White Paper

Telco CIOs, CTOs, Chief 5G/Edge Architects
Telecom

EnterpriseWeb CloudNFV Shows Edge Automation in Multi-Vendor Test[1]

Team of telecom vendors led by EnterpriseWeb remotely deploys containerized 5G Open RAN with a secure edge gateway and demonstrates optimized processing of secure packets with low latency and power consumption

EnterpriseWeb®

Table of Contents

Background

Network edge computing is not simply an extension of the cloud. It introduces new business use-cases, technical requirements, and opportunities for communication service providers (CoSPs). Similarly, the technology configurations that work for the cloud, core and data center do not always work for the multi-access edge compute (MEC) deployments.

MEC servers have different requirements for power, size, environmental hardening, access to high-speed networking and other factors. These requirements drive compute capacity, server dimensions, storage availability, system security and other configurations.

Another difference is automation, which is mandatory for managing edge networking at scale. Modern network services involve complex coordination and configuration of many participating network functions, supporting services and infrastructure resources. This interplay requires highly dynamic and intelligent orchestration to assure and optimize a network service in a "zero-touch" way.

To maximize the impact of automation, CoSP edge platforms must be cloud-native, edge-optimized, and secure. They need to support deployments on containers, VMs and bare-metal servers. Despite the resource and power constraints of edge sites, CoSPs cannot sacrifice compute agility at the edge.

Accordingly, hard, quantifiable test data is paramount to the design, development and rollout of MEC services. Testing tools need to support advanced MEC requirements, emulate realistic applications and attacks in order to document the performance and efficiency of edge platforms. These tools must be cloud-native, able to be orchestrated, and configurable so that they can be flexibly deployed for a wide-variety of environments and use-cases. The inherent remoteness of edge sites and the potential large numbers of those sites, demands distributable and automated testing to establish confidence and trust in this new frontier of network service delivery.

Intel® Network Builders ecosystem member EnterpriseWeb* developed CloudNFV, an edge orchestration platform that handles the significant orchestration requirements of a containerized 5G RAN network. In a multi-vendor Intel testbed, EnterpriseWeb demonstrates how dynamic configuration of the Intel® Ethernet Controller E810 can optimize secure packet processing for a 5G edge network site, while significantly reducing resource requirements and energy consumption.

CloudNFV Offers No Code Edge Automation

The test focused on the functionality and performance of EnterpriseWeb's CloudNFV 5GS automation platform that supports 5G RAN, MEC and core deployments. As the name suggests, CloudNFV bridges IT and telecom in a comprehensive solution, which includes service management and orchestration (SMO), life cycle management (LCM) and integration-platform-as-a-service capabilities.

CloudNFV is next-generation management and network orchestration (MANO) software based on EnterpriseWeb's no-code integration and automation platform for designing, deploying, and managing distributed edge networks. The software is:

- **Cloud-native:** runs as microservices in a container networking environment.
- **Model-based:** abstracts the network concepts and knowledge that governs a network into a domain model; this capability allows CloudNFV to abstract a wide range of CoSP environments and integrate them with other domains.
- **Event-driven:** CloudNFV uses an event driven programming approach where events or changes in state are communicated to applications, which is designed for distributed application architectures.
- **Policy-controlled:** utilizes shared metadata, relationships and state information for orchestration, automation, and management.

The goal for CloudNFV's umbrella abstraction is to become a single "source-of-truth" about network status and operations for complex multi-vendor, multi-domain, multi-cloud use-cases.

The model-based nature of the software is the source of its many advantages. CloudNFV features a harmonized telecom operational model using standard industry concepts, types, and relationships. This ready-to-use model can be flexibly extended to include existing customer information models.

CloudNFV is comprised of five modules that deploy together as a cluster of pods. The modules are based on common personas to align with typical telecom operations:

- **Model Manager:** Solution architects can maintain and extend the model as their requirements change and technologies evolve. CloudNFV has an extensible graph-connect domain model that includes Red Hat* OpenShift Operator concepts.
- **Application Manager:** IT can rapidly onboard solution elements via CloudNFV's API or UI through an interactive, model-driven process. The platform's type system drives mappings to the domain model. Properties are auto filled, and interfaces are generated. Completion triggers configurable DevSecOps processes. Successfully onboarded elements are registered as loosely coupled, typed objects in the CloudNFV's catalog.
- **Resource Manager:** Operations teams can model server, VM and container-based host environments, as well as networks, which are then exposed as targets for service deployments.
- **Service Manager:** Service designers can select and declaratively compose objects from the catalog into intent-based network services, which are infrastructure independent and protocol agnostic. Service models can also be tested via configurable DevSecOps process prior to registration in the catalog.
- **Task Manager:** Process designers can rapidly model event-driven dataflows, and onboard any required 3rd party engines, to automate processes.
- **Catalog and Active Inventory:** If an order from an operations support system (OSS) for a network service in the catalog explicitly identifies OpenShift as the deployment target, a background utility service generates OpenShift Operators for participating functions/applications to streamline deployment and management via OpenShift, as part of the automated deployment of the service, which is then registered in inventory.

Uses Programmable Ethernet Controllers

In Stage 2 of the testbed, CloudNFV utilizes the programmable networking capabilities of the Intel® Ethernet Controller E810 to optimize secure packet processing for a 5G edge network, while significantly reducing resource requirements and energy consumption. The Intel Ethernet Controller E810 is part of the Intel® Ethernet 800 Series Network Adapters, which support 10, 25, 50, and 100 Gbps speeds, multiple form factors (PCIe and OCP NIC 3.0), and feature broad operating system support.

For the test, EnterpriseWeb used the controller's programmability features, specifically its

- Dynamic Device Personalization (DDP) enables customizable packet filtering for more efficient packet processing.
- Application Device Queues (ADQ) filter traffic into a dedicated set of queues for key workloads, for greater predictability at scale.

Other technology that was used in the testbed includes:

- Red Hat OpenShift is a unified platform to build, modernize, and deploy applications at scale. Red Hat OpenShift provides a complete set of services for bringing apps to market. Red Hat OpenShift brings together tested and trusted services to reduce the friction of developing, modernizing, deploying, running, and managing applications.
- Fortinet* FortiGate provides SD-WAN and 5G user-plane security to address modern systems complexity and threat exposure to protect customers critical business workloads and the underlying network infrastructure. FortiGate delivers fast, scalable, and flexible secure SD-WAN and user-plane on-premises and in the cloud. Fortinet Secure SD-WAN supports cloud-first, security-sensitive, and global enterprises, as well as the hybrid workforce.
- Keysight* CyPerf is a network application and security test solution with lightweight agents deployed across a variety of physical, cloud and containerized environments to deliver unprecedented insights into end user experience, security posture, and performance bottlenecks. By realistically modeling dynamic application traffic, user behavior, and threat vectors at scale, CyPerf validates hybrid networks, security devices, and services for more confident rollouts.
- KX* provided the kdb+ time series database and real-time analytics engine. This technology enabled the testing team to build high-performance data-driven applications and turbocharge analytic, AI, and ML tools in the cloud, on-prem or at the edge.

- Tech Mahindra* is one of the largest independent network services providers and served as the system integrator. Tech Mahindra brought vast experience from its key service offerings in 5G RAN, core and network cloud and from its hyper automation platform, netOps.ai. The company specializes in delivering innovative and customer-centric information technology experiences. Tech Mahindra has more than 151,000 professionals across 90 countries, helping 1,224 global customers including many Fortune 500 companies.

Use-case: Optimized 5G/RAN Network with Secure Edge Gateway

Fortinet's FortiGate is deployed for Open RAN control and user-plane security. As network components scale, heal or are reconfigured to meet changing workloads, CloudNFV dynamically reconfigures FortiGate to allow it to adapt to cover the changing attack surface. Adaptive security supports complex and volatile 5G edge and core deployment.

Day 1 Network Deployment

The day 1 deployment demonstration shows how all the elements of a 5G remote base can be deployed on an Intel architecture-based server including 5G core and radio access networking (RAN) VNFs, along with the Fortinet Secure gateway, CyPerf test agent, and KX's kdb+ time series. Using CloudNFV and OpenShift, all these components were downloaded to the remote server, configured, and then instantiated to turn on the services.

As seen in Figure 1, CloudNFV is deployed from OpenShift which then deploys the required VNFs from the CloudNFV inventory. CloudNFV modeled the components and mapped them to the domain model.

To start the day 1 deployment, an order from the operations support system (OSS) triggers CloudNFV to execute the deployment workflow, which includes:

- Call OpenShift APIs to provision service accounts, management network and storage.
- Generate and deploy OpenShift Operators for all C/VNFs to edge and core.
- Call OpenShift with JSON payloads to provision application specific subnets.

This establishes the infrastructure enabling the platform to then instantiate the service using the following procedures:

- Call OpenShift Operator to deploy ONF 5G-core and RAN as clusters of pods at core and edge.
- Call OpenShift Operator to deploy Fortinet as a VM over containers at edge.
- Call OpenShift Operator to deploy CyPerf agent as a pod at edge.
- Call OpenShift Operator to deploy video host as clusters of pods at core.

With the service-provisioning software in place, CloudNFV then configures the service using a variety of APIs that include:

- Configuring ONF 5G-core and RAN using REST.
- Configuring Fortinet secure gateway via SSH.
- Configuring video host via YAML.
- Registering CyPerf Agent with CyPerf controller and load testing profile via REST APIs.
- Configuring DNS entries for service.
- Configuring Intel Ethernet Controller E810 with optimized policies.

CloudNFV successfully completed all of these actions resulting in a secure 5G edge gateway that was ready for testing.

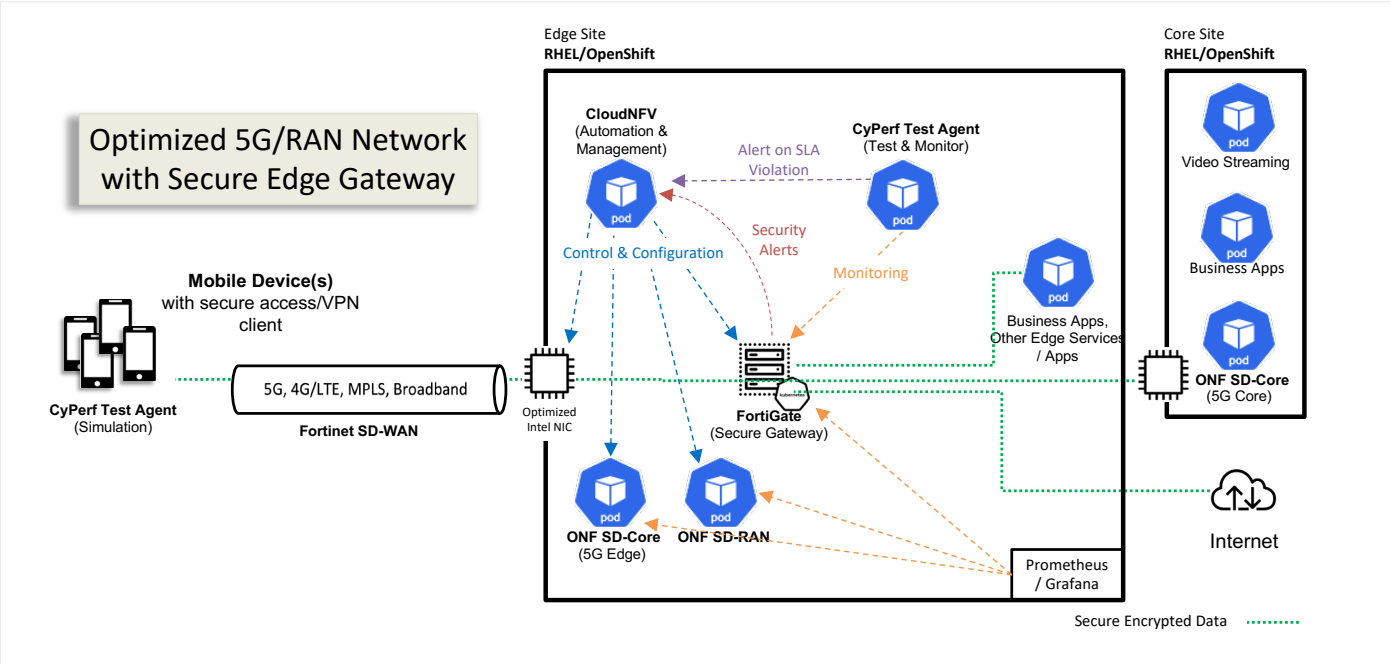

Figure 1. Day 1 deployment diagram showing a complete 5G RAN network being deployed with simulated mobile device traffic.

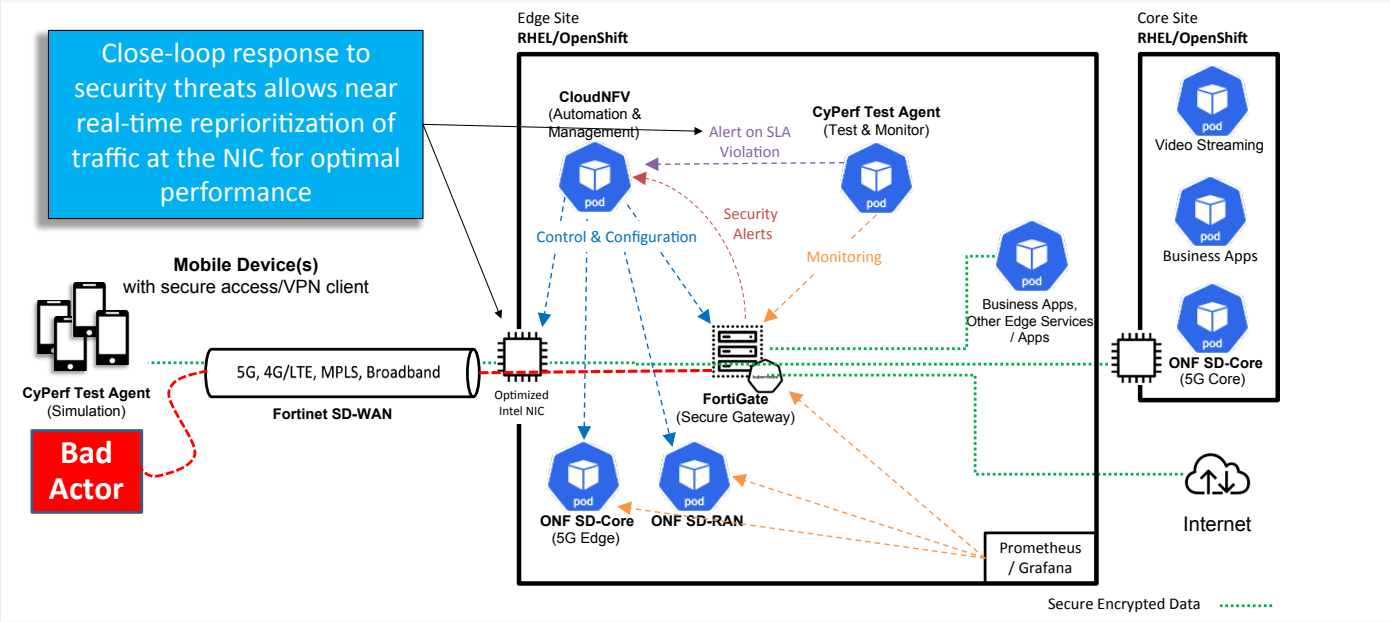

Figure 2. Day 2 deployment is depicted in this image with CloudNFV optimizing the data flows.

Day 2 Operations Testing

Orchestrated by the CloudNFV automation software, Keysight's CyPerf enabled the creation of digital twins that represent configurable users, applications and attack behaviors, emulating realistic traffic at scale.

Once instantiated, the server is live and providing 5G services. The day 2 tests demonstrate CloudNFV's ability to optimize the packet processing latency and power consumption. This is shown in Figure 2, which depicts the CyPerf test agent generating 1 Gbps of data traffic from 1,000 emulated users. CyPerf generated data flows are transported across the SD-WAN to the Intel® Ethernet Controller E810 in the edge site server which passes to the FortiGate secure gateway before being processed by the 5G core functions or the other business/edge apps.

Through the entire process, CloudNFV is providing control and configuration monitoring on the dataflows with Prometheus tracking the KPIs and other operational statistics made available to network technicians via a Grafana dashboard. The CyPerf test agent tracks the emulated dataflows to detect service level agreement (SLA) issues, and feeds that information with performance results into CloudNFV so it can instruct the network adapter to prioritize this data.

Traffic from a CyPerf emulated bad actor is added to this data flow to measure its impact on the latency and throughput. This traffic is detected by the FortiGate secure gateway which informs CloudNFV which then communicates with the network adapter to adjust the data priorities to improve performance.

The findings from this test show that latency for the service was 141µs. When CyPerf started to emulate the cyber-attack, the FortiGate secure gateway was able to block 98% of the attacks, and the dynamic re-prioritization of these packets by the network adapter resulted in a latency increase of only 15% to 163µs during the cyber-attack. The ability of CloudNFV to program the network adapter to optimize the packet processing also led to a 26% decrease in power consumption.

Day 2 Test Results:

- Service latency: 141µs
- Cyber-attack blocking percentage: 98%
- Service latency under attack: 163µs

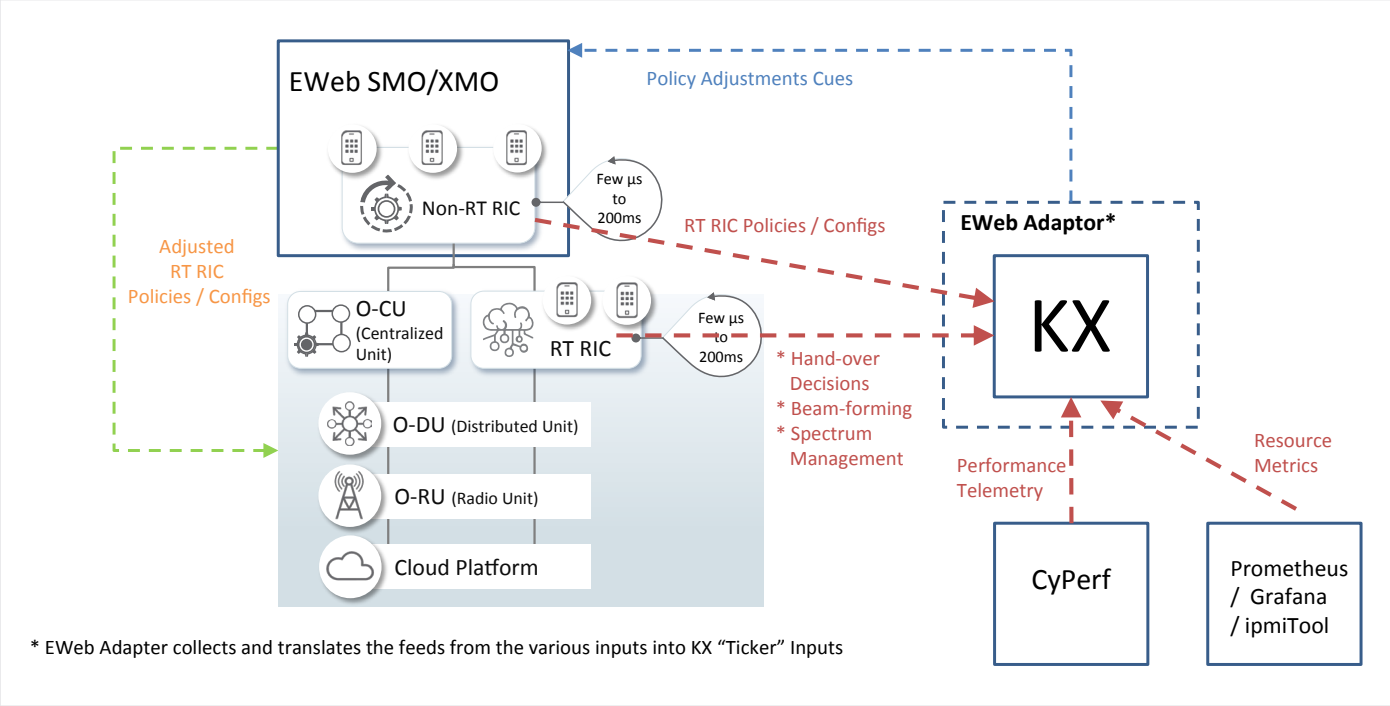

Figure 3. CloudNFV manages SON functionality to improve packet latency and reduce power.

Optimizing the RAN for Lower Latency and Power

Building on this testing, the EnterpriseWeb team expanded its optimization to improve RAN performance with the addition of self-organizing network (SON) functionality (see Figure 3). The real-time analytics engine of KX's kdb+ time series database used policy and configuration inputs from the CloudNFV RAN intelligent controller (RIC), hand over, beam forming and spectrum management data from the RAN centralized unit (CU)and performance telemetry from CyPerf. Using AI, this SON function sent policy adjustment information back to CloudNFV that was used to adjust the RAN functions.

This solution was then tested in a lab with no physical radios present using CyPerf to generate 10Gbps of realistic application traffic from 1,000 emulated users. Table 1 shows the latency and power reduction benefits of this system compared to the stage 1 test results.

	Stage 1	Stage 2	Difference
Total Throughput (simulated mix of Video, HTTP & REST traffic)	1Gbps	10Gbps	10x more traffic
Latency	141µs	137µs	2.8% improvement
Latency under Attack (simulated bad actor attempts exploits)	163µs	158µs	3.1% improvement
Block Rate	~98%	~98%	Same high level of security
Power Reduction from Optimizations*	26%	33%	Additional 7% power savings
Power Consumption per Gbps Throughput	1069 kW/h	113 kW/h	~9.5x more efficient
CPU Consumption per Gbps Throughput	54 cores	7.1 cores	~7x more efficient
RAM Consumption per Gbps Throughput	89 GB	11.7 GB	~7.5x more efficient

* Average power consumption across all tests of unoptimized vs optimized traffic on otherwise identical hardware, network functions and workloads.

Table 1. Test results.

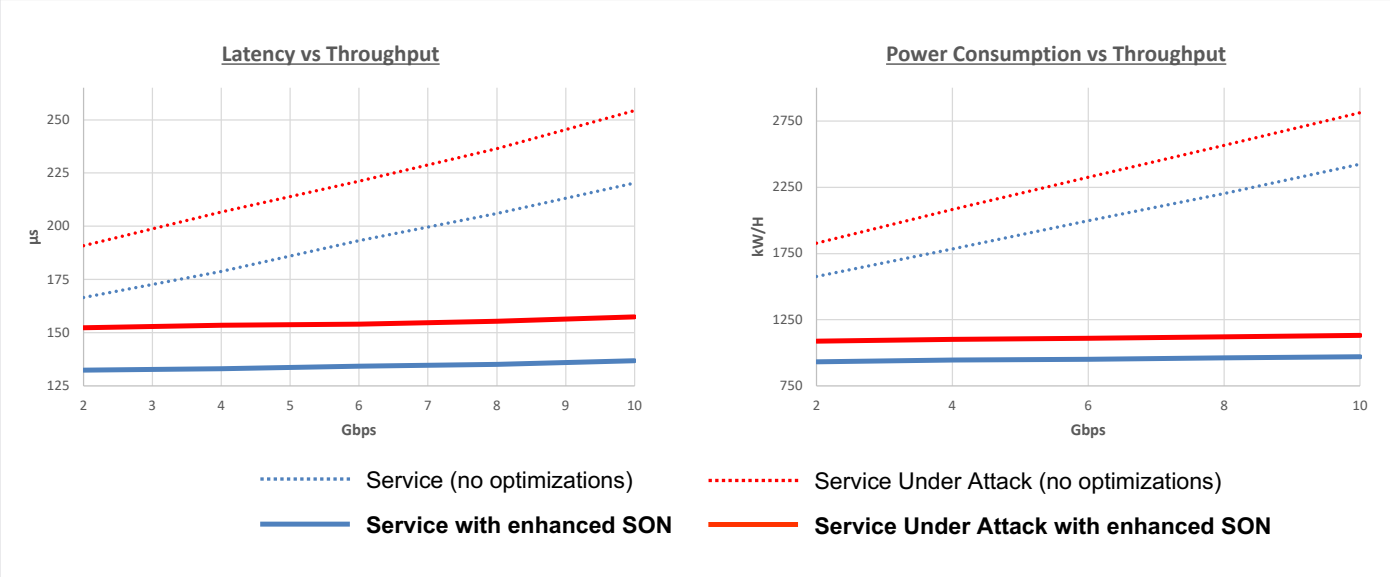

Figure 4. Latency and power consumption test results (Lower is better).

The results show that adding the enhanced SON functionality improves latency even with 10 times more traffic even while under attack from a bad actor. This point is illustrated more clearly in the test results shown in Figure 4 where latency and power consumption stay relatively flat despite the increased throughput and attacks.

Conclusion

For optimal performance, edge server automation must both deploy the software required for services and manage and optimize that software throughout the service lifecycle. In tests on a 5G base station conducted by EnterpriseWeb, its CloudNFV automation software, in conjunction with KX's kdb+ time series database, shows successful use-case deployment and the ability to optimize system latency and power consumption both in normal operation and while under a cyber-attack. With the addition of SON capability, further improvements were made to the data flows to show latency and power consumption reduction capabilities at 10Gbps. EnterpriseWeb's CloudNFV leverages the programmability of the Intel® Ethernet Controller E810 to make on-the-fly network changes to respond to changes in the network.

Learn More

EnterpriseWeb

Red Hat OpenShift

Fortinet FortiGate Secure SD-WAN

Keysight CyPerf

KX

Tech Mahindra

Intel® Ethernet Controller E810

[1] SUT1: 5-node, 200 total CPU cores on (1x) Intel® Xeon® 6338N and (4x) Intel® Xeon® Scalable 6238R, Intel® Ethernet Controller E810, with 1.5 TB total DDR4 memory, HT off, Turbo off, RHEL OS 9.0 (5.14.0-70.13.1) with 5 TB total storage, tested by EnterpriseWeb on 09/20/2022.

SUT2: 5-node, 200 total CPU cores using Intel® Xeon® E5-2699, Intel® Ethernet Controller E810), with 1.5 TB total DDR4 memory, HT off, Turbo off, RHEL OS 9.0 (5.14.0-70.13.1) with 5 TB total storage, tested by EnterpriseWeb on 09/20/2022.

Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

0423/LV/H09/PDF ♻Please Recycle 355127-001US