
spirent
Promise. Assured.
ASSURING THE PROMISE OF HYBRID CLOUD SERVICES
Solution Overview

The Hybrid Cloud Challenge

Cloud-native networks offer tremendous benefits: greater agility, faster release time, shorter time-to-market, lower costs, and the potential for telcos to avoid vendor lock-in. As network providers race to take advantage of clouds, how can they ensure that their services operate as promised and their customers enjoy the superior experience they expect?

In this paper, we look at the trends that are driving these challenges, particularly the move to hybrid clouds, and examine how test and assurance needs to evolve to support the agile new services running on cloud-native networks.

Cloud complexity

Cloud-based networks today are rarely monolithic. New services, particularly those that use 5G and SD-WAN technologies, as well as many applications, span a mix of cloud environments—edge clouds, private telco clouds, and increasingly, public clouds.

Private telco clouds are gaining traction, as telcos invest in cloud-native networks in order to bring down the cost of running networks and services and avoid vendor lock-in. To gain consistency between their data centers and the edge in their private clouds, network providers are evolving from virtual network functions (VNFs) on virtual machines (VMs) to Containerized Network Functions (CNFs).

What is a Hybrid Cloud?

Hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud, and third-party, public cloud services with orchestration between the two platforms.

Public clouds offer an increasingly attractive alternative for Communication Service Providers (CSPs). We're seeing growing partnerships between service providers such as AT&T and Verizon and public cloud providers including Amazon Web Services (AWS), Google Cloud (GCP)[1], and Microsoft Azure.[2] These cloud providers are connecting their services directly to the 5G networks in the carrier's data center. As carrier networks connect with public clouds, the public cloud edge is moving closer to the end customer. We'll also start to see private clouds being built on public cloud infrastructure.

Edge clouds are where we see this happening the most. Edge clouds can be closer to the customer, thereby enabling low latency and edge processing that are essential for new 5G services and the business applications that 5G enables. But as business applications migrate to the cloud, reliability, and performance are even more critical.

User demand is driving development.

Network providers have long enjoyed the luxury of building their services from the ground up, over several months. No longer. User demand for superior experiences is driving everything from the top. A joint Intel and Ovum report predicts that experiences enabled by 5G deployments will account for $1.3 trillion in cumulative revenue by 2028.[3] Carriers are innovating new ways to respond to user demands in real time, enabled by service agility that is now made possible.

1. Lardinois, F. (2020, March 5). Google Cloud goes after the telco business with Anthos for Telecom and its Global Mobile Edge Cloud. Retrieved June 2, 2020, from https://techcrunch.com/2020/03/05/google-cloud-goes-after-the-telco-business-with-anthos-for-telecom-and-its-global-mobile-edge-cloud/
2. Khalidi, Y. (2020, March 31). Microsoft partners with the industry to unlock new 5G scenarios with Azure Edge Zones. Retrieved June 2, 2020, from https://azure.microsoft.com/en-us/blog/microsoft-partners-with-the-industry-to-unlock-new-5g-scenarios-with-azure-edge-zones/
3. Gallagher, R., Schoolar, D., de Renesse, R., & Barton, E. (2018). How 5G Will Transform The Business Of Media & Entertainment. Ovum. Retrieved from https://www.omdia.com/resources/product-content/intel-5g-ebook

The future is here. Are network providers ready?

5G will unlock a raft of new applications: IoT, process management, building controls, and utility metering for enterprise; and augmented reality (AR) and virtual reality (VR), immersive haptic and 3D holographic experiences for consumers. 5G is changing the traditional media and entertainment—and, with them, service provider models. In order for these new models to succeed and this glittering future to be achieved, though, network providers must address some important infrastructure and security issues.

The problem with telco clouds

In the past, traditional network functions such as an MME (Mobility Management Entity) were built on specialized hardware. If there was a problem, the carrier could simply go back to the vendor for a fix. Now, however, in order to achieve the economies of scale for rapid network growth, networks have shifted to interoperability and open disaggregation. Services are composed of network functions from several vendors. And carrier cloud infrastructure might comprise combinations of Network Functions Virtualization Infrastructure (NFVI), Containers, and Container Network Functions (CNF).

As a result, while leveraging the benefits of the cloud network, CSPs also must contend with an increase in failure modes. Untested technologies are being pieced together in telco systems, so carriers are forced to act as system integrators. Moreover, there's considerable VNF (virtual network function) and CNF variability across carrier cloud infrastructure.

"Experiences enabled by 5G deployments will account for $1.3 trillion in cumulative revenue by 2028."—OVUM Report

With everything disaggregated, network providers need to test at every layer. The result is that upgrades and VNF/CNF integration are expensive and slow, a far cry from the ideal vision of agile cloud-native networks.

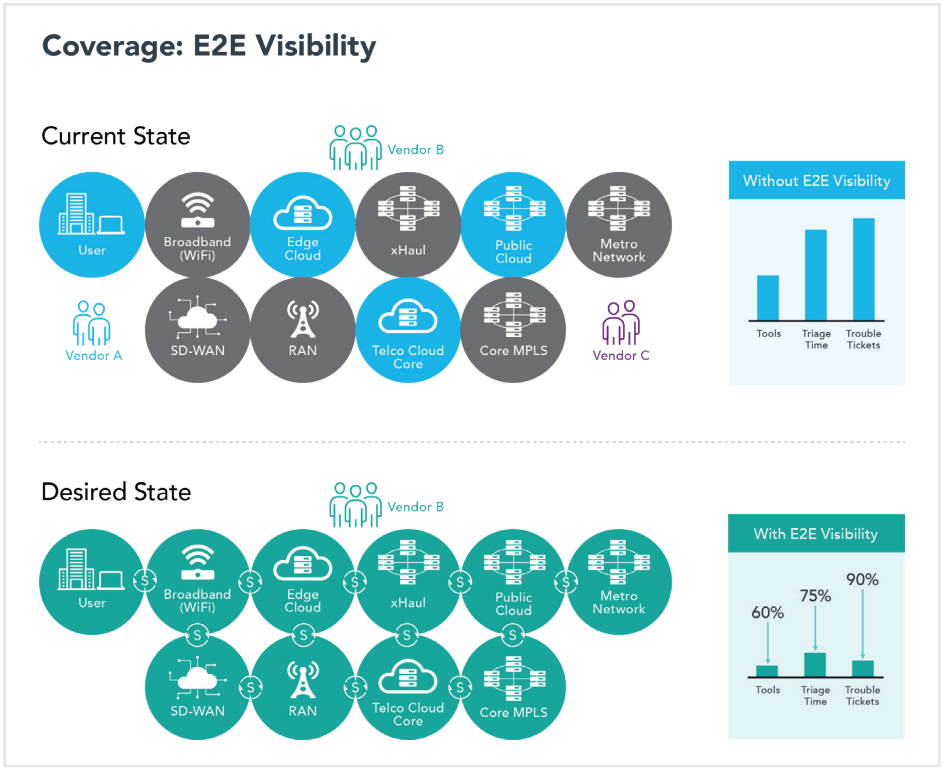
In general, the industry has been sluggish in adopting cloud-native NFV applications. Now, however, customers have higher expectations for service quality than ever before, placing greater demand for performance and reliability on the cloud infrastructure. Operators, in their role as systems integrators, are challenged with advancing cloud technology to meet these requirements to 5-9s reliability, while honoring the time and budget constraints inherent in a mature service rollout.

A new security approach is needed

The network security paradigm is changing, too. In the cloud network, traffic flows don't necessarily pass through a perimeter which serves as a location for security controls. In response, new means for achieving the desired security controls are evolving. For example, networks are shifting to distributed models with security localized and optimized to protect the resource.

All of this leads to a new attitude towards building the network. Expectations are now top-down: We say, "I want this service and the network needs to support it," rather than building networks from the ground up. Telcos are now adopting continuous integration and continuous delivery (CI/CD) practices, converging labs and live networks. This is not a new concept: Cloud providers faced the same agility problem long ago using automated deployment engines—Amazon's Apollo deployment engine, for example, makes more than one deployment per second. For telcos, the solution requires integrating new tools such as 5G, SD-WAN, Security, and NFVI testing.

Assuring Hybrid Cloud-based Services



Spirent has test and assurance solutions to address the complexities of the hybrid cloud network and to ensure that these new hybrid cloud-based services deliver on their performance and security promises. Spirent's solutions have three main components:

- Visibility of service performance and security efficacy
- Automation of assurance processes
- Analytics to drive closed-loop action

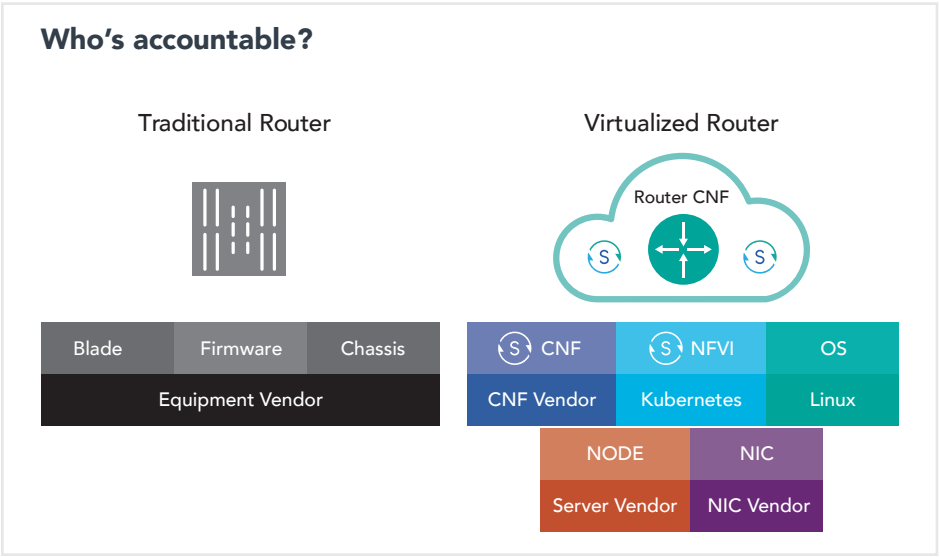
Visibility

To gain visibility in cloud-native networks, testing must approach network functions from two aspects: horizontal and vertical. Spirent provides end-to-end visibility in both directions.

Horizontal visibility

Is the network supporting the SLAs (service-level agreements)? What is the end-user experience? To answer these questions, we must first test each segment or domain individually (RAN, edge clouds, core) and then assess the end-to-end service performance across segments, including the hybrid clouds. Without this visibility, it could take months to launch a service.

For this testing, Spirent cloud-native test agents can be spun-up at key points in each of these segments to test individual functions before they are put into the live network (wrap-around testing), then to make sure the end-to-end service is working as expected.



Security vulnerabilities exist in every area: Internet, Data Center (DC), SD-WAN, Mobile Core infrastructure. Carriers and cloud providers need to validate the infrastructure of security operations, including functions that are inspecting traffic and enforcing policies. Before running live traffic over these services, we use wrap-around testing techniques to create incidences that will trigger these traps and send information to upstream monitoring and SIEM (Security Information and Event Management) systems. The result is end-to-end visibility that includes assessments of performance *and* security concerns.

Once the service is launched, we can rapidly instantiate container-based test agents at various points of the service in order to isolate an issue in real time.

Vertical visibility (up and down the IT stack)

The vertical aspect is one that is a new challenge for carriers as they move towards cloud-native networks. The traditional router has layers that are provided by the same vendor. The new world of cloud-native has layers from different vendors. What's more, the elements of the stack could be swapped out at any time and therefore require constant testing.

Spirent's test and assurance solution isolates the different layers using our container-based test agents and methodology. Our test agents can surround the router CNF to test the function itself, or replace the router CNF, mimicking the load of the router CNF to assess the performance of the infrastructure components. Here, too, being able to instantiate test agents in containers lets you understand if each layer is performing its function well enough to deliver the SLAs needed.

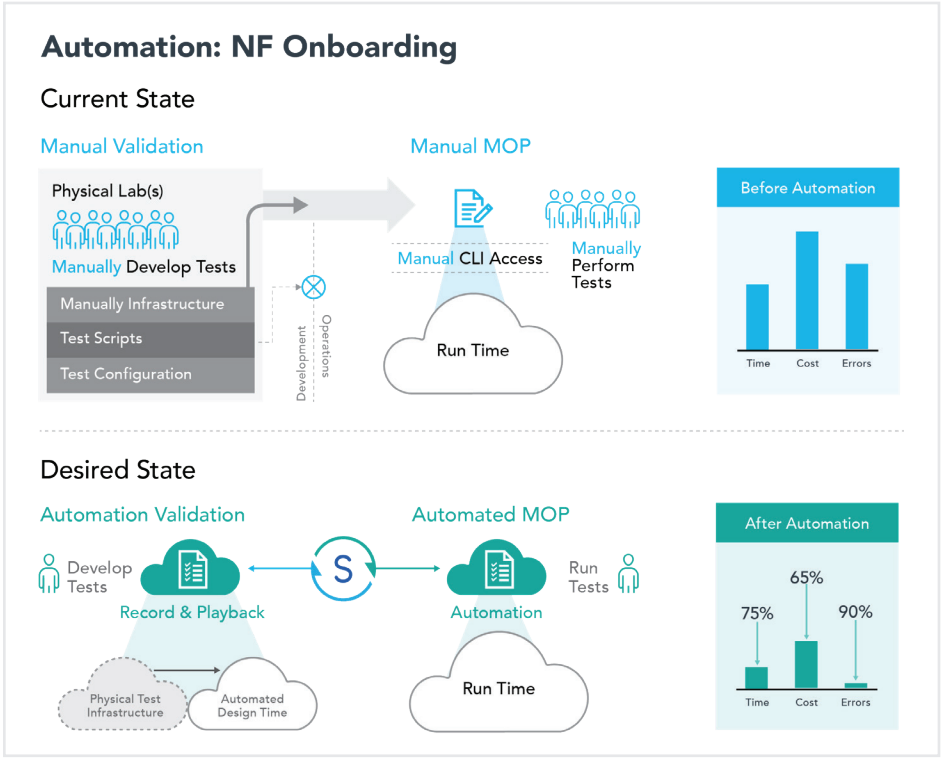
Automating assurance across the lifecycle

Automation is the next important aspect of the solution. Continuous integration, continuous testing, and continuous delivery (CI/CT/CD) methods enable the agility that is a key ingredient for success. The container-based test agents we describe above can be instantiated, used to execute tests, and then removed when testing is complete, as new CNFs/VNFs are integrated, tested, and deployed in the network.

With Spirent's solution, the same tools can be used in a pre-production environment and in production. As many CSPs have implemented automation frameworks, our solution fits seamlessly into carriers' current environments.

Analytics

Analytics is the final piece of the solution. To be successful in the new hybrid cloud environments, CSPs need to address any network issues before they impact customer experience. There needs to be a closed-loop analytics platform that can ingest and understand the performance of the entire hybrid cloud network that is delivering the service to the customer. Spirent's platform leverages ML and AI techniques to tie together all the network data from various sources, proactively predict service degradations, pinpoint root causes, and drive remediation actions. By turning mountains of data into actionable insights, we rapidly reduce mean time to repair (MTTR) and unnecessary escalations.



Conclusion

Spirent's solutions are already enabling CSPs to migrate to the cloud successfully while simplifying the complexity of the hybrid cloud environments. As the figures above illustrate, automating the testing and onboarding of new VNFs from lab-to-live production use led to a 75% reduction in time to deployment and a 90% reduction in errors.

In addition, better visibility into network issues reduced triage time by 75%. And customer escalations were reduced 80% when the analytics identified issues identified earlier than previously possible.

Security, too, is substantially improved. Security infrastructure is hardened as security issues are found and remediated proactively, reducing both time-to-fault visibility and time-to-fault remediation.

The agile, automated testing and assurance solutions we outlined here provide a roadmap for exploiting the advantages of cloud networks while navigating the complexities of the hybrid cloud environment in the race to deliver a secure, quality experience to customers.