SOLUTION BRIEF

# Keysight Cloud-Native Infrastructure Performance Validation

KEYSIGHT

# Evolution to Cloud-Native

New technologies and market demands are changing how networks and services are architected and operated. Cloud-native deployment models are emerging as the foundation of 5G, secure access service edge (SASE), multi-access edge compute (MEC), and enterprise networks.

While cloud-native advancements offer important benefits and opportunities, they also introduce additional layers of complexity and risk factors which can impact service performance and reliability, leading to major disruptions when challenges arise.

## Cloud-Native Infrastructures Are Different, So Is Testing Them

Cloud-native infrastructures are designed to provide a highly scalable, resilient, and agile environment for cloud-based applications and network functions. They represent a significant departure from traditional infrastructure models and require a specialized set of tools and practices to deploy and manage effectively.

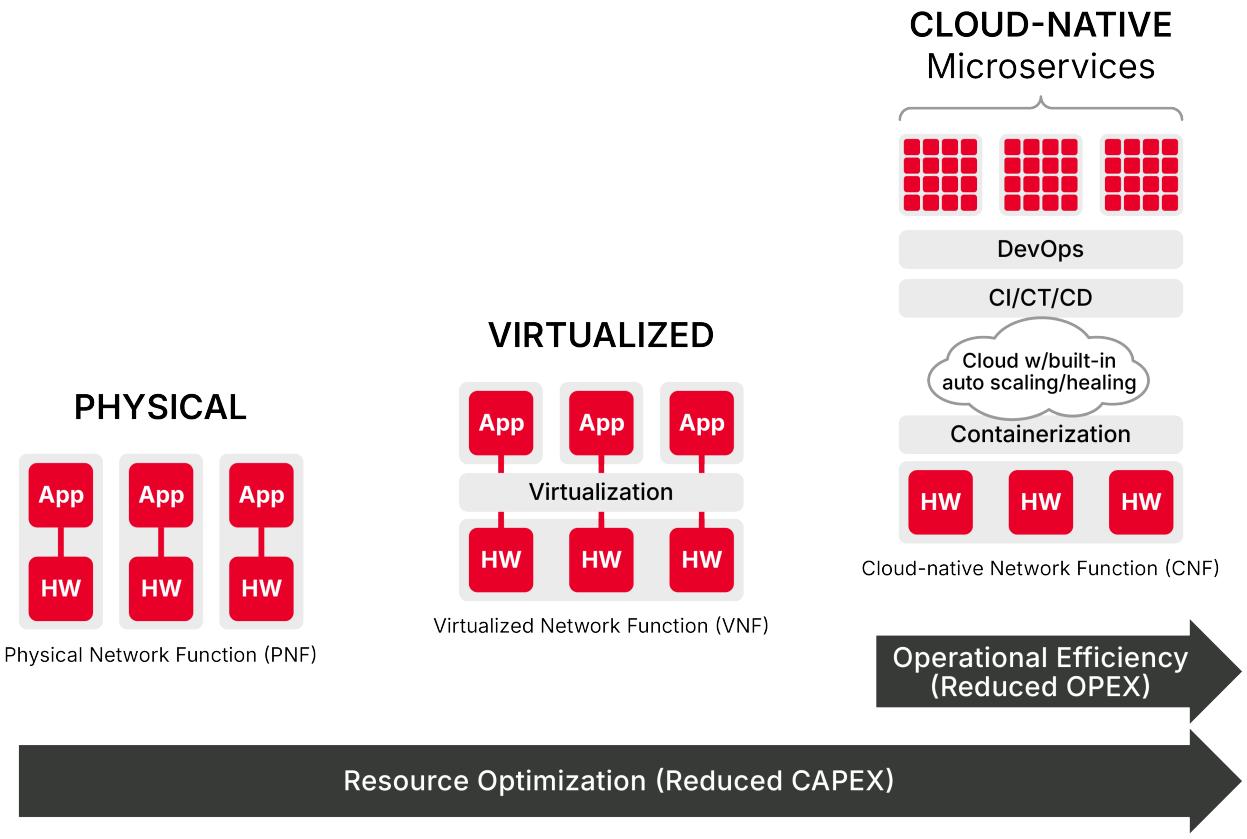


**Figure 1.** Test solutions must rise to a new level of agility and responsiveness to deliver the benefits of the evolution to cloud-native

Cloud-native infrastructure and networking are different from traditional virtualized cloud infrastructures in several ways:

- **Architecture:** Cloud-native infrastructure is typically built on using lightweight a microservices architecture, which breaks down applications into small, independent components that can be deployed and scaled independently. This contrasts with traditional monolithic applications, which are built as a single unit and require significant resources to scale. In this architecture, there is a lot of east-west communication occurring between the microservices that make up the cloud-native application or network functions, and the underlying cloud-infrastructure needs to deliver the performance (throughput, connections/transaction per second and latency) required for high-quality service experiences.
- **Hardware abstraction:** Cloud-native infrastructure abstracts the underlying hardware, allowing the application to be developed and deployed independently. This includes providing tools for managing the resources used by containers, including CPU, memory, and storage, and allowing applications to be deployed and scaled based on their resource requirements, rather than being tied to the specific hardware infrastructure. This flexibility offers network operators many options for compute, NICs, container orchestrators (OpenShift, TANZU, Kubernetes), cloud instances (AWS EKS, GCP GKE, Azure AKS), and CNF options from multiple vendors, potentially leading to increased points of failure. Even a simple upgrade to a newer CPU or a new version on Kubernetes CNIs or Linux distribution can have unexpected consequences on performance. With so many moving parts, troubleshooting and root cause analysis becomes much more difficult.
- **Scalability:** Cloud-native infrastructure is designed to be highly scalable, with the ability to handle rapid changes in demand. This is achieved using horizontal scaling and automatic load balancing, which allows applications to be scaled out or in as needed. This presents a new set of challenges in rightsizing cloud infrastructures, fine-tuning auto-scale policies and optimizing cost, while minimizing disruptions to end-user Quality of Experience (QoE) as cloud-native network functions and services are scaled out and in.
- **Security:** Due to the agile nature of cloud-native environments, security controls that are servicing or securing inter-microservices or inter CNF communications face a unique set of challenges. They now need to handle the elastic, dynamic nature of containers at a much faster and larger scale since cloud-native applications tend to have hundreds of microservices associated with them. Network operators need to ensure security and application policies automatically scale in and out with application assets as soon as they are created, tracking all changes until that resource no longer exists.
- **Resiliency:** The built-in resiliency of cloud-native infrastructures is one its key advantages, however fine-tuning the infrastructure to mitigate the unexpected is a key challenge. In a dynamic cloud-native infrastructure, microservices may restart, scale out, and even be redistributed to a different node. Network operators can't assume they will just work, instead need to ensure they characterize the impact of cloud impairments (e.g., pod failures, node reboots, network latency, CPU spikes, etc.) on cloud-native network functions (CNFs). The goal should be to emulate real-world cloud degradations during preproduction to proactively uncover issues before CNFs are deployed into production networks.
- **Automation:** Cloud-native infrastructure is highly automated with many processes and tasks automated using a continuous integration/continuous deployment (CI/CD) model, to keep pace with the rate of change. Vendors delivering cloud platforms, NFVI, and CNFs are continuously bringing new innovations to market and at much faster rates than ever before. Incorporating continuous and automating testing into the CI/CD pipeline accelerates testing cycles and helps reduce the manual effort required to manage infrastructure, making it easier to deploy and maintain as a result.

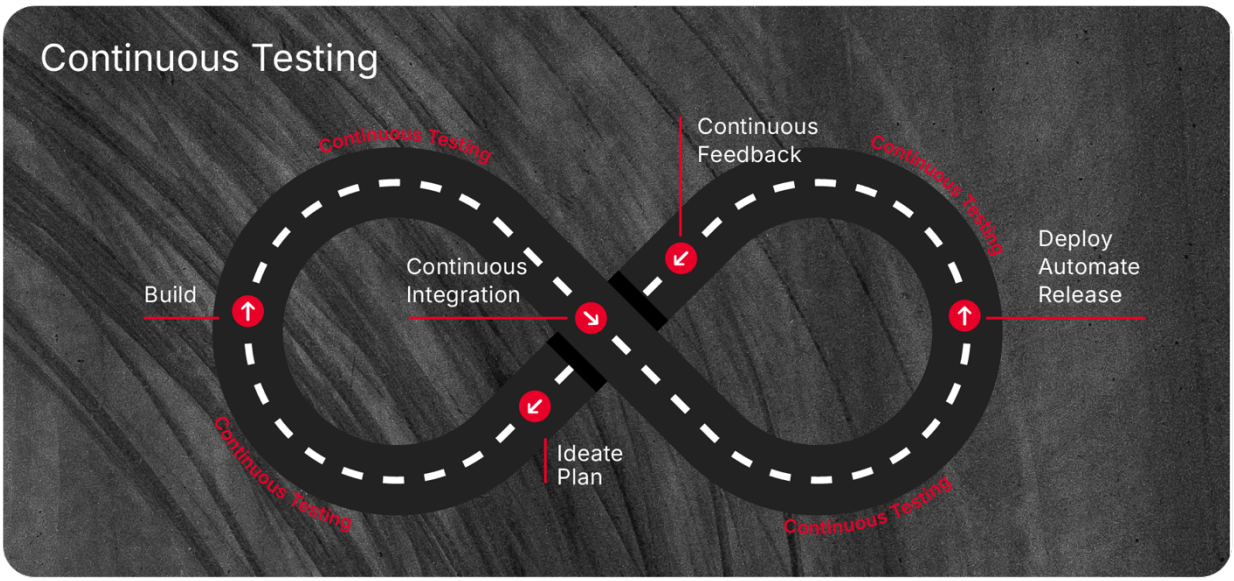


**Figure 2.** Continuous, automated testing is the key to successful 5G cloud-native deployments

Testing cloud-native infrastructure can be challenging, but with the right tools and processes, organizations can ensure their infrastructure is efficient, providing a high-quality user experience, while maintaining security and reliability.

# The Benefits of Testing

Cloud-native infrastructure validation offers numerous benefits to network architects and engineers in service provider or enterprise organizations building and deploying this type of infrastructure, including:

- **Improved infrastructure performance:** continuous, proactive validation will help identify and address performance bottlenecks, enabling network operators to ensure their infrastructure performs optimally, providing high-quality service experiences
- **Enhanced resiliency:** testing also helps identify and address issues with resiliency and fault tolerance, enhancing overall infrastructure reliability as a result, so it is ready to support the multitude of dispersed 5G CNF workloads running on top of it
- **Accelerated time to market:** identifying and addressing issues early in the development process will help accelerate the time required for testing and deployment, enabling service providers to bring new services and features to market faster
- **Reduced downtime and maintenance costs:** baselining cloud infrastructure performance to proactively determine the impact of changes pre and post deployment will save valuable support time by preventing unplanned operational issues and ensuring optimal performance through selection of the right vendor configurations
- **Optimized resource utilization:** gaining insights into how resources are being used will help network operators optimize their infrastructure for maximum efficiency. This can reduce costs associated with over-provisioning resources or under-utilizing them.

# Validation Solution for Cloud-Native Infrastructure Performance

In the new, highly dynamic cloud-native world, Keysight delivers a comprehensive, end-to-end test solution dedicated to validating cloud infrastructure performance, scale, and resiliency. The Keysight Landslide CNF Testing solution enables network equipment vendors, service providers, and enterprises to verify their Kubernetes cloud-native infrastructures, network functions, and services like ingress controller are ready to deliver and maintain required performance and resiliency.

The solution enables users to deterministically exercise the built-in resiliency and self-healing capabilities of cloud-native networks with its real-world cloud impairments. Adding Landslide's realistic and scalable traffic emulation, users can characterize the impact of cloud degradations on performance, QoE, and robustness of CNFs.

Keysight solutions help maximize profitability by right-sizing the infrastructure spend, reducing the number of unplanned operational issues and cost to address them.

# Key Features and Use Cases

- Benchmark the performance and scalability of cloud-native applications, such as NGFW, WAF, IPS/ IDS, LB CNFs using real application workloads
- Measure the maximum throughput and capacity of cloud-native services, such as ingress controllers, by emulating external to cluster traffic emulation (north-south)
- Optimize cloud infrastructure resources, cloud-native instances with the right NIC drivers, Linux distributions, and CNIs
- Measure cloud-native networks directly from within each application's containerized microservice workload with multiple unbounded traffic generation test agents
- Quantify the effect of failures and cloud degradations on key performance indicators for CNFs and in turn Quality of Service (QoS)
- Ensure full automation via API support to seamlessly integrate into any CI/CD pipeline to provide automated, repeatable testing at any deployment phase of new services

Keysight's Landslide cloud-native infrastructure performance validation solution offers quick and simple-to-use performance tests for content-aware networks to:

- Verify your cloud-native infrastructure will deliver expected performance
- Quickly isolate performance issues to specific areas and vendors in your cloud stack
- Understand how to best invest money to improve your cloud's efficiency
- Validate cloud-based services with high load, realistic traffic, and peer device emulation
- Stay flexible with options for a wide range of deployment types

# Balancing the Promise and Pitfalls of Cloud-Native Applications

Cloud-native networking is an innovative development that strives to deliver secure, flexible, robust, and scalable network connectivity. This is achieved by merging the network and application infrastructures into a single, adaptable, and versatile platform. To guarantee optimal network functionality, it is imperative to have a comprehensive understanding of network efficiency.

Cloud-native infrastructure encompasses both the hardware and software necessary for the deployment and operation of cloud-native network functions, including data center servers, storage, networking equipment, and their respective operating systems. Additionally, it involves sophisticated orchestration and management software, such as Kubernetes, which dynamically allocates these resources to cloud-native network functions.

Keysight test solution for cloud-native networks and services is unparalleled in its ability to provide realistic and proactive testing. With the capacity for scalable and accurate emulation of application workloads across various environments, including on-premises, VM, public cloud, and container environments, Keysight solution helps optimize the performance and user experience of content-aware cloud-native networking solutions.