WHITE PAPER

The Power of Proactive

Active Assurance Use Cases

KEYSIGHT

We need a fundamental shift in our approach to assuring the network. The network is moving to the cloud. Functions are now virtualized. And next-gen networks are too dynamic for manual troubleshooting to handle. There is a compelling argument for employing Active Assurance in tandem with Passive Assurance. As 5G and SD-WAN drive us to adopt virtualization, Active Assurance will be a critical enabler of the automation needed to successfully ensure differentiated performance and quality for these next-gen services.

Active Plus Passive Assurance: Getting the Best of Both Worlds

Passive Assurance is the traditional method for determining the health of the network. It collects data from virtual or physical network functions and other sources once the function, slice, or service is up and running. Passive Assurance is good for identifying severe, customer-impacting problems as traffic runs through the network. But, as we pointed out in a previous paper, Passive Assurance has its limitations when it comes to turn-up, monitoring, and troubleshooting.

Active Assurance fills the gaps left by Passive Assurance by emulating network functions, devices, and users to create highly realistic synthetic traffic (via virtual test agents, or VTAs). Active Assurance inserts this synthetic traffic across the end-to-end network and evaluates performance, making it ideal for pinpointing the root cause of a problem. It enables service providers to evaluate performance at turn-up, check critical services and links regardless of traffic levels, proactively identify issues by using defined traffic so minor fluctuations are discernable, and isolate problems anywhere in the network cost effectively. This makes Active Assurance ideal for when the service provider first turns up a function, makes a change to a function, wants to ensure a public safety network is functioning properly, or needs to isolate a complex problem.

Passive Assurance is ideal to:

- Monitor performance once the network is up and running.
- Track services and links that have consistent traffic flows.
- Detect issues in high-priority parts of the network.
- Determine how many users are impacted by these issues.

Active Assurance lets you:

- Evaluate performance at turn-up before customer usage starts.
- Continuously check services and links even when traffic levels are low.
- Proactively identify issues before they become major problems.
- Troubleshoot complex issues in any part of the network, including customer premises and over-the-air (OTA)/RF.

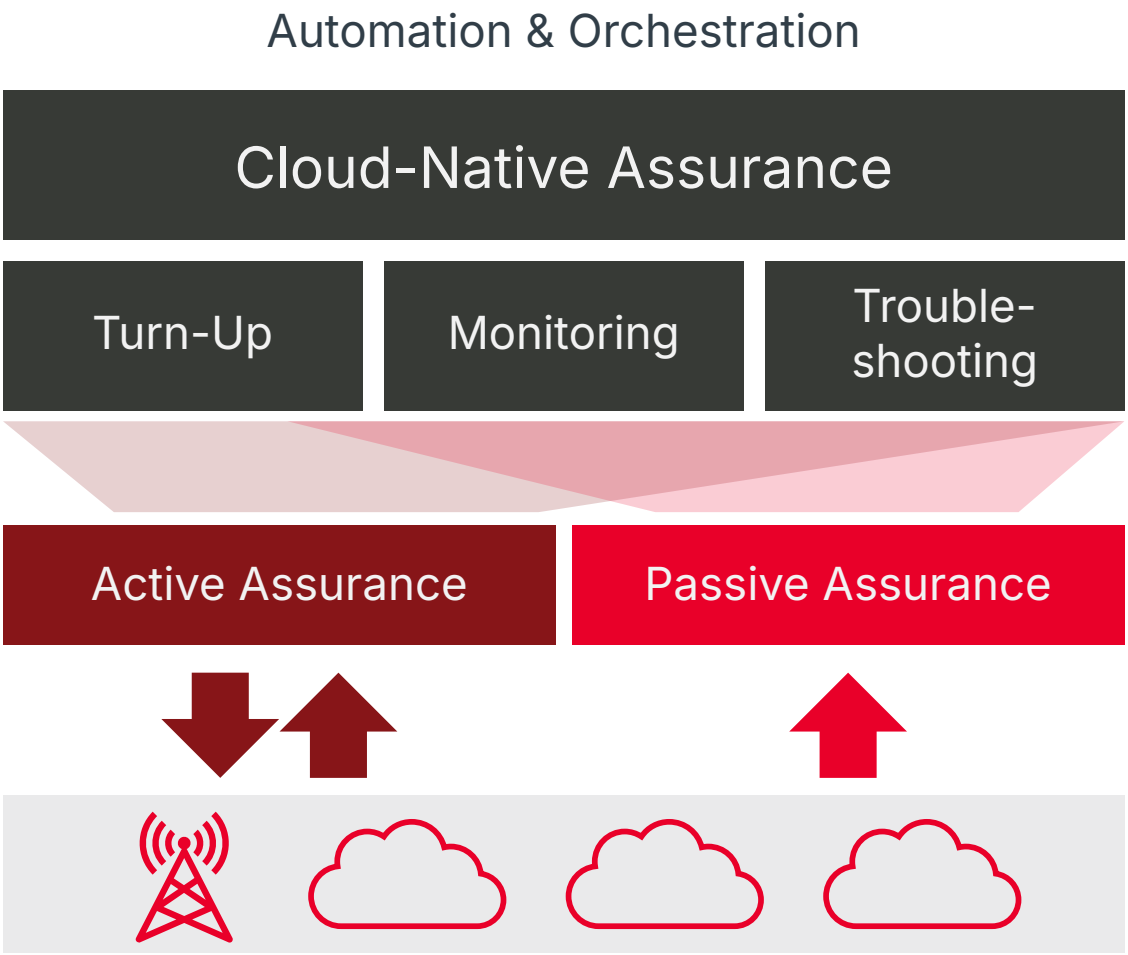

Figure 1. Active plus Passive Assurance provides the tools for comprehensive automation of turn-up, monitoring, and troubleshooting

To fully grasp the benefits — and necessity — of Active Assurance in a real-world context, it would help to examine several specific examples. The following examples are based on our experience implementing assurance in a wide variety of networks and environments for both fixed and mobile service providers:

- Turn-up, monitoring, and troubleshooting for 5G slicing
- Turn-up, monitoring, and troubleshooting for SD-WAN
- Monitoring of an IP mesh network
- Turn-up and change management of LTE mobile networks

Use Case: Active Assurance for 5G Slicing

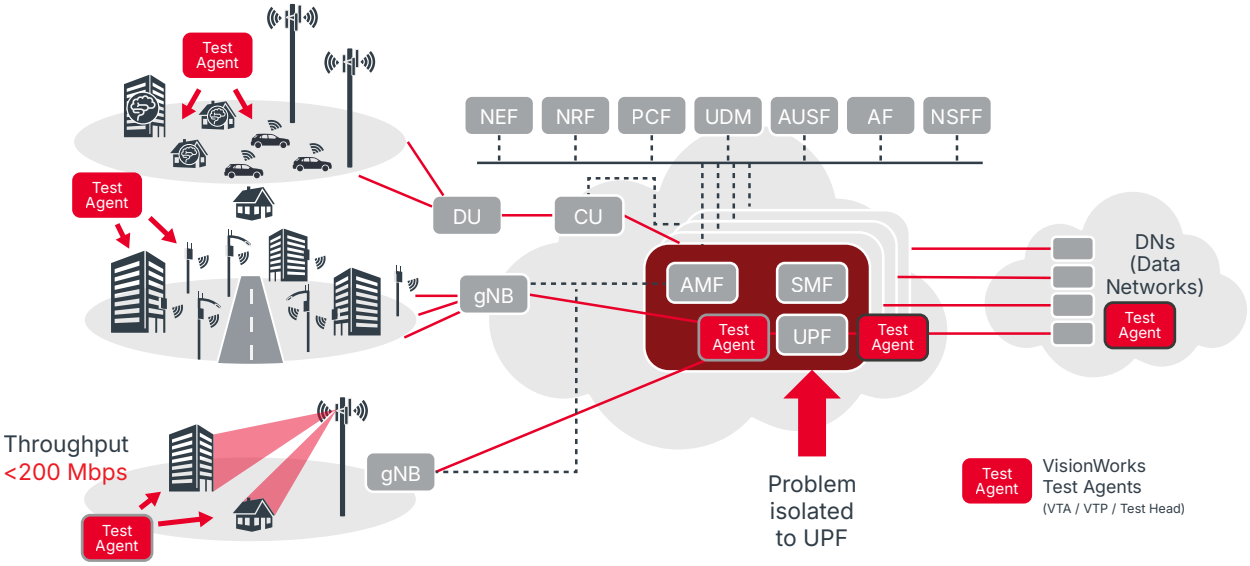

Figure 2. End-to-end slice monitoring and troubleshooting for 5G

Expectations have been set that 5G will be a complete game changer. So, the stakes are higher than ever for operators to deliver differentiated experiences and guaranteed quality for a range of new applications, from connected vehicles to IoT sensors and beyond. To this end, 5G revolutionizes network slicing with improved control over end-to-end performance and enhanced scalability to support the deployment of large numbers of slices. However, the potential for a multitude of slices, each with differentiated performance expectations, creates real challenges for assurance.

To ensure customer expectations are met, you want to be certain that each slice is delivering the service desired and meets all SLAs as it is turned up and before it goes live. And after turn-up, you want to continuously monitor the slices based on a "birth certificate" or benchmark, established at the start.

In the example illustrated here, a test agent deployed at the end user's premises continuously tests the 5G Fixed Wireless Access network using small amounts of synthetic user traffic. Consider a hypothetical scenario where the test agent experiences a reduction of throughput, dropping down to 200 Mbps from the expected 300 Mbps. By instantiating virtual test agents (VTAs) at strategic points in the network and inserting synthetic traffic in each location, we can test across all of the segments in the end-to-end service delivery path and rapidly isolate the problem.

In this example, everything from the UPF in the core network to the data networks is "green," or operating correctly. From the premises to the UPF, however, test agents report errors including the on-premises agent. The problem, therefore, is isolated to the UPF, its infrastructure, and the associated network connections. We can then find the root cause so it can be fixed before the customer notices a service disruption and before any SLAs are violated. Once the fix is implemented to the UPF, we can test the new UPF before it goes live, ensuring the problem is truly fixed.

Because it is dependent on actual user traffic, Passive Assurance, in contrast, has a limited ability to detect performance issues that occur during periods when usage is low, such as the middle of the night. In addition, after the turn-up of a new UPF, Passive Assurance is not able to assess the UPF before it goes live. And while Passive Assurance can monitor latency, jitter, and packet loss for the user-plane, due to the high cost of decryption, it is not cost effective to directly examine user-plane packets, so quality measures such as Mean Opinion Score (MOS) are statistical estimates. Active Assurance inserts known synthetic traffic into the network and directly measures performance and perceptual quality (MOS) of user-plane packets at endpoints and across each network segment.

Use Case: Active Assurance for SD-WAN

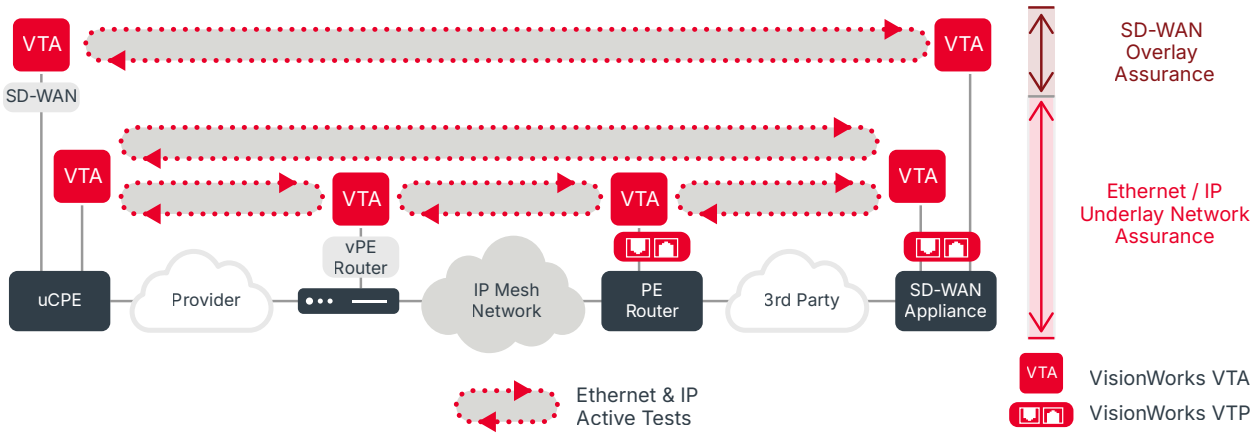

Figure 3. Turn-up, monitoring and troubleshooting of underlay and overlay for SD-WAN

SD-WAN is a multi-layered service delivery challenge. Consider an individual store that is part of a multi-national chain. Its network connection to another store is illustrated above. One store has a uCPE with a virtualized SD-WAN function providing access to the other store which uses an SD-WAN appliance with integrated hardware and software.

As you can see, the network includes an SD-WAN overlay supported by an Ethernet/IP underlay which includes both own-network and third-party access and an IP mesh network. We need to assure the network end to end (from one store to another) and also need the ability to segment out each part of the underlay network including parts not owned by the SD-WAN provider. Consider, too, that SD-WAN service providers may implement multi-vendor networks with a variety of on-premises configurations such as the uCPE and SD-WAN appliance options mentioned above. In addition, the underlay network may cross multiple providers, each with different vendors and virtual and physical routers. You would need to be able to test all of this to reliably and efficiently assure services including rapid isolation of issues.

To summarize, a comprehensive SD-WAN assurance approach requires visibility across five different dimensions:

1. Network location (premises, access networks, IP mesh networks)
2. Service provider — own-network and third-party networks
3. Network stack and layers — Ethernet and IP for the overlay and underlay
4. Infrastructure type — virtual, physical and hybrid
5. Multiple vendors

Active Assurance is the one approach that allows you to verify performance from all these angles, up the stack, and across the network end to end, to make sure everything is working properly. As the diagram below illustrates (Figure 4), Active Assurance enables you to put VTAs at each end to test performance on each layer and through every connection — including the Provider's network, IP mesh network, and third-party cloud — from the store's uCPE to the other store's SD-WAN appliance.

Active Assurance is uniquely suited to the SD-WAN use case because it provides the needed assurance at turn-up, when there is no traffic in the network, for continuous monitoring, and for troubleshooting when issues arise.

Use Case: Active Assurance for IP Mesh Networks

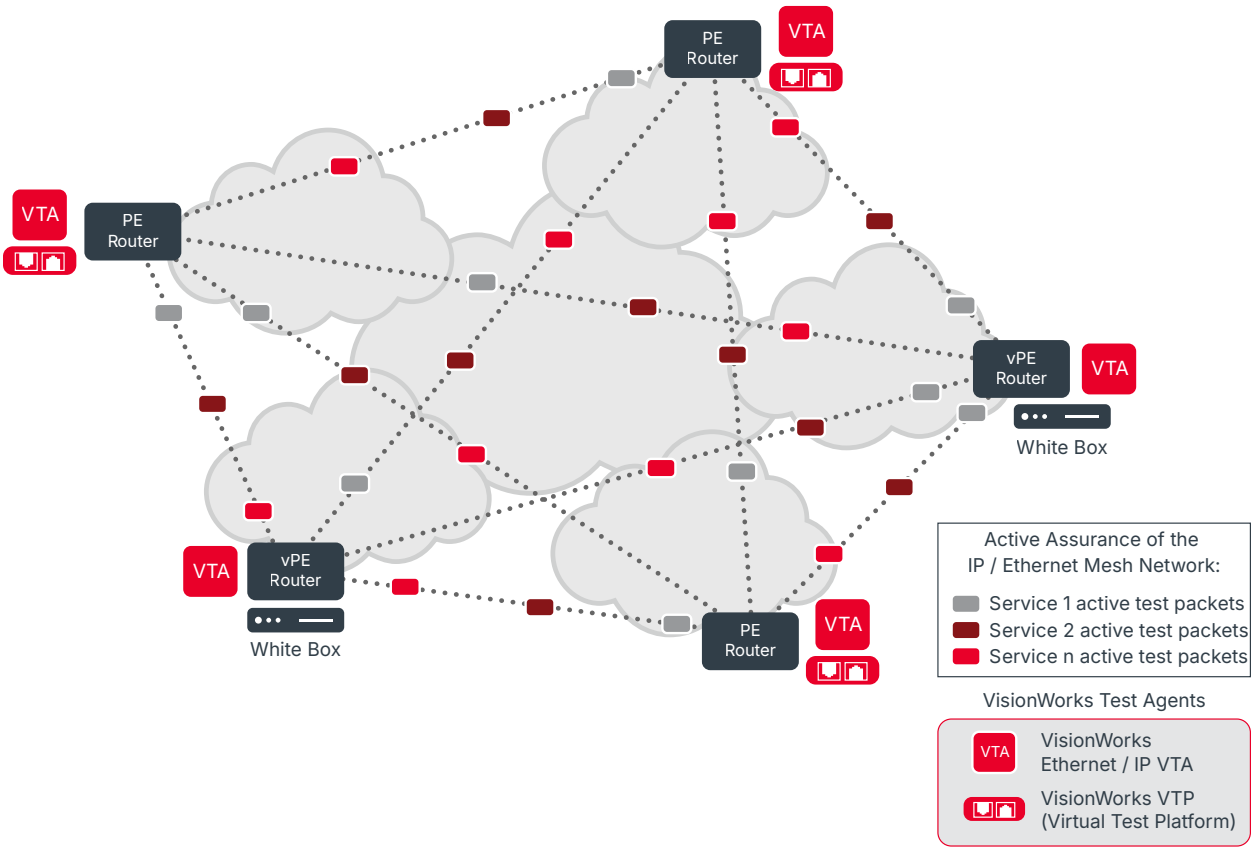

Figure 4. IP mesh performance monitoring using Virtual Test Agents (VTAs) deployed at physical and virtual PE routers

In our previous use case, there was an IP mesh network between the white box running a virtual router (vPE) and the third-party cloud network. Let us now focus in on this IP mesh network, which presents its own very special use case for Active Assurance.

The IP mesh network sits on the back end of the overall network, connecting regional networks to customers. As a service provider, you may not actually "own" all of these regional networks; in fact, many of the clouds depicted in the IP mesh above might belong to third parties. If anything goes wrong, you have no visibility into what is happening in those third-party networks. So how can you get this visibility? Passive testing is obviously not an option!

The solution is Active Assurance — using virtual test agents (VTAs) to test across the third-party network. By deploying a VTA at the locations where you have a physical (PE) or virtual (vPE) router, you can insert active test packets to test the Ethernet and IP protocol layers and the different services to understand how the customer is experiencing each service across all the layers.

Use Case: Active Assurance for Virtual EPC/IMS

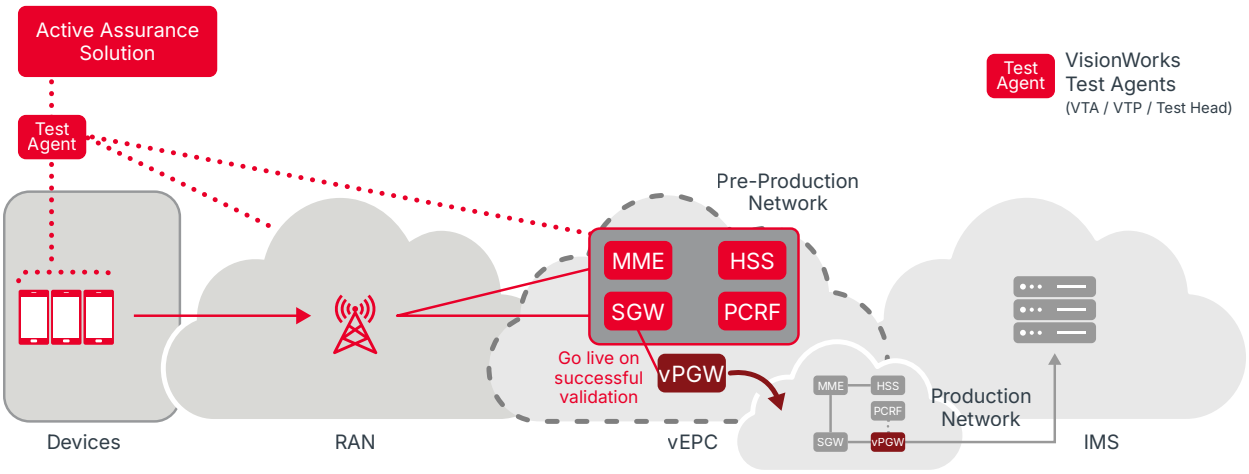

Figure 5. vPGW turn-up validation/change management

For an LTE core network, validation at turn-up and when changes are made is critical. Since the validation needs to happen before going live, Passive Assurance is not helpful. Active Assurance is the only solution.

The diagram above (Figure 5) illustrates a typical use case involving a virtualized EPC (vEPC). For our example, let us posit that there was a problem with the vPGW function or that the vPGW was upgraded to improve performance. We cannot risk just flipping the switch and moving the new vPGW into the live network — first we need to validate it in a pre-production environment. By definition, the pre-production/offline network does not have any live users, so we need to generate synthetic traffic that mimics realistic usage and then assess performance.

An Active Assurance approach allows us to surround the vPGW (in dark orange on the diagram) with Test Agents that emulate user devices, the RAN, and other functions that are part of an LTE core network. We can then perform wrap-around tests that isolate the vPGW and after this

progress to end-to-end tests which assess the performance of the vPGW when integrated with other real (non-emulated) infrastructure. Once it is successfully validated, the vPGW can go live and start taking traffic and supporting live users. If this is an upgrade, we would test before the change is made to create a benchmark, and then compare against this benchmark as part of validating readiness to go live.

In addition to Test Agents, an Active Assurance approach includes Controller and Analytics components which manage the Test Agents and aggregate and analyze validation of test results. These components link to orchestration and network management functions so that validation can be performed as part of automated workflows for network function turn-up and change management.

A Keysight Solution for Every Use Case

Keysight Assurance Solutions

These are just four compelling use cases where Active Assurance provides solutions that are not possible with traditional, passive approaches. You may think of many others pertinent to your business — business Ethernet services and cellular backhaul come to mind. For all of these, Keysight Service Assurance Solutions have been proven to ensure performance and quickly resolve complex end-to-end issues.

Keysight solutions perform active testing from both outside and inside the network, supporting end-to-end testing as well as segment testing of access, backhaul, core, and data center networks. They combine active test agents and intelligent analytics to provide actionable results to network operations teams and automated systems. They are cloud-native, ready to be integrated with new cloud and automation platforms that service providers are building. With open interfaces, they are also designed to easily integrate with legacy systems.

Keysight solutions do not just support Active Assurance. They also deliver a rich array of Passive Assurance capabilities based on customer and network data sources including telemetry, performance counters, and much more. Our Passive Assurance solutions have been proven in deployments for some of the largest networks on the planet — processing billions of transactions each day. Bringing together Active and Passive Assurance in one platform enables comprehensive automation of turn-up, troubleshooting, and monitoring — with a unique ability to “close the loop” and deliver full automation of troubleshooting workflows.

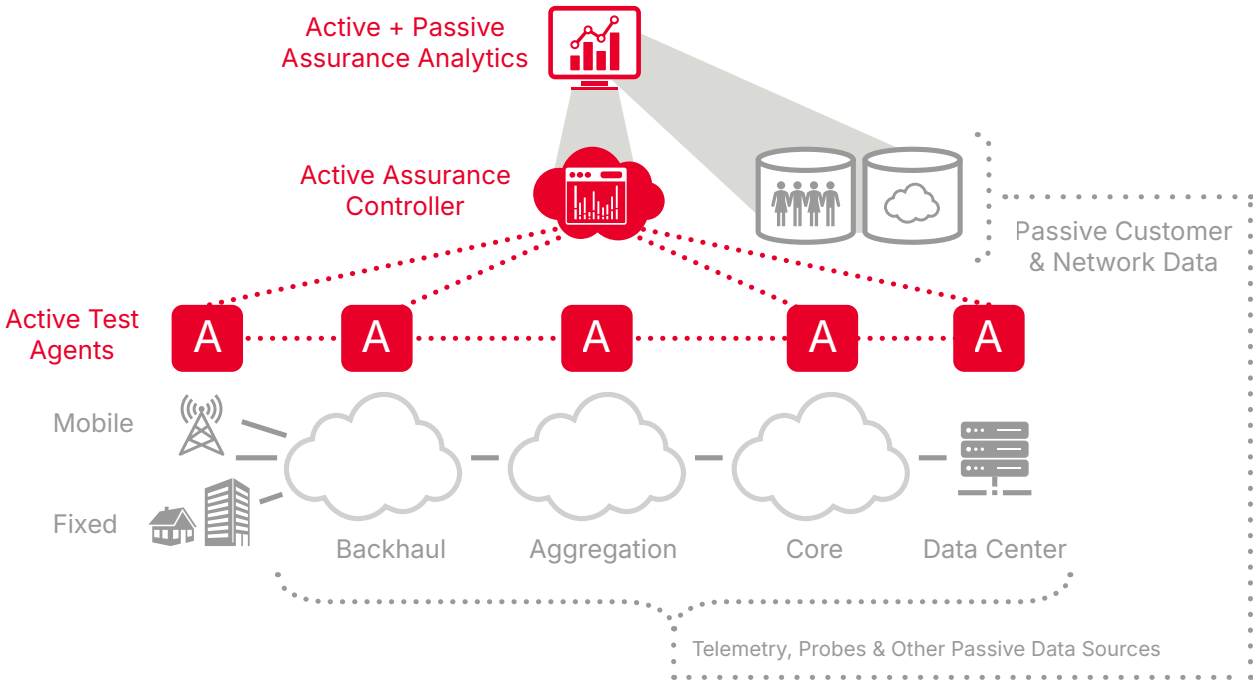

Figure 6. Keysight Active and Passive Assurance Solutions

From Turn-Up to Troubleshooting, Test with Confidence

Our Active Assurance customers have been able to turn up high performance services more than 10x faster, reduce SLA costs by millions of dollars by avoiding penalties, and save millions in customer care and troubleshooting costs by more efficiently finding, isolating, and rapidly resolving problems.

For turn-up, monitoring, troubleshooting, and change management, Keysight Active Assurance solutions help ensure that operators meet the expectations of their customers and fulfill their promises of a quality experience.