disasters much better and continue to guarantee availability and SLAs.

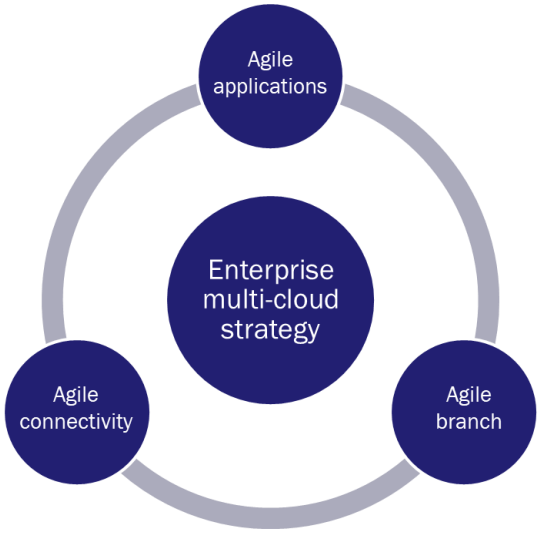


Figure 2.1: Multi-cloud environment for application agility [Source: Analysys Mason, 2018]

However, to fully realize the benefits of application agility in multi-cloud environments, enterprises must overcome the twin bottlenecks of static connectivity and rigid branch networks. Enterprises need:

- *Agile connectivity*: enterprises need a dynamic and cost-efficient approach to connect to multiple clouds and branches. The current mechanism of using static WAN connectivity services such as IP/MPLS was designed to link traditional branches and is not entirely fit for purpose for multi-cloud environments, not easy to scale, and often requires weeks to provision.
- *Agile branch*: enterprises need branch networks that can rapidly adapt according to the changing demands of the branch and the applications that are accessed from that branch. Existing branch networks employ a plethora of dedicated CPE appliances to perform specific network functions such as a router, a firewall, or a load balancer, which take weeks to procure, install, and provision. These static branch networks, which are often costly and time consuming to deploy, must be reimagined to cater for agile multi-cloud access.

CSPs are playing a significant role in enabling enterprises to make the move to a multi-cloud environment by offering managed SD-WAN services for agile connectivity and uCPE platforms to transform the branch networks.

2.1 CSPs are offering managed SD-WAN services to enable agile connectivity

SD-WAN technology provides improved control for enterprises to leverage hybrid WAN services. It delivers greater application agility and simplified software-defined control by allowing dynamic traffic routing based on the destination (i.e. public cloud, private cloud, data center, or another branch) and the criticality of the applications (Office365, YouTube or SAP, etc.). Traffic that is deemed critical can be routed via the IP/MPLS network for guaranteed QoS and performance. Traffic that is destined to locations that have no dedicated connectivity or that is deemed non-mission critical can be routed via the internet.

To capture this emerging market demand, many CSPs are now offering managed SD-WAN services, bringing together a range of different access technologies including IP/MPLS and internet. This allows CSPs to retain the primary customer relationship with the enterprises while taking full ownership of designing, provisioning, and maintaining the network and services, as well as service management for guaranteeing quality of service. Furthermore, a managed SD-WAN service provides CSPs with a strong foundation to strengthen the business relationship beyond network connectivity to guaranteeing application performance.

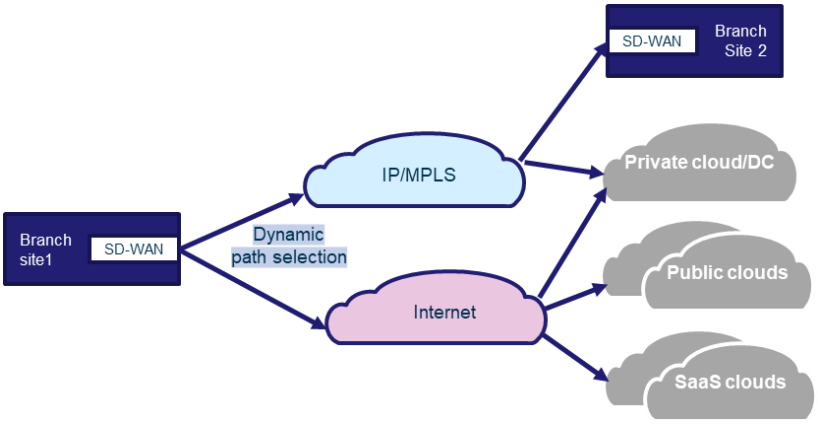


Figure 2.2: SD-WAN for agile connectivity [Source: Analysys Mason, 2018]

Initial SD-WAN solutions relied on proprietary technology on a dedicated appliance but lacked open interfaces and interoperability – this is not a preferred deployment model, as the SD-WAN appliance further increases the complexity of the branch network and contradicts the principles of an agile branch. However, with significant industry efforts (e.g. MEF) and increasing demands from several influential Tier 1 CSPs, the industry is working towards standardizing SD-WAN and pushing vendors to develop SD-WAN as a virtualized network function that can run on a cloud-based white-box environment (see Section 2.2). SD-WAN as a VNF provides a whole

other level of operational control, allowing CSPs and enterprises to deploy, provision, and configure SD-WAN on demand.

2.2 SD-WAN is driving demand for uCPE – the foundation of an agile branch

Traditionally, CSPs have delivered WAN services such as routing, firewall, load balancer, and WAN optimization using physical appliances. New site turn-ups typically take weeks to fulfil because the appliances must be shipped, installed, integrated, and provisioned. Moves, adds, or changes are also time consuming because of the complexities related to migration activities and change management overheads. Figure 2.3 illustrates the traditional appliance-based branch network architecture, including SD-WAN.

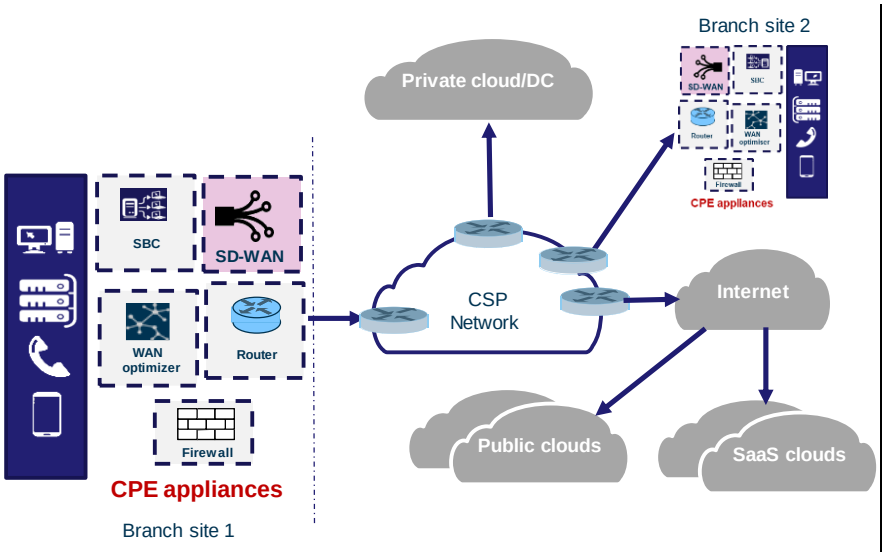


Figure 2.3: CPE and PNF based architecture [Source: Analysys Mason, 2018]

In contrast, uCPE platforms offer a revolutionary approach to the way WAN services are offered, procured, and consumed. uCPE platforms significantly reduce the complexity of the branch networks by replacing the plethora of dedicated CPEs and network appliances, such as firewalls and WAN optimizers, with equivalent software-based VNFs, all running on cloud-based NFV infrastructure. Using an NFV orchestrator, CSPs can dynamically provision certified multi-vendor VNFs onto the uCPE platform and configure the end-to-end service (i.e. service chain), as per the needs of the enterprise. An SDN controller is used to make traffic-steering decisions to route traffic in the network based on network and security policies, and real-time traffic conditions.

The uCPE-based approach enables CSPs to reduce time-to-market cycles by automating service turn-up through zero-touch deployment, while enterprises can instantly provision new sites and modify services on demand using a self-service interface. From an operations perspective, uCPE deployment allows CPSs to remotely monitor and troubleshoot problems while reducing truck rolls and mean time to resolution, and associated opex. Figure 2.4 illustrates the uCPE and VNF-based architecture.

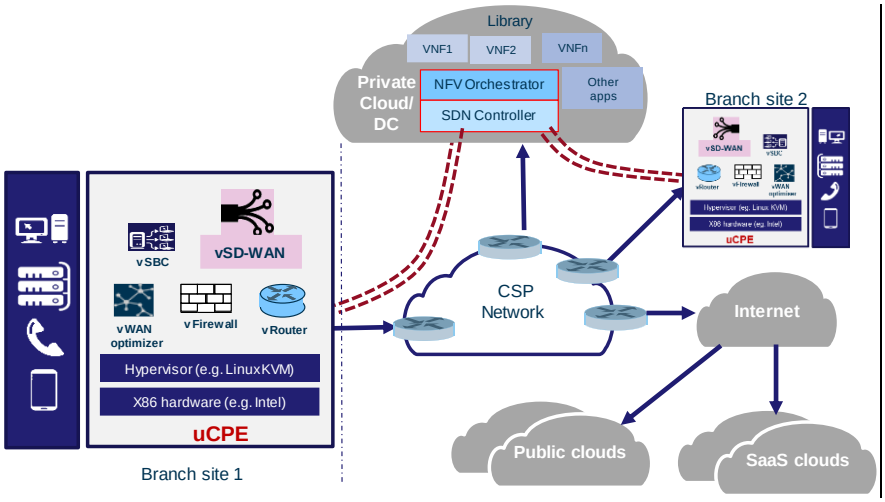


Figure 2.4: uCPE and VNF-based architecture for agile branch [Source: Analysys Mason, 2018]

2.3 Leading CSPs are rolling out uCPE-based SD-WAN and other services

Commercial uCPE platforms are now widely available from many vendors and CSPs are moving quickly to offer uCPE-based SD-WAN solutions. For example, British Telecom (BT) is offering the Cisco SD-WAN solution as a VNF over the Cisco Enterprise Network Compute System. Telstra is offering the VeloCloud (VMWare) SD-WAN VNF over Juniper's uCPE platform. Verizon is using Adva and Dell EMC for the uCPE platform and has partnered with Cisco and Versa Networks for SD-WAN.

In addition to SD-WAN, many CSPs are offering a catalogue of other WAN services as VNFs over their chosen uCPE platforms; the most common being: routing and switching, firewall, SBC and WAN optimization (see Figure 2.5).

Figure 2.5: CSP case studies for uCPE [Source: Analysys Mason, 2018]

CSP	uCPE market offering
AT&T – FlexWare services	AT&T positions the service as a combination of FlexWare Devices and FlexWare Applications. Enterprise customers can deploy an AT&T-branded x86 server at a site and provision a series of AT&T-certified VNF applications to suit the needs of the site. AT&T also offers a customer self-service portal. The FlexWare services are available in over 200 territories and countries. The FlexWare VNF applications portfolio includes Cisco and Juniper virtual routing, Fortinet, Juniper, Palo Alto and Check point virtual security, and Riverbed virtual WAN acceleration.
Verizon Communications – Virtual Network Services	Addressing its enterprise customers' demand to move from hardware to software-based cloud-enabled solutions, Verizon launched a premises-based uCPE platform. The solutions allow Verizon's customers to rapidly install and deploy software-based network services on a common uCPE platform. The uCPE platform uses OpenStack for hypervisor and NFV Infrastructure management and supports both wired and LTE connections. Verizon offers a range of virtual network services from a catalogue of leading vendor options on its uCPE platform, such as security (e.g. firewalls, IPSec VPNs, intrusion detection and protection, URL filtering) and WAN optimization (data compression, TCP acceleration, and application streamlining).
NTT Communications – uCPE Services	With uCPE services, NTT Com works closely with customers to optimize their branch networks by leveraging a combination of VNF services. Customers can use the web portal to self-manage the uCPE services or employ NTT Com's managed services. NTT Com's uCPE

CSP	uCPE market offering
	services provide a comprehensive set of VNF functionalities including routing, VPN, WAN optimization and acceleration, application delivery controller and many more.

3. Service assurance for static WAN and branch networks is limited to assuring connectivity

In the era before the emergence of public clouds, SaaS service providers and multi-clouds, enterprises typically hosted their applications at predefined private clouds, own and/or third-party data centers. The applications were largely stagnant and were not expected to move around the data centers that often. Enterprises required static WAN connections to link the branches and deliver on a predefined set of network performance metrics such as bandwidth and SLAs. Consequently, CSPs primarily focused on providing layer 2/3 WAN connectivity services, and some value-added services such as WAN optimization and security.

Similarly, CSPs developed their assurance and operations capabilities focusing mainly on ensuring accurate WAN service delivery and network monitoring for KPIs such as availability, bandwidth, network performance, and QoS for the WAN connectivity services. Industry organizations such as MEF worked in collaboration with the ecosystem players to standardize the carrier Ethernet and WAN services and associated assurance processes, which helped CSPs and vendors to coalesce around a common framework for assurance.

Overall, the inherently physical and static nature of the WAN connectivity services, coupled with predefined network/service topologies, the robustness of the IP/MPLS networks, and the MEF standardization, made the task of WAN assurance and operations a relatively straightforward exercise for CSPs. Broadly, CSPs use the following approaches to assure WAN services:

- Monitor the performance and health of network appliances using multi-vendor network monitoring tools to identify and report device faults, performance, and availability issues. Various health and usage metrics such as bandwidth, disc, memory, CPU, traffic trends, power, and uptime data are collected and reported for further action.
- Monitor QoS KPIs such as jitter, latency, and packet loss to identify and report SLA violations. Enterprise customers request SLA reports to ensure CSP compliance with the contracted terms and demand hefty fines for SLA violations. CSPs and enterprises have used Ethernet demarcation devices such as a network interface device (NID) to perform integrated functions of monitoring and optimizing traffic, and for other activities related to the administration and maintenance of Ethernet operations.
- Perform standards-based test and turn-up testing (RFC 2544/Y.1564) of WAN services to ensure they are accurately provisioned. Conduct active testing (TWAMP/Y.1731) periodically to identify any QoS performance degradations. In cases where performance issues are detected, further on-demand active tests are triggered for troubleshooting and problem isolation. Some of this functionality is integrated in the NIDs, but CSPs have increasingly gravitated towards independent active probes to perform these functions.

In addition, enterprises use a plethora of application performance tools to monitor and identify how network performance affects the application experience, and to isolate application and network issues for further troubleshooting.

4. Application performance-led unified service assurance approach is key to multi-cloud success

With the emergence of SD-WAN for dynamic WAN connectivity and uCPE for virtual branch networks, CSPs must reconsider how they approach service assurance. The prevalent assurance technologies which were designed to primarily monitor the network performance of static WAN networks are not fit for purpose to support enterprises moving to multi-cloud environments. CSPs must look at service assurance for multi-cloud as an end-to-end challenge underpinned by the need to deliver optimum application performance at costs considerably lower than current levels. In this context, CSPs should consider a new, multi-pronged approach to assurance for multi-cloud, as discussed in the following sections.

4.1 End-to-end single pane visibility into application and network performance using virtual probes

In multi-cloud environments, applications and workloads will be distributed across various cloud environments and will likely move between environments on short notice. Service assurance systems must provide a correlated view of the application performance and the hybrid WAN (SD-WAN and IP/MPLS) network performance. The solution must provide detailed analysis of how network performance affects application performance, so operations can rapidly isolate issues and take remediation actions. The solution must demonstrate the following capabilities:

- Provide a near real-time and highly granular view of application and network performance to identify micro trends in performance degradation and take pre-emptive action even before customers experience the degradation. This can be a crucial differentiator for CSPs looking to position their managed services in the highly competitive market that is enterprise business services.
- 'Shadow' the applications as they move around the multi-cloud environment, and closely track the network path that the application traffic is traversing to obtain the most accurate end-to-end performance view. The assurance system must work with the SD-WAN controller and the orchestrator in a closed-loop manner to (a) obtain real-time information on the service chains within the uCPE and the chosen dynamic paths, and (b) provide performance intelligence to the controller and orchestrator to proactively trigger remediation actions to prevent service degradation.
- Provide real-time reporting capability so enterprises can instantly view the key service performance metrics. Enterprises demand such reporting capability as part of the managed services engagement, and CSPs can monetize this capability by charging a fee. Furthermore, CSPs should aim to expose the same real-time reporting capabilities to their own operations teams responsible for delivering on the managed services. Knowing that the CSP has the same view of service performance as the enterprise provides complete transparency and improves customer trust. CSPs can use a network analytics platform that can centrally perform the aggregation and correlation of the network and application performance data, deliver the reporting capabilities for operations and paying customers, and use advanced analytics capabilities such as machine learning to predict service quality degradations.
- Monitor the hybrid-WAN environment encompassing the SD-WAN overlay and the IP/MPLS underlay to provide a comprehensive view of network performance.

To address the end-to-end challenge, CSPs have a variety of monitoring approaches to choose from. For example, they can take a best-of-breed approach by deploying different tools for NPM, APM, end-user

experience and fault monitoring to name a few. This has its advantages, such as providing the best-in-class capability in each area. However, this will require some level of integration and correlation to obtain an accurate end-to-end view. Even when they opt for a unified monitoring solution, CSPs can either choose a top-down monitoring approach (e.g. based on NetFlow, IPFIX, SFlow data) enriched with packet-level data, or a bottom-up packet-based monitoring approach using virtual passive probing technology enriched with NetFlow-type data, with both approaches offering their own benefits.

While evaluating solutions for unified performance monitoring, CSPs should consider the virtual probes-based monitoring solution. At a fraction of the cost of traditional appliance-based probes, software-based virtual probes are flexible, scale better, and provide a high-definition view of application and network performance at a packet level, which can then be correlated and enriched with active testing data (see Section 4.2) to obtain a unified view across the multi-cloud environment, including the SD-WAN network, and the uCPE infrastructure (see Section 4.3) in the branch.

4.2 Dynamic active testing of the agile network and applications

Active testing provides a whole other dimension of assurance and confidence to CSPs and enterprises. However, the active testing solutions must evolve with new capabilities to support the dynamic nature of SD-WAN, uCPE, and agile applications in the multi-cloud environment. CSPs must:

- Deploy independent active testing technology to perform test and turn-up on demand. Services such as SD-WAN and other business services are most likely to be ordered via a self-service interface by the customer. Tests must be performed at the end of the provisioning process to validate service configuration, performance and QoS, before the service is made live and handed over to the customer. Similarly, active tests must also be performed to validate service configuration changes as well as during the troubleshooting process. The key difference between active testing for dynamic WAN and static WAN services is that, in the case of dynamic WAN, active test solutions provide software control, so they can be triggered and executed in near real time and should become an integral part of the orchestration process.

- Perform ongoing active tests on the applications hosted in the various cloud environments to ascertain their availability and performance. Particularly, CSPs must focus on the applications in the public cloud and SaaS environments because the cloud service provider hosting the applications provides a limited set of native tools for monitoring, so CSPs may need to supplement them with their own tools. Furthermore, by simulating the user traffic accessing the applications on the SD-WAN selected paths, CSPs can gain proactive insights on application performance for the chosen network paths. This can also help identify blind spots and congestion points in the network with respect to specific application types in relation to providing an extra layer of performance insights for remediation and troubleshooting.

The active tests have been traditionally performed using appliance-based active probes with proprietary hardware and interfaces. Much like the CSP networks and passive probes, new-age active probes have evolved to software functions running on commodity hardware. The combination of virtual passive probes and virtual active probes provides a rich and rounded set of performance data for troubleshooting.

4.3 Assuring the uCPE infrastructure

uCPE platforms tremendously simplify the branch network with standardized cloud-based infrastructure, offering great flexibility and dynamicity for CSPs and enterprises. However, assuring the uCPE platforms is going to be essential to guarantee network and application performance. Performance degradations of the VNFs

hosted in the uCPE environment or the underlying virtualized infrastructure will have a catastrophic effect on the overall service performance. Therefore, CSPs must:

- Monitor the performance of the uCPE infrastructure to ensure availability of resource capacity to support the VNFs running in the environment. CSPs must use the platform telemetry feeds, events and other data points to develop a comprehensive view of the infrastructure performance. To achieve this level of monitoring, the assurance solution must capture data points from the virtualization layer (hypervisor) and the management layer (virtual infrastructure manager), which in most cases are likely to be OpenStack or VMWare, or both.
- Monitor the health of the VNFs (e.g. SD-WAN VNF) to identify performance issues. It is likely that the SD-WAN vendor will provide native monitoring and analytics capability along with the core solution, so CSPs may not need additional assurance capability for day 1 operations. However, CSPs will end up with another set of siloed monitoring tools and swivel chair operations. In the long run, as CSPs push for standardization of VNF management interfaces, an independent assurance and reporting solution may be more viable.
- Integrate infrastructure monitoring with the overall application and network performance monitoring to gain a unified view encompassing the underlying uCPE infrastructure and VNFs, the hybrid WAN performance (SD-WAN overlay, IP/MPLS underlay), and the application performance.
- Consider an independent assurance and monitoring solution to monitor the uCPE platforms. CSPs have traditionally used vendor-independent solutions to give them an unbiased view of performance issues. The need for such solutions will likely be even more important because of the high level of VNF vendor diversity expected in the uCPE platforms, with the CSPs allowing the enterprises to pick and choose the vendors they want deployed. The monitoring solution must provide assurance across the entire service chain of multi-vendor VNFs, potentially using a passive probe VNF, which allows CSPs offering a managed service to remotely manage and troubleshoot problems, reduce MTTR, reduce truck rolls, and improve overall customer satisfaction.

5. Conclusion and recommendations

Enterprises moving to multi-cloud environments need agile WAN connectivity and agile branch networks to achieve the intended application agility. To satisfy this emerging demand, CSPs are launching managed SD-WAN services based on virtualized uCPE platforms providing high levels of flexibility and software-based control to enterprises. The CSPs' success in delivering these services, and ultimately the success of the enterprises' multi-cloud strategy, will hinge on the CSPs' ability to guarantee application and network performance in the dynamic network and cloud environments.

Traditional assurance solutions are not entirely fit for purpose as they were intended for rigid WAN services, with a siloed approach for monitoring the device, network and application performance. CSPs must take a fresh approach to assurance for multi-cloud environments, and should consider the following capabilities when choosing a service assurance solution:

- Take an end-to-end view of the service performance, encompassing the applications (hosted in the various cloud environments), the dynamic WAN (SD-WAN and IP/MPLS), and the enabling infrastructure (uCPE).

- Consider an independent assurance solution, such as a unified assurance solution based on virtual passive probes, when evaluating end-to-end monitoring approaches for multi-cloud environments, providing highly granular insights on the application and network performance in the context of the chosen WAN paths to identify signs of performance degradation. Enrich the performance data with the uCPE infrastructure performance to obtain an end-to-end performance view, encompassing the service, network, and infrastructure.
- Consider new-age virtual active testing technology that can support: (a) test and turn-up of the SD-WAN services, and other WAN services hosted on the uCPE, (b) periodic active tests to proactively monitor the network performance of the dynamic SD-WAN traffic flows, (c) on-demand active tests triggered for troubleshooting and fault isolation, and (d) active tests against the applications hosted in the various cloud environments (public, private or SaaS) to identify any issues of availability, latency, responsiveness, and most importantly, the end user experience.
- Bolster the overall efficacy of multi-cloud assurance by correlating the virtual passive and active performance data, within a network analytics platform, generating rich insights for troubleshooting and guided actions for issue resolution, as well as applying machine learning to predict service quality degradations. Additionally, use the analytics platform to provide value-added services such as performance reports, enabling CSPs to monetize their investments, deliver superior customer experience, and satisfy the enterprise's customer requirements.

About the author

Anil Rao (Principal Analyst) is the lead analyst for the Automated Assurance and Service design and Orchestration research programs, covering a broad range of topics on the existing and new-age operational systems that will power telcos' digital transformation. His main areas of focus include service creation, provisioning, and service operations in NFV/SDN-based networks, 5G, IoT, and edge clouds; the use of analytics, ML and AI to increase operations efficiency and agility; and the broader imperatives around operations automation and zero-touch networks. In addition to producing both quantitative and qualitative research for both programs, Anil also works with clients on a range of consulting engagements such as strategy assessment and advisory, market sizing, competitive analysis and market positioning, and marketing support through thought-leadership collateral. Anil is also a frequent speaker and chair at industry events. He holds a BEng in Computer Science from the University of Mysore and an MBA from Lancaster University Management School, UK.

This white paper was commissioned by Netscout Systems. Analysys Mason does not endorse any of the vendor's products or services.

Published by Analysys Mason Limited • Bush House • North West Wing • Aldwych • London • WC2B 4PJ • UK
Tel: +44 (0)20 7395 9000 • Email: research@analysysmason.com • www.analysysmason.com/research

Registered in England No. 5177472

Analysys Mason's consulting and research are uniquely positioned

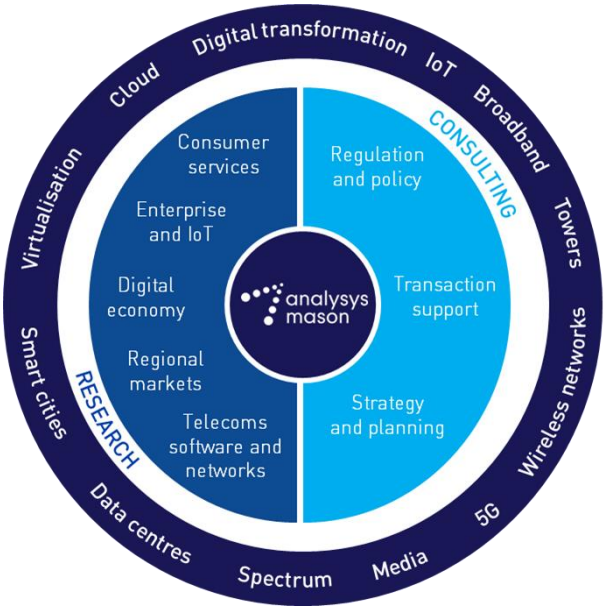
Analysys Mason is a trusted adviser on telecom, technology and media. We work with our clients, including communications service providers (CSPs), regulators and end users to:

- design winning strategies that deliver measurable results
- make informed decisions based on market intelligence and analytical rigor
- develop innovative propositions to gain competitive advantage.

We have around 250 staff in 16 offices and are respected worldwide for the exceptional quality of our work, as well as our independence and flexibility in responding to client needs. For over 30 years, we have been helping clients in more than 110 countries to maximize their opportunities.

Consulting

- We deliver tangible benefits to clients across the telecom industry:
  - communications and digital service providers, vendors, financial and strategic investors, private equity and infrastructure funds, governments, regulators, broadcasters, and service and content providers.
- Our sector specialists understand the distinct local challenges facing clients, in addition to the wider effects of global forces.
- We are future-focused and help clients understand the challenges and opportunities that new technology brings.



Research

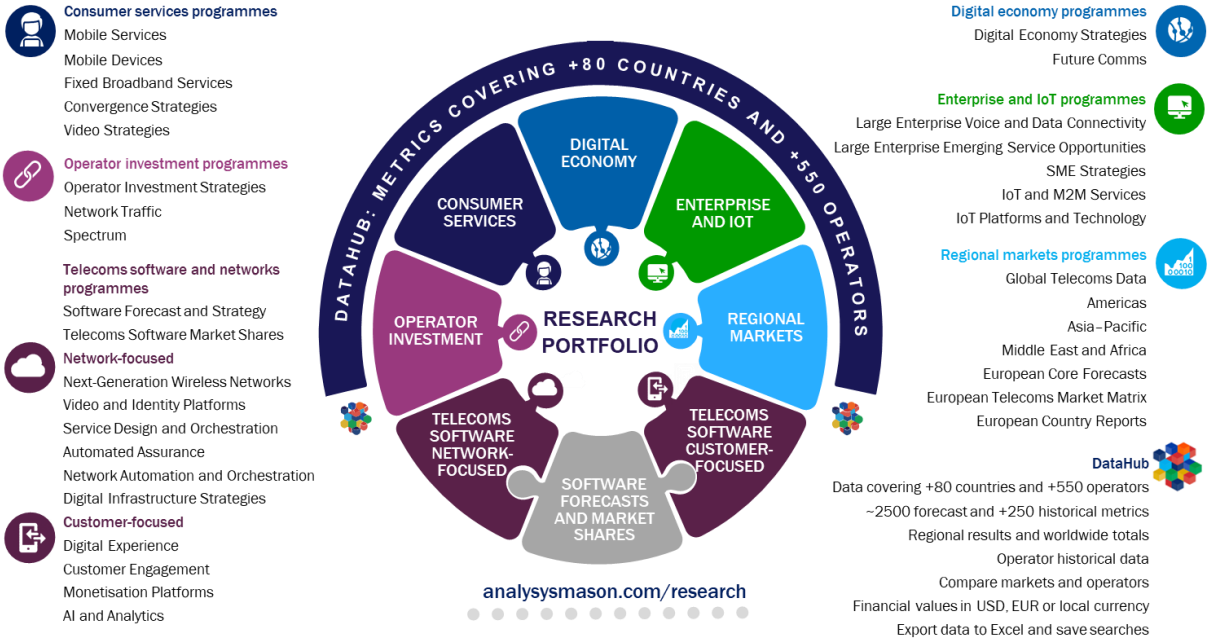
- Our dedicated team of analysts track and forecast the different services accessed by consumers and enterprises.
- We offer detailed insight into the software, infrastructure and technology delivering those services.
- Clients benefit from regular and timely intelligence, and direct access to analysts.

Research from Analysys Mason

We provide dedicated coverage of developments in the telecom, media and technology (TMT) sectors, through a range of research programs that focus on different services and regions of the world

The division consists of a specialized team of analysts, who provide dedicated coverage of TMT issues and trends. Our experts understand not only the complexities of the TMT sectors, but the unique challenges of companies, regulators and other stakeholders operating in such a dynamic industry.

Our subscription research programs cover the following key areas.



Each subscription programme provides a combination of quantitative deliverables, including access to more than 3 million consumer and industry data points, as well as research articles and reports on emerging trends drawn from our library of research and consulting work.

Our custom research service offers in-depth, tailored analysis that addresses specific issues to meet your exact requirements

Alongside our standardized suite of research programs, Analysys Mason's Custom Research team undertakes specialized, bespoke research projects for clients. The dedicated team offers tailored investigations and answers complex questions on markets, competitors and services with customized industry intelligence and insights.

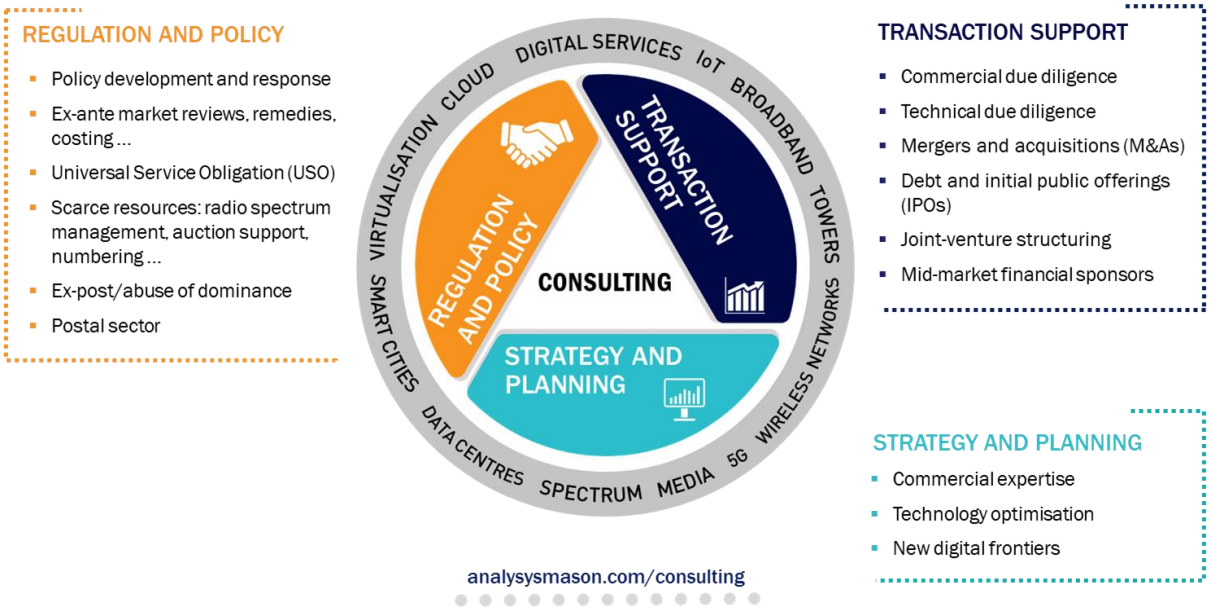
For more information about our research services, please visit www.analysysmason.com/research.

Consulting from Analysys Mason

For more than 30 years, our consultants have been bringing the benefits of applied intelligence to enable clients around the world to make the most of their opportunities

Our clients in the telecom, media and technology (TMT) sectors operate in dynamic markets where change is constant. We help shape their understanding of the future so they can thrive in these demanding conditions. To do that, we have developed rigorous methodologies that deliver real results for clients around the world.

Our focus is exclusively on TMT. We advise clients on regulatory matters, help shape spectrum policy and develop spectrum strategy, support multi-billion dollar investments, advise on operational performance and develop new business strategies. Such projects result in a depth of knowledge and a range of expertise that sets us apart.



We look beyond the obvious to understand a situation from a client's perspective. Most importantly, we never forget that the point of consultancy is to provide appropriate and practical solutions. We help clients solve their most pressing problems, enabling them to go farther, faster and achieve their commercial objectives.

For more information about our consulting services, please visit www.analysysmason.com/consulting.