5G Active Assurance: Embracing a New Perspective

eBook

KEYSIGHT

Contents

5G

CHAPTER 1

5G Opportunities and Challenges

5G Opportunities and Challenges

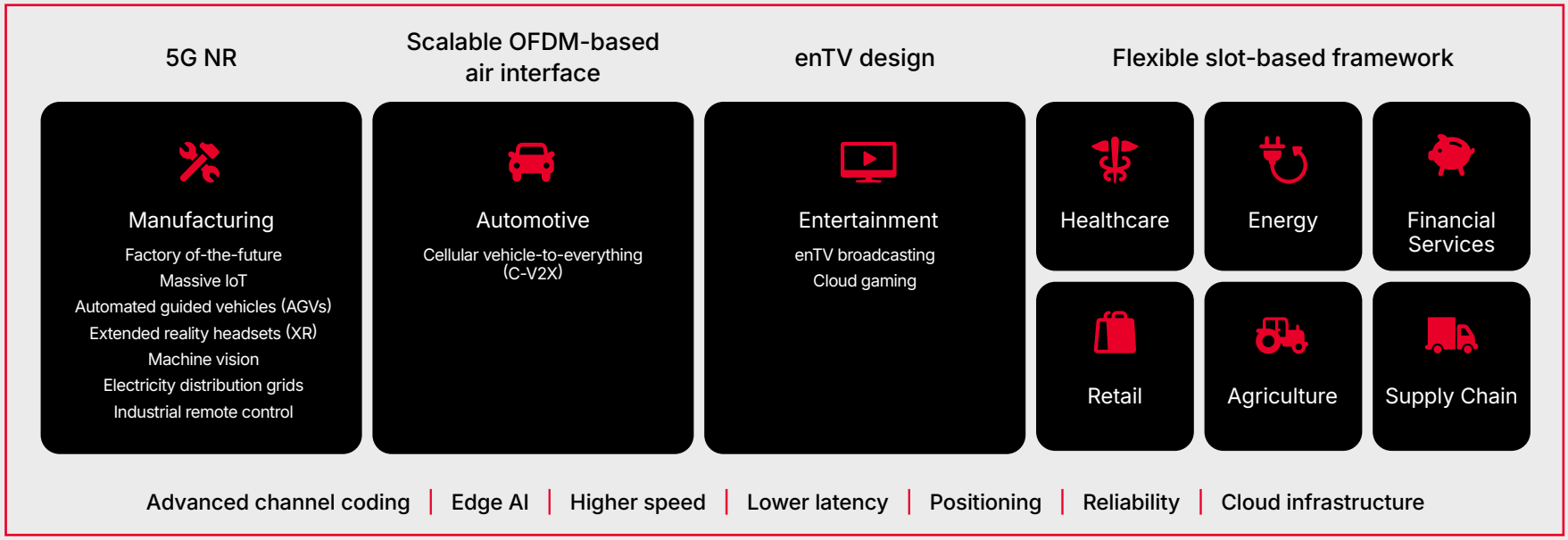
5G is here. According to Ericsson[1], there were 2.9 billion 5G subscriptions worldwide across 370 service providers by the end of Q4 2025. 5G is driving a wide range of new use cases beyond simple voice and data:

5G Global Reach

2.9B
SUBSCRIBERS

370
SERVICE PROVIDERS

Advanced 5G Technologies Create New Revenue Opportunities



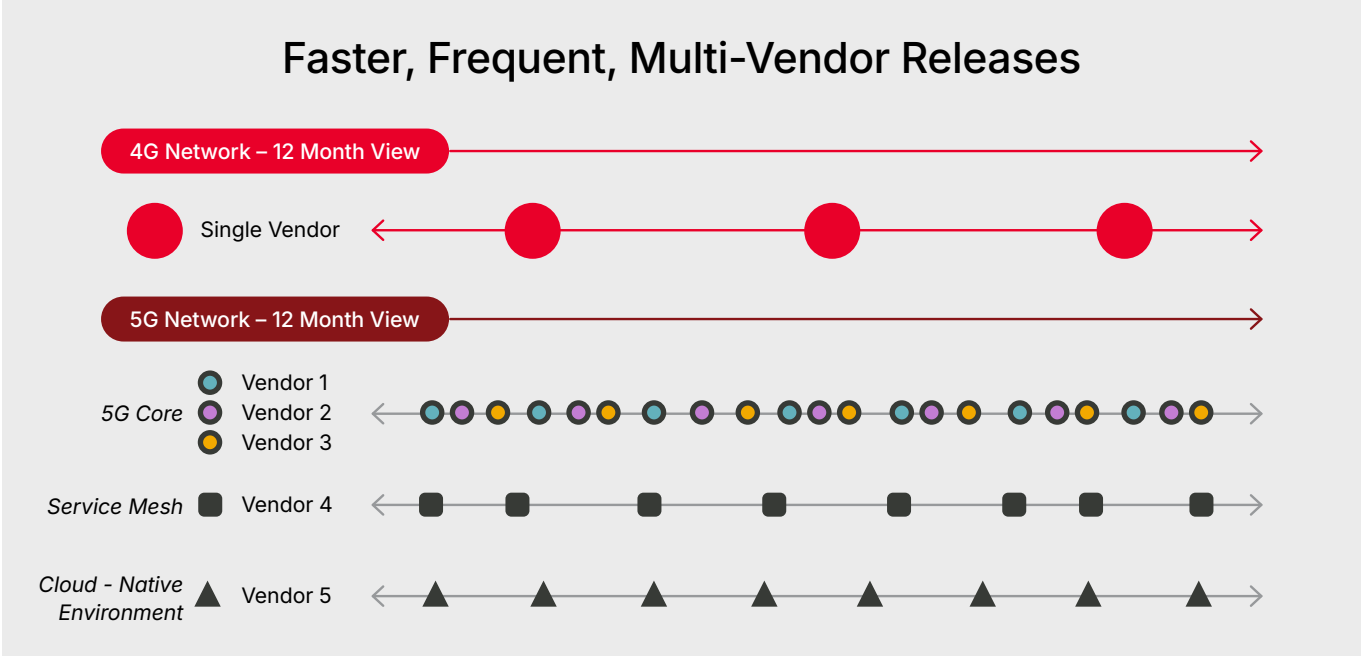
1 Ericsson, Mobile subscriptions outlook report, 2025.

The demand for these new use cases brings with it exciting opportunities for new services and revenues, but these opportunities do not come for free. They are underpinned by new technologies and a cloud-centric architecture that bring new capabilities, but also new challenges. In this eBook, we focus on the post-development challenges of deploying, operating, and optimizing 5G. We will explain why service assurance needs a complete rethinking to address these challenges and highlight why active service assurance (or more simply active assurance) must be part of the solution.

We begin with how 5G is changing the network and the assurance challenges these changes are driving.

Today's 5G networks are dynamic hybrid clouds

The core network has become cloudified and the radio network is beginning a long evolution. 5G network functions scale in and out dynamically. They no longer sit in a physical box, co-located with groups of related functions. This new disaggregated architecture brings an expanded vendor ecosystem with more layers and interfaces, leading to a constant stream of new and updated functions and services going live. On top of this, the path from users to apps and resources can (and does) change dynamically.



5G's cloud architecture leads to a constant stream of updates going live, dynamic instantiation of resources, and greater use of third-party clouds and networks.

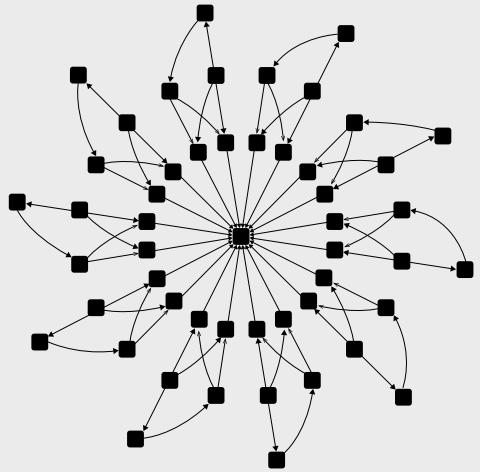
Key parts of the path may pass through cloud or physical infrastructure that service providers (SPs) do not own or control due to leveraging third-party cloud providers or supporting private mobile networks.

The passive analysis of user traffic and signaling SPs historically relied on for service assurance is not accessible outside their own network and cannot help them with new resources prior to launch, as there is no live traffic yet. As SPs move to 5G they will need to rethink how they get visibility of the entire network — even the parts they do not own or control. With more vendors and more layers in their networks, and a constant stream of updates, they will need a new approach that ensures newly activated resources deliver the high quality and performance next-gen use cases require.

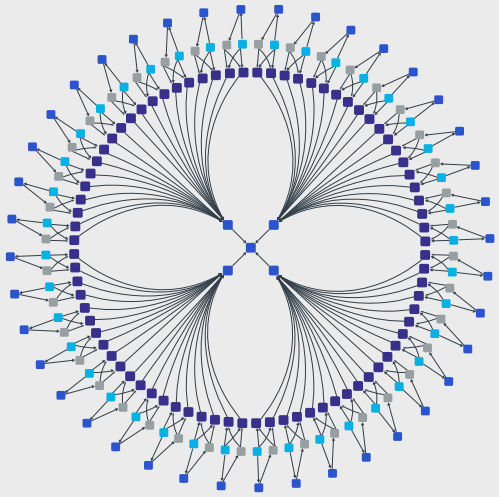
The edge of the network is expanding

Everything about 5G networks is bigger. For 4G, a large national provider might have a network topology with ten physical data centers. Mobile core functions deployed at these locations represent the edge of the mobile network — the point at which core networks interface with radio networks via IP aggregation and backhaul networks. While expensive, for 4G, a service provider could deploy service assurance probes at each of these locations to effectively monitor all user traffic and signaling.

With 5G, it is a much different story. Due to the need for lower latency, 5G core networks for a large national provider will extend to 50+ edge data centers around the country. And it does not stop there.



4G core network topology (few edge data centers)



5G core network topology (many edge data centers and hundreds of far edge)

The network edge is expanding drastically with 5G and so is the need for visibility into every corner of it.

Providers are already making plans to move core network functions even closer to end-users with “far edge” data centers. For a national provider, there could be hundreds of these. In addition, private 5G offerings from carriers will locate core network functions at enterprise locations, for an even greater number of far edge data centers that will need attention.

Let’s look closer

What’s driving 5G’s expanding edge? New use cases such as mobile VR gaming require latencies of 7–15 ms. Latency requirements for some industrial applications are as low as 1 ms. These ultra-low latencies are only possible using edge data centers.

A 5G service assurance model must cost-effectively match this expanded footprint. Far edge data centers will likely have limited physical footprints, and energy and bandwidth restrictions. The potential costs of passive service assurance probes that monitor all user traffic, all the time, in all these locations is prohibitive, even if resource needs could be met. To overcome these assurance challenges, fresh thinking for 5G is needed.

Cybersecurity + encryption

In the past, networks had perimeters. Beyond the firewall, traffic was encrypted. Within the perimeter, it wasn’t needed. But now, there is no perimeter — everything is outside the firewall. The result? Now everything is encrypted everywhere. At the same time, much of the network has transformed into software running in the cloud, creating new vulnerabilities to attack.

As they rethink service assurance for 5G, service providers must ask:

- *How can we measure end-user performance and perceived quality in an always-encrypted world?*
- *What new vulnerabilities are emerging and how do we continuously evaluate and mitigate against these?*

So, if the old model for service assurance won't work for 5G, what will? As modern test and assurance methodologies are designed, the challenges SPs must address include:

- **Complex, dynamic environments.** Dynamic networks where resources spin up and down rapidly must be monitored, including where SPs do not own or control much of the infrastructure.
- **High volume networks.** Test and assurance methods must work with massive networks with large numbers of nodes and sky-high traffic flow.
- **Intermittent issues.** Responsiveness to intermittent issues, such as problems that occur sporadically and unpredictably, must be accounted for, including problems that disappear before SPs can react and passively analyze.
- **Encrypted and secure networks.** Finally, assurance methodologies are required that work even when all the network traffic is encrypted and that enable proactive assessment of vulnerabilities.
- **Finding issues before users do.** This is perhaps the highest priority. How can SPs proactively uncover issues before users notice them? For example, the network has a flaw that will cause degradation and outages during peak traffic on Black Friday. How can these issues be spotted (and fixed) at 2 a.m., before customers swarm the customer-facing website? For retailers, this can prevent millions in opportunity cost losses. And, for network providers, this can avoid huge service-level agreement (SLA) violation costs and customer churn.

A service assurance methodology that solves all these problems is active assurance.

Distributed

Validate micro segmentation and network slicing security across complex, distributed networks

Disaggregated

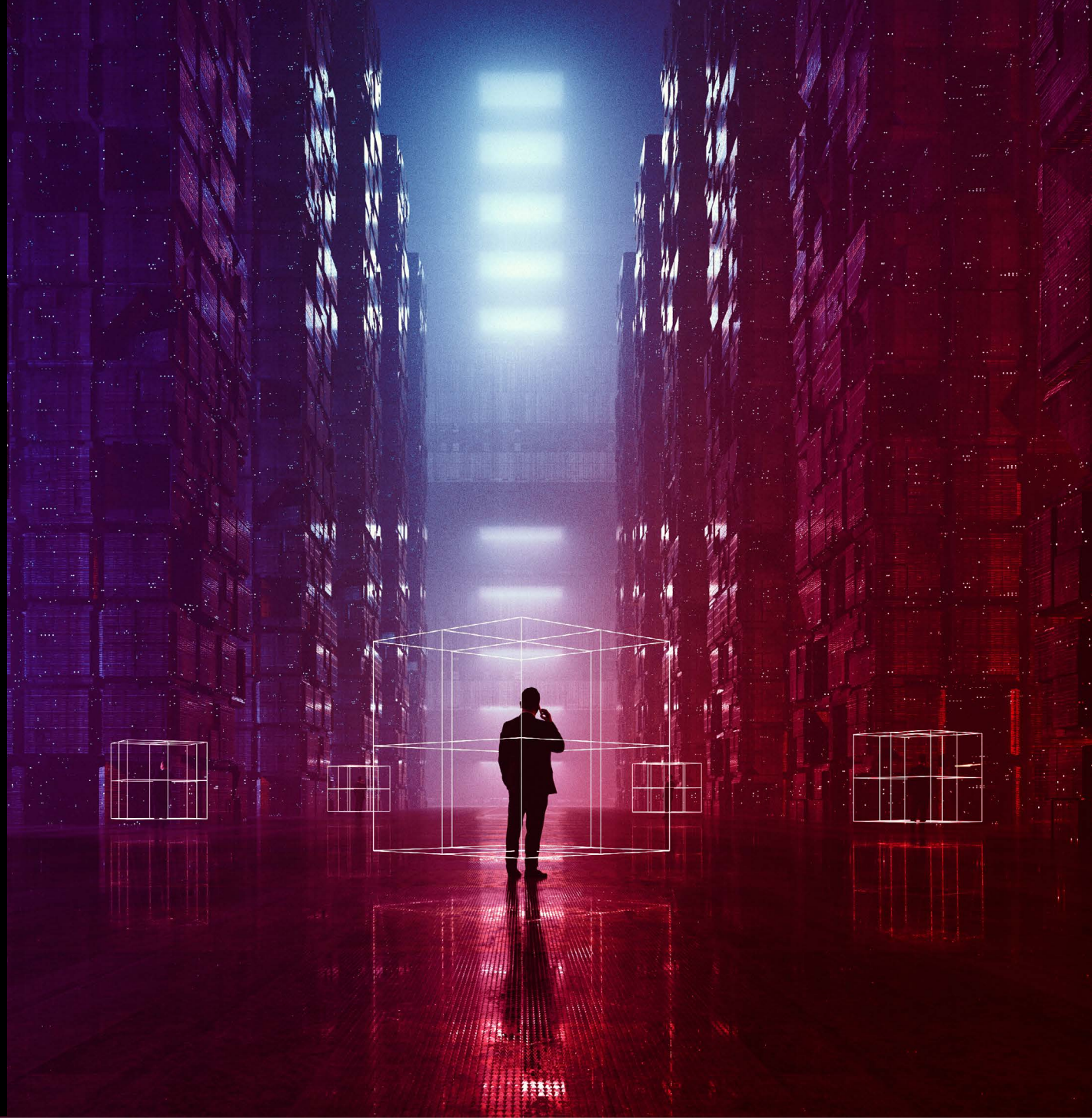
Ensuring consistent security and performance across hybrid compute infrastructures and security solutions

Dynamic

Continuous validation of security policy and QoE coverage of dynamic 5G ephemeral systems as they are spun up and down

CHAPTER 2

Meet Your Active Test Agent



CHAPTER 2

Meet Your Active Test Agent

How an active test agent rises to the 5G challenge

My responsibilities

Hi, I'm an Active Test Agent and I make network assurance possible. Think of me as a virtual 5G end-user device and user combined into one. My ability to emulate 5G network functions means I am capable of plugging into any part of the end-to-end network from over-the-air to radio access network (RAN) to mobile core to IP multimedia subsystem (IMS). I use the same SIM-based authentication and share the same security-trust relationship with the network as real devices. And I also run the same apps as a real device. For example, I can connect directly to the mobile core network by emulating both an end-user device and the radio network that links devices to core networks. SPs love me because they can instantiate copies of me throughout the network to test how the network performs end-to-end and across each network segment.

How I work

Once deployed, I can generate realistic 5G network traffic just like the real traffic that would normally emanate from that specific network location. Realism is the key here. Keysight tells me that is one of my most important capabilities because problems are often linked to specific traffic profiles. For example, I can mimic a drone streaming 4K or 8K video on an uplink while receiving small amounts of telemetry on the downlink. I've seen first-hand that such an unbalanced load can be extremely susceptible to latency on the lower-throughput link. One common issue is that the high bandwidth upstream video can cause congestion issues and the low bandwidth telemetry stream can be buffered causing a bursty or jittery delivery navigation instruction to the drone.

What I deliver

After I generate synthetic traffic, I insert it into the production network and measure the response. Then I send back the results of my tests to an active assurance control function that analyzes the results to get answers to critical questions. Is the network responding normally? Is the response slow? Is there no response? The results of the tests I perform across the network can be aggregated to paint a holistic picture of the network's health. One of my most important roles in delivering active assurance is continuously monitoring the real-time performance of new 5G applications and services.

> By accurately emulating real application traffic, I help ensure expectations and SLAs are met for even the most demanding new applications.

Active Test Agent profile

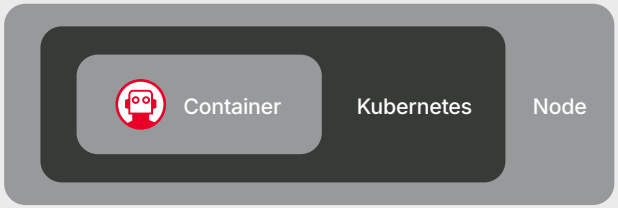
End-to-end and every interface in between coverage

SIM-based authentication

"At a high level, active assurance is a simple solution."

My areas of expertise

- Service activation
- Proactive monitoring
- Root cause analysis
- Change management validation



CHAPTER 3

Advantages of Active Assurance

CHAPTER 3

Advantages of Active Assurance

Active assurance provides unique advantages:

First, active assurance identifies problems before end users experience them. Imagine tomorrow is the date of the World Cup Finals. A service provider needs to ensure their 5G network is ready to host potentially record-setting traffic levels. At 3 a.m., they run a series of active assurance tests that trigger a machine learning (ML)-derived threshold identifying performance issues with end-to-end streaming video services. A workflow is then triggered in the network topology to deploy additional agents at key network interfaces along the end-to-end path. After gathering and analyzing data, the problem is isolated to a backhaul network. The traffic is rerouted to the secondary link and within minutes everything is fixed, and the extra agents are de-instantiated.

Let's look closer

The ability to dynamically create and update thresholds using machine learning enables the detection of network issues. This, together with the ease of automatically deploying and redeploying agents where they are needed, leads to faster issue resolution and avoidance of customer-impacting issues.

Eight hours later, the finals begin, and the SP's network performs like a champion. Contrast that with not discovering the issue until 3 minutes into the finals match, and it is clear why this advantage is so critical.

Active assurance works in modern, complex, dynamic environments. Today's networks are more complex than ever. Gone are monolithic, single-vendor architectures and dedicated hardware-based network functions — replaced by disaggregated, multi-vendor, hybrid cloud networks. Service providers must contend with ensuring everything works end-to-end, even though traffic traverses parts of the network that the SP has no control over and traditionally no visibility into.

Passive assurance will not work in such cases. Service providers simply cannot place probes across all locations and interfaces and test parts of the networks that live in these "digital wildernesses."

Active assurance elegantly gets around this problem. It sends synthetic traffic through the network (and across these digital wildernesses) and then observes how the network performs. It provides valuable insights into end-to-end performance even when the SP does not control all the parts of the network.

Works with encrypted traffic. Because modern networks are so open, encrypting traffic in motion has become universal. This complicates service assurance by reducing visibility. Active assurance, however, participates in security and encryption schema using the same mechanisms as real users. Passive assurance systems, on the other hand, must utilize deep packet inspection (DPI) and attempt to recognize patterns and make assumptions about the encrypted user plane traffic, and have the keys shared to decrypt the control plane, thereby limiting the interfaces on which they can be deployed and increasing security risks. This diminishes the accuracy of their KPIs and adds security risks. Active assurance is unaffected by having to cross vast digital wildernesses uncontrolled by the SP and works with encrypted traffic while in motion.

Works in high-volume environments. Probes that passively monitor all user traffic and signaling can become overwhelmed in high-traffic environments. Active assurance is unaffected by this. It simply observes the performance of the active test agent's network requests, undeterred by any concurrent high traffic volumes. It may seem counter intuitive at first, but active agents actually put less aggregate traffic load on the network when compared to the massive captures that must be moved from passive probes to a data lake for post analysis.

Easy to automate. Active assurance lends itself to highly automated environments.

- It can be part of a continuous integration / continuous delivery (CI/CD) automation process, running a series of standard tests when new revisions are released to the network. For example: an SP just updated a component in the fronthaul network — has it affected performance?
- It can initiate triage test scripts automatically.
- Based on the results of these triage tests, it runs secondary and tertiary tests to further isolate the root cause of the performance deviation.
- This immediately requires fewer senior staff to handle network problems, freeing them for more pressing issues. As carriers move toward network orchestration and closed loop automation, active assurance will provide the real-time feedback needed and foster development of self-healing networks in the future.

Let's look broader

Active assurance is a proven approach that has been used for years to monitor critical network segments and services such as cell site Ethernet backhaul and is the eyes and ears of all the cloud-scale services. While it is not new to 5G, today's active assurance has been completely transformed to take advantage of 5G's cloud architecture.

CHAPTER 4

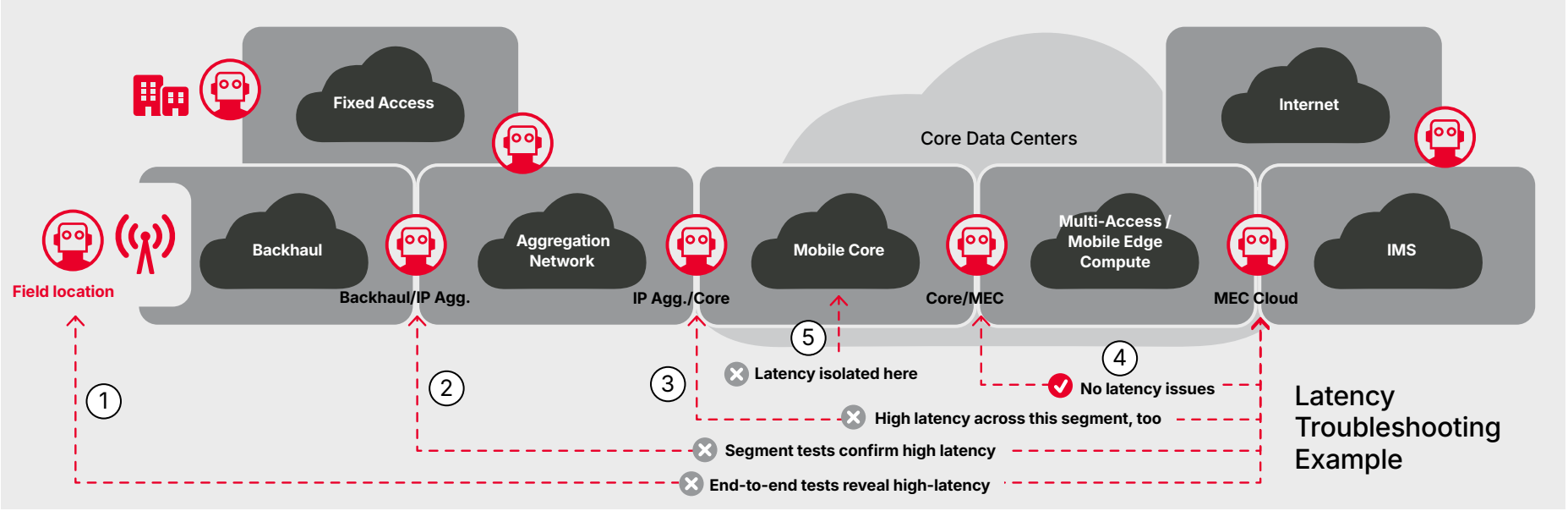
Deploying Active Assurance in 5G Networks

CHAPTER 4

Deploying Active Assurance in 5G Networks

Active assurance is a simple process in theory. But how does one deploy active assurance in a modern, complex 5G network? The diagram below shows a 5G network and where active test agents are typically deployed.

Active test agents inject synthetic traffic into the network under test at endpoints and various points in between, where performance and quality are assessed at each point. The realistic traffic that is being injected is a known quantity, enabling the service provider to easily measure what is coming out at the endpoint. By inserting known traffic into the network, active assurance enables providers to perceive fine variations over time, via machine learning, differentiating normal variation from significant issues and providing an accurate view of the network and the user experience.



Active test agents can be placed anywhere in the network to measure end-to-end or segmented areas of focus so that issues can be identified using step-by-step isolation methods.

In addition, a service provider can instantiate an active test agent into a specific part of the network, run their tests, and then de-instantiate the agent easily and cost-effectively. Using artificial intelligence (AI) and ML signature-triggered workflows, coupled with network topology information, active assurance systems work with the network orchestrator to insert active test agents wherever they are needed in the network at any time, to:

- Perform validation testing of newly activated functions, network slices, and infrastructure (before, during, and after they go live)
- Proactively and continuously monitor critical links and services from an end-user perspective
- Troubleshoot any issues by deploying end-to-end and segment-level tests to isolate underlying root causes
- Confirm fixes with change management use cases, which completes the assurance cycle: activate, monitor, isolate fault, validate change

Let's look closer

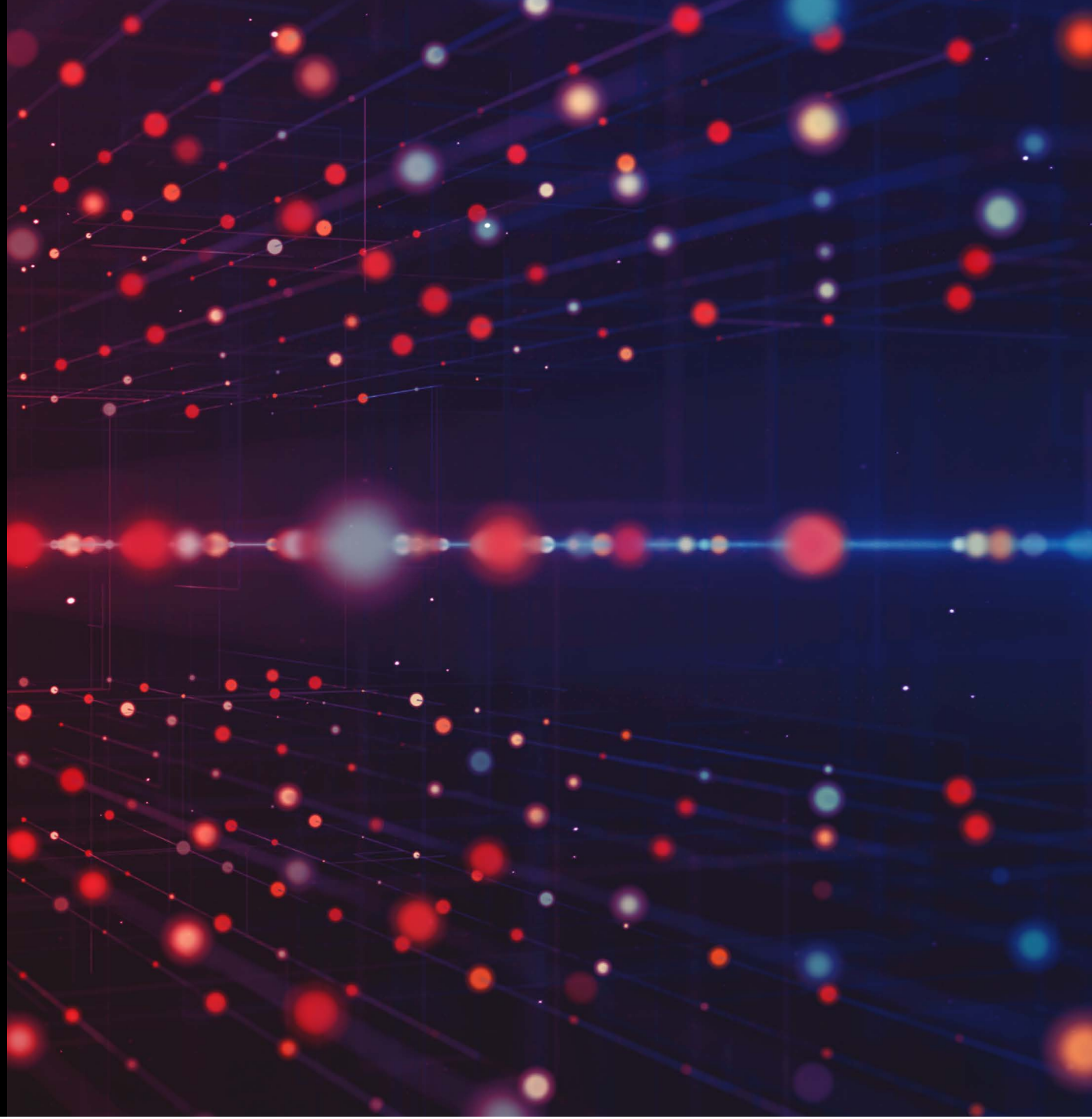
Just as important as end-to-end visibility is the ability to narrow down and isolate the root cause of a discovered issue. Layered regionalized or technology-specific views aid in pinpointing the source of the issue.

Let's look broader

5G creates a complex, multi-vendor, CI/CD world where release cycles have shifted from years or months to weeks or days. Service providers must also shift to automated, agile testing as part of the CI/CD innovation pipeline.

CHAPTER 5

Active Assurance Use Case: Edge Networking



CHAPTER 5

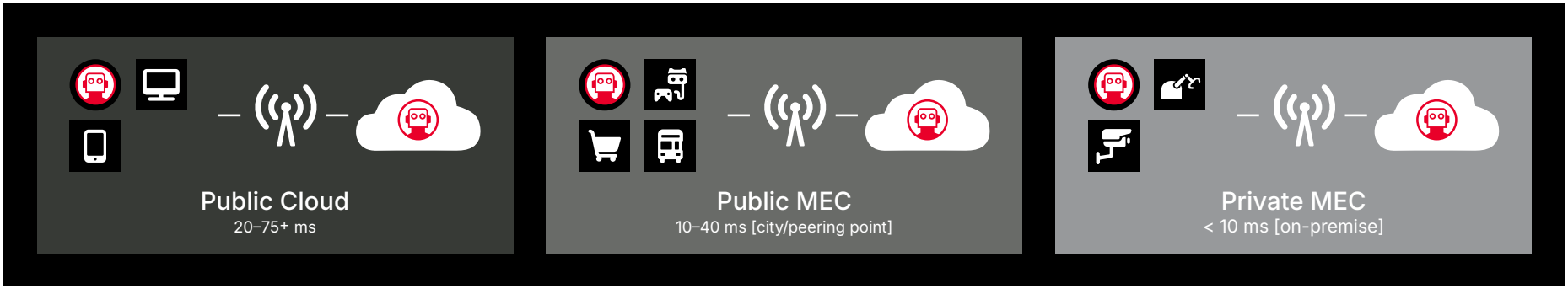
Active Assurance Use Case: Edge Networking

Companies are creating edge networks for several reasons. First, for applications that require very low latency, such as autonomous vehicles or remote surgery. And, second, for applications that create a massive amount of data that would be impractical to send back to a centralized cloud, like many IoT applications.

To support these edge networks, service providers are building disaggregated networks near or even on the client's site. In doing so, they are pushing core network components to the far edge, or in the case of private networks, into the enterprise. Deploying a 5G network today is a manual, labor-intensive process. That is not feasible for turning up a high volume of small edge networks.

The solution is automation — adopting the CI/CD methodology to the building and deployment of complex 5G networks. In a perfect world, a test team schedules an inventory of virtual and physical test equipment, deploys the antennas, sets up the test campaign, hits the green button, and testing begins.

Environment	Use case	Latency
AR/VR/gaming	AR/VR motion-to-photon (picture)	7–15 ms
	Collaborative gaming	< 20 mss
Transportation and logistics	Time critical sensing	< 30 ms
	Remote drone operation	10–30 ms
	Real-time control for discrete automation	≤ 1ms
Automotive	HD digital map update	100 ms
	Remote operation	10–30 ms
	Sensor sharing	< 20 ms
Smart cities	Time-critical sensing	< 30 ms
Industrial	Mobile robots (machine control)	< 10 ms
	Mobile robots (video-operated remote control)	10–100 ms
	Process automation	50 ms
	Mobile control panels (assembly robots, milling)	4–8 ms
	AR monitoring	< 10 ms



Use case examples for multi-access edge computing (MEC) networks

The validation process automatically tests that network functions are running correctly and issues a birth certificate for that network. That is not possible with passive assurance. In the pre-deployment phase, there is no traffic to monitor passively. Active testing simulates live traffic and can identify any issues before a new service or new portion of the network goes live.

Once the edge network is live, application roll outs begin. It is crucial to monitor these new applications to ensure they are running as planned, which active assurance supports comprehensively in real time. In contrast, passive monitoring is based on statistical analysis, which may be problematic with ultra-low latency applications at the edge. By the time a significant departure from statistical norms is identified, a real problem has already occurred.

For example, a factory floor may have cameras installed on assembly line robots that are programmed to spot dangers like a human walking into their field of view. By using DPI to analyze encrypted traffic, passive analysis may miss a critical change in the latency or jitter. In this case, high network latency means a human might be injured before the robot spots the human. Passive testing may send the alert too late to help.

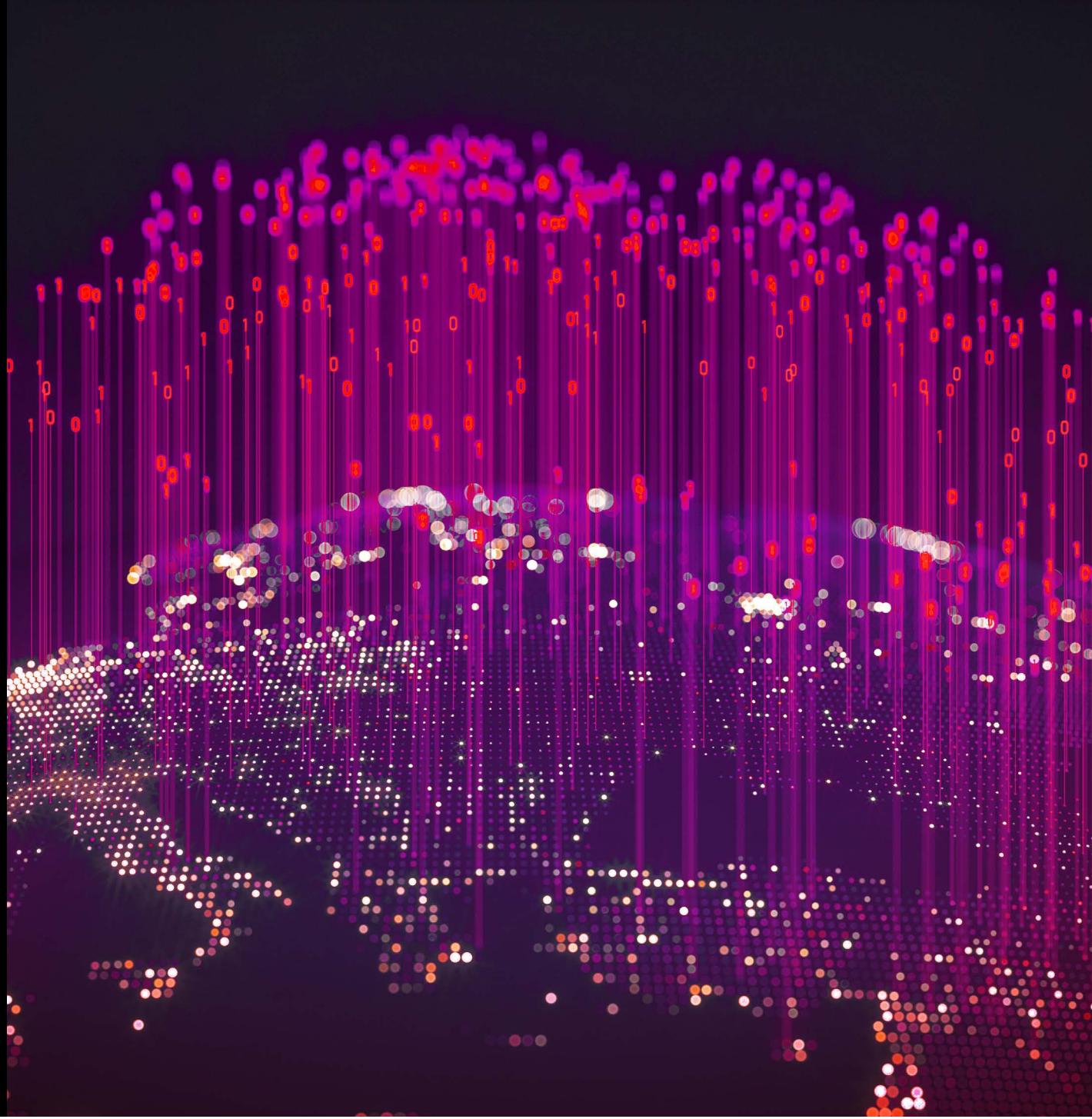
Active testing would have spotted any latency issues before the human even got to work that morning. It would have triggered the orchestrator with a remediation routine that would test other critical parts of the network, looking for the issue. It would have found the root cause quickly, allowing the fix to be implemented in near real-time. The problem is solved long before it becomes a dangerous issue. In the most advanced form, active assurance becomes a core component enabling a self-healing network.

Active Test Agent

Monitoring connectivity to industrial robots to ensure latency SLAs are met: **< 10 ms**

CHAPTER 6

Testing in a 5G World



CHAPTER 6

Testing in a 5G World

5G changes everything for service assurance. New 5G networks are high-volume, dynamic, multi-vendor networks where traffic is almost always encrypted. As we have seen, 5G networks are impossible to assure with traditional tools and outdated strategies.

Active assurance — service assurance powered by active testing — works in modern, complex multi-vendor disaggregated networks. Active testing and assurance are key elements of all cloud service providers, from Amazon to Netflix to Google. It will be the eyes and ears of closed-loop orchestration of carrier networks. Even with encrypted traffic in high-volume scenarios, active assurance identifies issues before end users do and is easy to automate to speed root cause analysis and timely resolution of critical issues.

Looking to learn how Keysight tackles 5G assurance?

Keysight VisionWorks brings the complex, dynamic, and abstract into view with network-aware mobility service assurance. Visit our site.

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.