White Paper

It’s Time to Be Pro-Active:

Why 5G, SD-WAN and NFV require automated Active Assurance

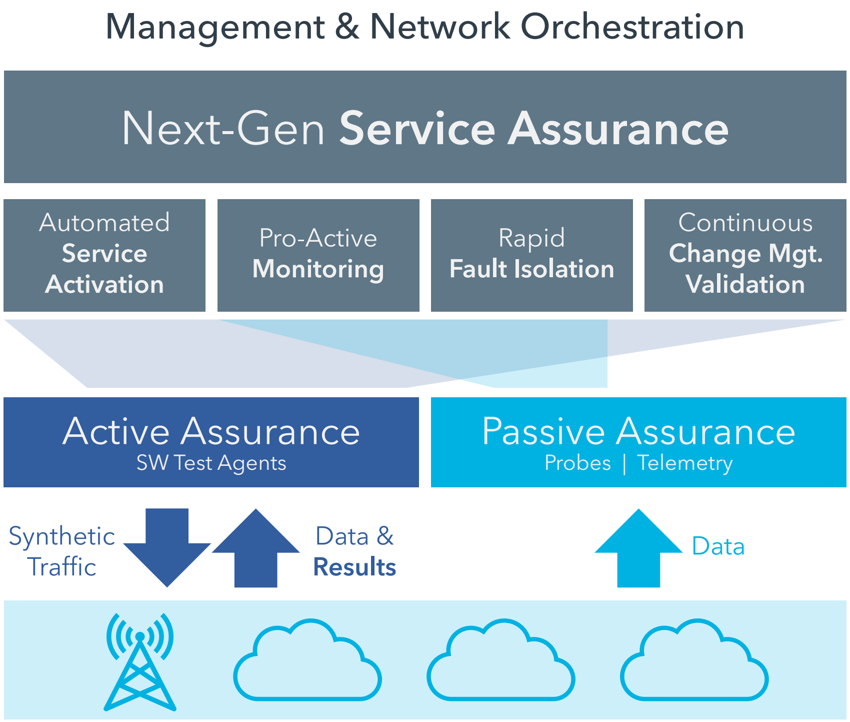
Containing issues in today’s networks is a never-ending effort—as soon as service providers fix one issue, another one springs up. They spend tens of millions of dollars instrumenting the network with traditional passive service assurance systems – yet still struggle to isolate root causes of end-to-end issues, avoid major network outages, and automate problem resolution.

As the race to deploy 5G, SD-WAN and NFV heats up, the network is moving to the cloud and functions that used to sit in well-defined elements are now virtualized and may be deployed anywhere from centralized data centers to the customer premises. Moreover, next-gen networks are much more dynamic than traditional networks, changing so often that manual troubleshooting simply can’t keep up. It’s getting more difficult for service providers to stay on top of network issues, let alone get out ahead of them.

Two paths to assuring the network

Simply adding more passive instrumentation isn’t going to fix the problem. We need a fundamental shift in our approach to assuring the network. As part of that, service assurance needs to be integrated with the network so it can be substantially automated. Unfortunately, the majority of today’s assurance instrumentation is based on passive data sources and probes that can’t support all assurance use cases. So our ability to automate is severely limited.

Active Assurance complements Passive Assurance to provide extensive coverage of assurance needs so that comprehensive automation can take place. Active Assurance has been used by service providers for years, but prior to virtualization it simply wasn’t cost-effective for network-wide deployment. As 5G and SD-WAN drive us to adopt virtualization, Active Assurance is poised to become a critical and essential enabler of the automation needed to successfully ensure differentiated performance and quality for next-gen services.



Next-gen service assurance requires both Active and Passive approaches.

To better understand the strengths and weaknesses of each approach, let’s take a look at the differences between passive and active assurance.

Passive assurance

Passive assurance is the traditional method for determining the health of the network. Passive assurance uses physical devices to collect telemetry from virtual or physical network functions, DPI (Deep Packet Inspection), or protocol probes that passively monitor the signaling and user traffic on the network. Data can also be gathered from other sources of subscriber data such as billing records that inform the operator about the subscribers and how they're using the network.

Best for when things are up and running

Passive assurance gathers all the data from all of the operator's subscribers as they use the service. It's particularly adept at detecting a problem that affects masses of customers and issues that can be inferred by looking at signaling data or statistical analysis of data flowing through the network. Passive assurance is also helpful for looking at issues in specific parts of the network and works best once a new function, slice, or service is up and running.

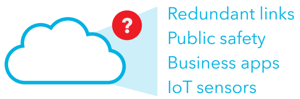
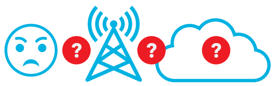
Not as good for turn-up and end-to-end troubleshooting

Passive monitoring relies on data generated by use of the network and services. As its name implies, it's passive—it waits for customers to use the network—and is therefore not very helpful at turn-up, when there's no traffic running through the network, or for critical, always-on but mostly inactive functions such as in public safety networks

In addition, as networks are virtualized, service providers are shifting to more agile release schedules, meaning new and upgraded network functions are constantly being integrated into the production network. Passive assurance has no ability to proactively validate these changes during maintenance windows before actual customer usage begins. When a problem passes into the production network undetected, the consequences can be severe including inefficient rollbacks of changes, customer dissatisfaction and SLA penalties.

Because passive assurance relies on dedicated physical equipment, it's expensive to deploy on a widespread basis. Operators must be judicious about where they place their monitoring, typically inserting probes just into key parts of the network. It's simply not cost effective to monitor all traffic, in all parts of the network, at all times. Therefore, if a problem appears in a location in the network where few problems typically occur (and therefore is not monitored), the operator may not detect the fault.

When it comes to end-to-end troubleshooting, passive systems aren't able to effectively isolate performance and application-layer quality issues across the entire end-to-end service delivery path including customer premises and over-the-air / RF links. What's more, due to the high cost of decryption, passive systems are typically limited to statistical estimations of perceived quality based on high-level metrics like packet loss, jitter and latency. While useful for wide-scale monitoring of quality, these metrics are less helpful for precise isolation of the root causes of quality degradations or user-specific traffic policy issues.

Turn-up: Will the network perform when customers use it?	**Monitoring:** How is the network performing right now?	**Troubleshooting:** What part of the network is causing the issue?
	 ? Redundant links Public safety Business apps IoT sensors	
Limitation: No usage means no data to assess readiness	**Limitation:** Doesn't cover all parts of the end-to-end network	**Limitation:** Weak at isolating certain service quality / network issues

Passive Assurance Weaknesses:

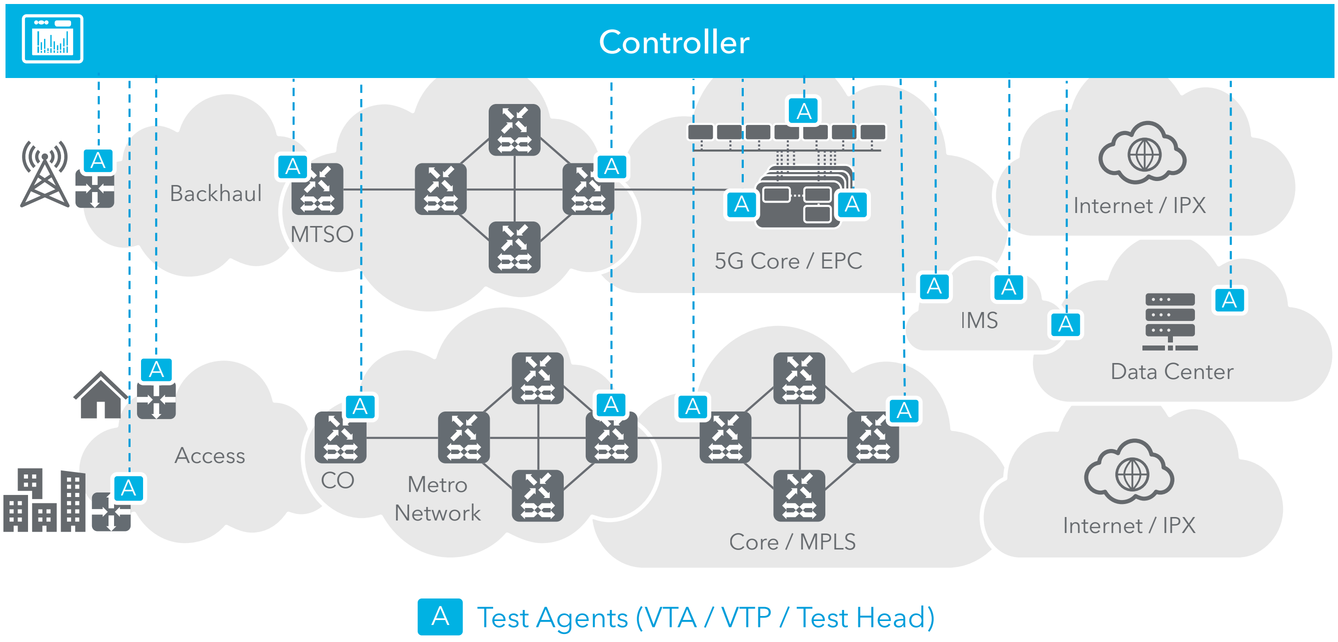
Active assurance fills the gaps

Active assurance emulates real network functions, devices, and users, to create highly realistic synthetic traffic. This traffic—created via virtual test agents or VTAs—is then injected into the network under test at end points and various points in between, and performance and quality are assessed at each point.

At one time, due to the relatively high cost of physical test heads in traditional physical telecom networks, active testing was relegated to a handful of high-value applications such as cellular backhaul and business Ethernet service assurance. But that's no longer the case. Virtualization and the move to cloud networks reduces the costs of active testing by an order of magnitude, laying the foundation for network operators to broadly adopt this proven approach.

With active assurance, the realistic traffic that you're injecting is a known quantity, enabling the service provider to easily measure what's coming out at the endpoint. Remember what we said about how hard it is to tell if small fluctuations were due to user behavior or to a real problem? By inserting known traffic into the network, active assurance enables providers to perceive fine variations over time, allowing them to differentiate normal variation from significant issues and providing an accurate view of the network and the user experience.

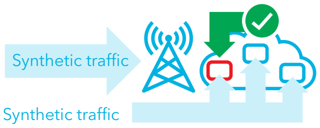
With Active Assurance, active test agents can be dynamically instantiated across the network:



Even better, a service provider can instantiate a VTA into a specific part of the network, run their tests, and then de-instantiate the agent easily and cost-effectively. VTAs can be inserted anywhere in the network, enabling one to perform similar tests at different locations—something that's very cost-prohibitive or even impossible with a physical probe.

By inserting known traffic across the network, active assurance not only enables operators to troubleshoot complex issues, it opens a window into user plane application-layer performance and quality in a way that's not possible with passive monitoring. Spirent deployments of active assurance solutions have demonstrated seven to ten times faster turn-up of new network functions, saving millions of dollars per year by reducing the costs of manual testing and troubleshooting, and by avoiding service level agreement (SLA) penalties.

Passive Assurance Weaknesses are Active Assurance Strengths:

Turn-up: Will the network perform when customers use it?	**Monitoring:** How is the network performing right now?	**Troubleshooting:** What part of the network is causing the issue?
Emulated Synthetic traffic	Synthetic traffic Redundant links Public safety Business apps IoT sensors	
Strength: Active Assurance ensures the network is ready for users	**Strength:** Active Assurance proactively finds issues for critical services	**Strength:** Active Assurance mimics realistic usage to isolate service issues

Getting the best of both worlds with active and passive assurance

Active assurance is the perfect complement to passive assurance to help service providers “close the loop” and achieve the ideal of continuous automated testing. Passive assurance is well-designed for monitoring and finding major issues. It can identify how many users are impacted by a problem and troubleshoot high priority parts of the network.

Active assurance, on the other hand, is ideal for pinpointing the root cause of a problem. It enables service providers to evaluate performance at turn up, check critical services and links even when traffic levels are low, proactively identify minor 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, wants to ensure a public safety network is functioning properly, or needs to isolate a complex problem.

Passive Monitoring is ideal for:

- Monitor performance once the network is up and running
- Track services and links that have consistent traffic flows
- Detect major issues and determine how many users are impacted
- Troubleshoot issues for high-priority parts of the network

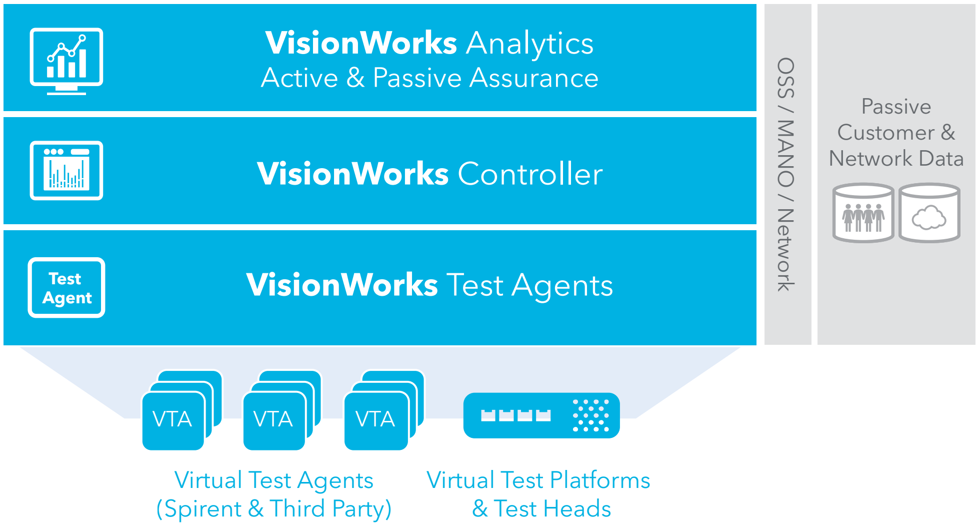
Active Test enables you to:

- Evaluate performance at turn-up before customer usage starts
- Continuously check critical services and links, such as an IoT sensor or emergency communications, regardless of traffic levels
- Proactively identify minor issues before they become major
- Troubleshoot complex issues in any part of the network because it’s virtualized and inserts small amounts of traffic, so it’s not a heavy lift.

Performance challenges are growing. But so are our tools.

Clearly, to truly close the loop of continuous, automated testing, passive and active assurance must be linked. Spirent's VisionWorks combines intelligent analytics based on both active testing and passive customer and network data to provide actionable results to network operations teams and automated systems. It's cloud-native, ready to be integrated with new cloud networks and automation platforms that providers are building. VisionWorks, with its open interfaces, is also designed to easily integrate with legacy systems, facilitating the closing of the troubleshooting loop and building a system in which passive and active assurance work together for optimal results.

VisionWorks Active & Passive Assurance Platform:



VisionWorks Analytics
Active & Passive Assurance
VisionWorks Controller
Test Agent
VisionWorks Test Agents
OSS / MANO / Network
Passive Customer & Network Data
VTA
VTA
VTA
Virtual Test Agents (Spirent & Third Party)
Virtual Test Platforms & Test Heads

Develop, Deploy, Operate

VisionWorks is a key part of Spirent's vision to provide a holistic solution that supports the needs of service providers across the entire lifecycle of their network—from validation in the lab and preproduction environments to assurance in the operational network.

Our approach:

- Bridges the gap between development and operations teams to support NetDevOps across the stack and throughout the service lifecycle
- Facilitates automation of the testing process, of utmost importance when things are moving faster than a human can keep up
- Emphasizes continuous testing, driven by test and lab automation, to optimize the validation of an organization's networks and business offerings

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

DEVELOP
OPERATE

DEVELOP

Spirent reduces time and cost to develop, secure and launch new products, services, and networks.

Accelerated Time to Market

DEPLOY

We assure things work as expected by testing the most realistic scenarios at scale.

OPERATE

Spirent improves network performance and customer experience while radically reducing operating costs.

Improved Customer Experience

Spirent provides expert guidance and award-winning testing, validation, and analytics methodologies that help our customers find clarity in the midst of complexity, overcome the challenges of the fast-approaching future, and assure that they ultimately deliver on their promises to their own customers of performance and security.

As a result, our customers are able to turn-up high performance services more than 10 x 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.

SD-WAN, Virtualization, and 5G, along with snowballing demand from impatient consumers for data-intensive, bandwidth-scarfing applications, will challenge operators as never before. To fully address these challenges, service providers must take a holistic approach to assurance. By utilizing thoughtful pairing of passive and active assurance and taking a NetDevOps approach, operators can better meet the expectations of their customers and fulfill their promises of a quality experience.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com