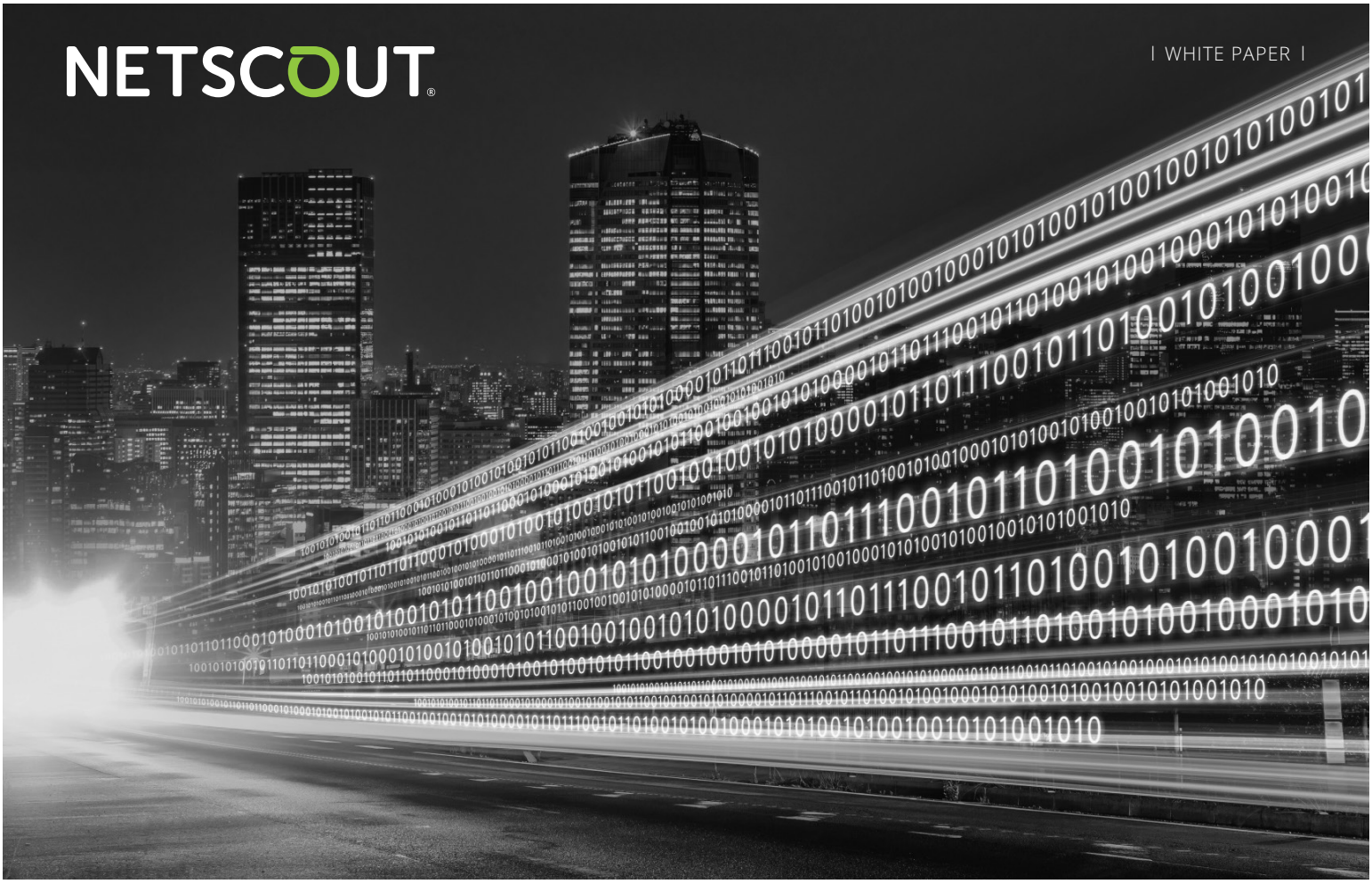
NETSCOUT®

I WHITE PAPER I



Recipe for Success

Enterprises and Service Providers Need to Trust a Proven Recipe to Assure Hybrid Cloud Environments

SERVICE PROVIDER

TABLE OF CONTENTS

Introduction

Recipes are the foundation of the food business and for good reasons. They help chefs assure the quality of food by using proven techniques, trusted ingredients, and prior successes. Similarly, the tech industry leans on its proven leaders. However, with new types of networks being deployed, cloud computing becomes an integral part of network infrastructures. They provide cost-effective collaboration and productivity for employees, vendors, and customers while improving network scalability and performance and ensuring business continuity against cybersecurity attacks. Sounds like the start of a good recipe!

As a result, investment in cloud services is expected to grow by more than 23 percent this year, from $257.5 billion in 2020 to $304.9 billion in 2021. Not surprisingly, the global pandemic has increased enterprise dependence upon the cloud, with 90 percent of business leaders reporting that their company's cloud usage is higher than initially planned to meet increased demand for online assets and ensure business continuity for remote workers.

Growing reliance on the cloud is also being driven by increases in 5G rollouts – especially those of standalone 5G networks. In the *5G Standalone January 2022 – Member Report*, the Global Mobile suppliers, Association (GSA) states almost 99 operators in 50 countries are investing in 5G Stand-Alone (SA), with 20 of those operators already launching 5G SA networks in 16 countries. 5G SA provides a digitized platform necessary to deploy new cloud services and take advantage of cloud-native 5G benefits like massive Internet of Things (IoT) networks, edge computing, and network slicing.

Of the four types of cloud architecture – private, public, hybrid, and multi – 78 percent of enterprises have adopted a hybrid cloud strategy. Hybrid cloud is the ideal IT model for today's digital business climate, enabling enterprise IT teams and service providers to shift workloads as business needs evolve by moving data and computing workloads across private, public, and third-party clouds.

But hybrid cloud systems also pose complex architecture and security challenges. Indeed, 81 percent of business leaders say the top cloud challenge is security. Not surprisingly, service assurance in this type of environment can be extremely complex. What's needed is a trusted, proven recipe for service assurance that provides deep insights across all parts of the hybrid cloud network with established, verified success as the outcome.

What's needed is Visibility Without Borders®.

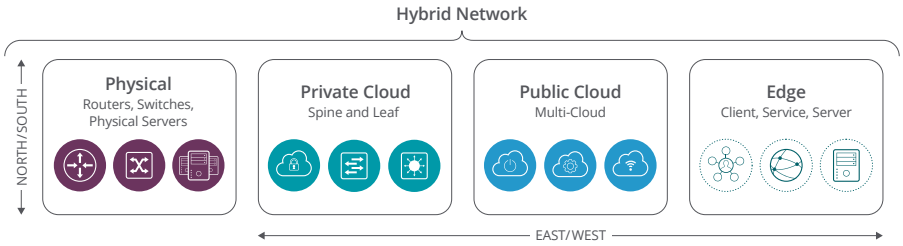
A Recipe Built with New Ingredients

As service providers advance their 5G network rollout plans, they're maintaining a laser focus on creating new revenue-generating services. But their ability to create those services rests in large part on ensuring that end-to-end Customer Experience (CX) meets or exceeds expectations. Assuring this level of CX requires cross-domain/cross-silo visibility, even when the service provider doesn't control the underlying infrastructure (ingredients), as with public clouds.

Likewise, architectural changes in 5G networks – think virtualization, disaggregation, and cloudification – require an approach to assurance that it is more agile, flexible, and software-centric than in the past. The impact of these changes is evident when considering service assurance for hybrid networks.

A hybrid network is made up of four primary ingredients:

- Physical network, including routers, switches, and physical servers
- Private clouds
- Public clouds
- The edge; including client, service, and server edges



While many service providers have relied on service assurance recipes that only look at north/south traffic, hybrid cloud networks demand a new service assurance recipe that is more complete and looks at all traffic: north/south and east/west. Likewise, service assurance in a hybrid network requires a complete view within and between:

- The physical network; including 5G, 4G, LTE, and data centers,
- Private clouds; including 5G, Kubernetes, OpenStack, and VMware
- Public clouds; including 5G, AWS, Azure, Google Cloud Platform, and IBM Cloud
- The edge; including 5G, client, service, and server edges

That subtle shift in the recipe represents a massive shift in applicability and therefore success because assuring hybrid cloud networks requires a solution that can seamlessly traverse multiple types of networks.

Service assurance now must consider traffic that's crossing public clouds and private clouds as well as microservices within the cloud. Drilling down even further, service assurance needs to examine individual containers to determine whether they're working and performing as expected. If the solution is monitoring a Kubernetes container, it will have IP addresses that change and duplicate repeatedly, and a service assurance solution must be agile enough to operate in such an environment.

Simply stated, the complexity of hybrid networks completely and radically changes everything about service assurance.

In hybrid networks, there must be visibility across all network implementations to assure the high-quality delivery and security of applications and services. That visibility must extend to any network, across any vendor, for any service and over any cloud.

Any network includes 4G/5G, Wi-Fi, Citizen's Broadband Radio Service (CBRS), cable, fixed and open RAN.

Any vendor means the solution is essentially vendor agnostic and can work with solutions from Ericsson, Nokia, Cisco, Huawei, Dell, and more.

Additionally, a successful recipe for service assurance must work in any use case, including VoIP, VoLTE, Voice over New Radio (VoNR), enterprise 5G, over-the-top (OTT) services, video, and the Internet of Things (IoT). And it needs to occur over any cloud, including Kubernetes, OpenStack, VMware, public, edge, and multi-access edge computing (MEC).

Service providers can no longer leave service assurance up to the network solutions that provide assurance only on their own elements. They find proven, reliable, and provider agnostic solutions for success that includes end-through-end visibility.

Achieving Visibility Without Borders

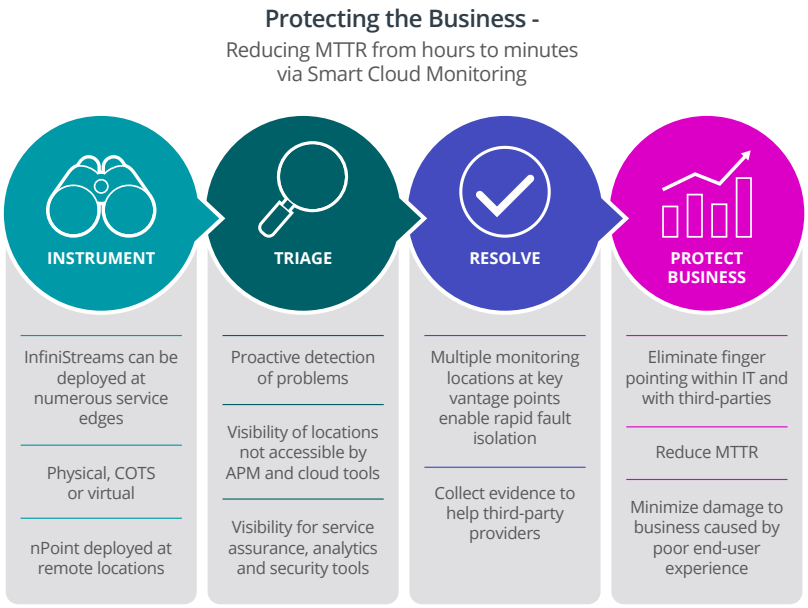
Assuring hybrid cloud network reliability and security also requires the use of a key ingredient, Smart Data, to gain deep visibility that provides both granular and service-level views into the network.

Smart Data is derived from direct access to the wired data source: IP packets. As such, Smart Data provides full visibility across any network–physical, virtual, cloud– application programming interface (API) to develop a holistic, end-through-end view of network health by subscriber, device, and session.

Smart Data is based on metrics important to service providers and IT teams–everything from latency, throughput, and audio gaps to mean opinion score (MOS), OTT video quality, radio access network (RAN) radio power measurement, and more. Not only can a service assurance solution based on Smart Data reduce mean time to repair (MTTR), but it also provides full visibility into edge services, cloud availability zones, cellular and IP networks. It enables service providers to see every communication between different virtualized networks, all from a single pane of glass.

With a seamless and proactive view of the network for service assurance, operations teams can rapidly identify, triage, and isolate issues that impact services from degradation to outages, thereby reducing MTTR from days to minutes. By applying artificial intelligence (AI) and machine learning (ML) to Smart Data, the service assurance solution can spot anomalies and trends that would otherwise be missed.

To better understand this process, consider a cell site in Manhattan that services thousands of customers. The service provider knows that the cell site normally operates at a 90.7 service threshold. As such, the service provider sets an alarm to alert if the service threshold falls to or below 85.0.



However, by the time poor service quality has triggered an alarm, it often degrades even further before a service provider can locate the alarm, identify the issue, and repair it. In contrast, a service assurance solution based on Smart Data doesn't wait for service quality to drop to the alarm level. Using the same scenario, a service assurance solution based on Smart Data can extrapolate historical information and current conditions for the site to intelligently determine that a network/service/application is degrading and indicate why network quality is being impacted.

For the hypothetical cell site in Manhattan, the service assurance solution based on Smart Data could send an alert before the alarm threshold is reached telling the service provider, for example, "I know that the site is operating at 82.7 right now, but you should probably pay attention to it, because it's usually at 90.7." Furthermore, a service solution based on Smart Data can even tell a service provider the number of unique subscribers that are being affected by a service quality issue in real-time, and then compare that information to historical data for the site. That information can then be used to guide the service provider so that the right resources are directed to the right places to ensure service quality–a proven recipe for success.

The Tasty Result

Today's service providers must be agile and offer lower-cost, highly reliable services that enable enterprise IT customers to self-provision service through digitization. 5G networks are the foundation for next-generation business services, leveraging the power of low latency, high throughput, and ultra-reliability. Service providers and IT operations teams also are tasked with managing the complexity of multi-cloud environments. Disaggregated cloud infrastructure is complex, requiring visibility into how every microservice and containerized service interworks so service providers can proactively manage and triage services on the network and guarantee user experience.

Ultimately, service providers and IT teams must be able to ensure that they're meeting service-level agreements on these networks. They need a proven recipe for service assurance that enables them to see everything on the network applications and services running in the cloud, whether hybrid, public, private or multi-cloud.

The complexity of 5G networks and cloudified environments demands that service providers and enterprises employ a proven recipe for service assurance that provides the key ingredient for success on every part of the network. NETSCOUT® has spent 30 years refining that recipe for success. We call it Visibility Without Borders.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SPWP_018_EN-2202 02/2022