SOLUTION BRIEF

Network Analytics

# Intelligent Edge Shows Power of Splunk Analytics for Enterprises

**Two use cases exhibit security, resiliency, and WAN optimization applications of Splunk Analytics. System utilizes software from Intel® Network Builders partners ADVA, Dell Technologies, Fortinet, and Nuage Networks.**


Data analytics are evolving to automate management of universal customer premises equipment (uCPE) edge network compute nodes. The applications for uCPE are growing, but success with these remote deployments is dependent on cost-effective management of these systems. Splunk offers a powerful analytics platform that enables communications service providers (CommSPs) and the enterprises that they serve to gain end-to-end visibility of their uCPE infrastructure, WAN connections, security, and other applications, with automatic response when network events violate network policies.

## Analytics Needed for Growing uCPE Deployment

More data is created and consumed at the edge of the network, driving demand for uCPE local compute. Growth in internet of things (IoT) devices, video surveillance, branch office computing, and high-speed, private 5G wireless networks are providing the impetus for the expanding market for uCPE. At the same time, network functions virtualization (NFV) and software defined networking (SDN) are maturing and providing cost effective ways to deploy uCPE and manage the lifecycles of edge-delivered services.

What is still needed for edge computing to fulfill its promise? Reducing the cost and lag time for network management is still a critical issue. When a resiliency, security, or network congestion issue impacts an edge server, network management software reports this data to a network administrator who can take action. However, that action might be too late to avert an issue with either equipment failure, packet loss, or a successful malicious attack.

To show how a uCPE analytics solution can increase levels of visibility for business operations, Intel implemented an edge-IoT reference architecture that uses Splunk Analytics to aggregate platform telemetry data from a Dell EMC Virtual Edge Platform 4600 (VEP4600), along with NFVI OS telemetry from ADVA Ensemble Connector and application data from the Fortinet FortiGate firewall VNF and the SD-WAN 2.0 VNF from Nuage Networks from Nokia, and support remediation as described below.

## Building the uCPE Reference Configuration

Edge network analytics improve the management of remote compute nodes. Analytics applications process telemetry data from hardware platforms, applications, and data flows and compare that data against business policies to provide real-time visibility and historical insights into a wide range of security, reliability, and network activities. Analytics at the network edge allow for smarter planning, faster issue resolution, and better decision making, ultimately resulting in improved edge service throughput, reliability, and data security.

The system shows the analytics capability of Splunk in two edge network use cases that involve anticipating and avoiding a hardware failure to improve system

reliability and altering security policies, or re-routing data traffic in direct response to a potential security threat.

The components of the system include the following:

**Dell EMC Virtual Edge Platform 4600 (VEP4600)** server is purpose-built for next-generation uCPE deployments, including hosting SD-WAN and other virtual network functions (VNFs) like routing, firewall, or deep packet inspection. The VEP4600 uses an Intel® Xeon® D-2100 processor, which brings the advanced intelligence of the Intel Xeon Scalable processor architecture into an optimized, dense, low-power system-on-a-chip (SoC) form factor for environments constrained by space and power. The 1-RU-high server offers hosted virtualized network functionality for either CommSP edge applications or enterprise branch deployments.

**ADVA Ensemble Connector** is a complete network function virtualization infrastructure (NFVI) solution that is designed to host multi-vendor VNFs. The Ensemble Connector supports OpenStack controller and OpenStack Compute for cloud services. Virtualization is done using Kernel-based Virtual Machine (KVM)/Quick Emulator (QEMU). Ensemble Connector provides its own high performance and fully featured virtual switch that is compatible with standard VNFs. The Ensemble Connector also has zero-touch provisioning and other operational features for simplicity and scalability. The platform comes with advanced networking support, including MEF Carrier Ethernet 2.0 compliant services, support for popular virtual routing protocols, and for industry-standard encapsulation and tunneling formats.

**Fortinet's FortiGate VNF** delivers significant increases in application and carrier security performance through innovative security processing optimizations and the latest packet processing acceleration technologies. The FortiGate VNF provides comprehensive and advanced layer 7 network security capabilities, including threat protection, intrusion prevention, web filtering, and application control. The software has a small footprint, boots within seconds, and requires minimal storage, thereby helping service providers to cost-effectively protect their virtual networks and cloud platforms.

**Nuage Networks SD-WAN 2.0** is based on the company's Virtualized Network Services (VNS) SDN solution, and builds on the Network Services Gateway (NSG), which uses Intel® architecture-based branch hardware. When connected to the network, the NSG VM calls for a policy engine and downloads a pre-defined configuration based on location. SD-WAN 2.0 transcends basic WAN connectivity and enables IT services across all parts of the network. Enterprises can use SD-WAN 2.0 for connectivity, visibility, and control from a single interface and to orchestrate enterprise IT services in data centers, public clouds, and enterprise branch sites. SD-WAN 2.0 automates and manages connectivity to branch offices and also includes seamless WAN connectivity, including MPLS, 4G/LTE, or broadband connections, allowing users to access data centers, SaaS, and public cloud providers. SD-WAN 2.0 also provides a platform for deploying such value-added services as voice-over-IP, next-generation firewall, Wi-Fi access, and IoT.

**Splunk** turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, analyze, and act on data at any scale, from any source over any time period. The Data-to-Everything Platform removes the barriers between data and action, so customers—regardless of size or business—have the freedom to deliver meaningful outcomes across their entire organization. Splunk's unique approach to data has empowered companies to improve service levels, reduce operations costs, mitigate risk, enhance DevOps collaboration, and create new product and service offerings.

The components are deployed as shown in Figure 1.

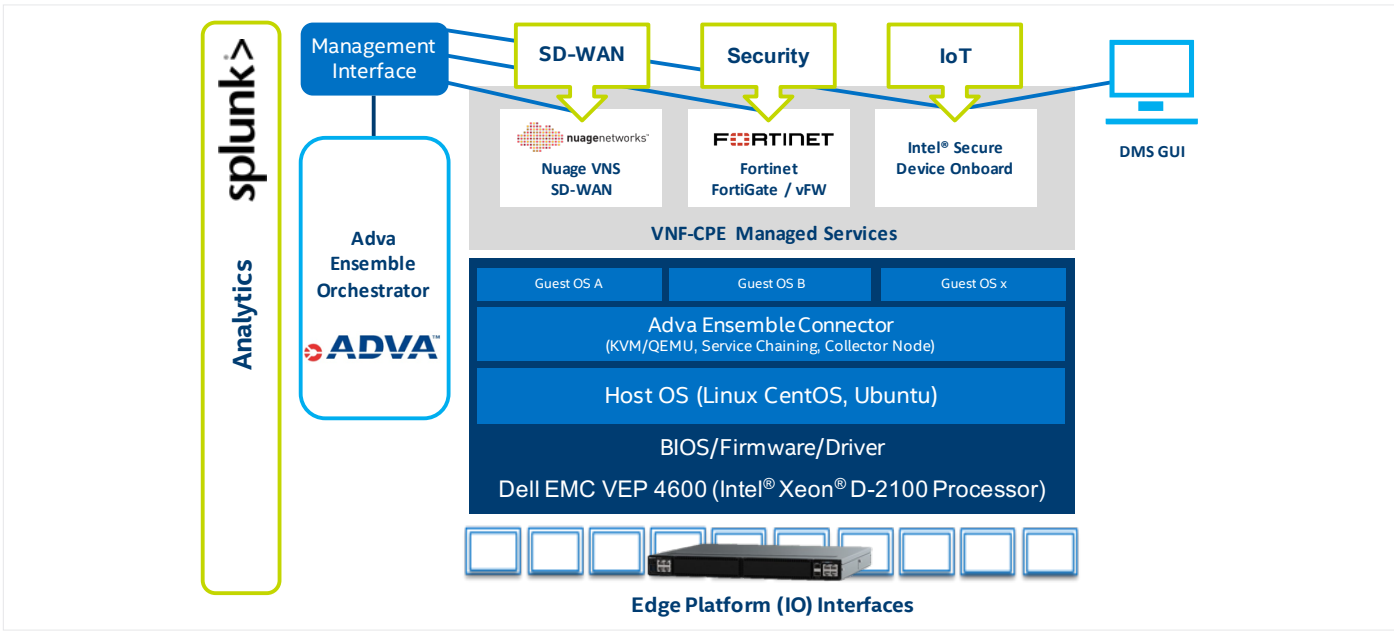


**Figure 1.** uCPE reference configuration block diagram.

Another element of the platform is support for Intel® Secure Device Onboard (Intel® SDO). This system features a zero-touch onboarding function that automatically begins the process once enabled hardware has been powered up and connected to the internet. The Intel SDO agent connects to a centrally located Intel SDO rendezvous server for authentication and then is redirected to a device management system (DMS) to download the entire software stack.

Intel SDO is designed to onboard IoT devices quickly, more securely, and without the need for technical skills at the remote destination. Intel SDO offers support for CPUs from multiple vendors and utilizes Intel® Enhanced Privacy ID (Intel® EPID) for secure device ID. Intel® SDO contributes to reducing uCPE deployment and management costs.

## Supporting Two Edge Network Use Cases

Two recently demonstrated use cases show how Splunk can be used to improve security or network operations.

**Use Case 1: Platform Resiliency:** In this use case, a matrix multiplication application (stress-ng) is deliberately run to mimic a compute intensive workload. It is designed to stress the CPU, triggering various platform resiliency KPIs like last level cache (LLC) load misses and others that lead to increased CPU core temperature. The application itself will also start to consume cache and memory bandwidth resources on the platform, degrading the performance of other applications trying to operate within their SLAs. In addition, synthetic memory errors are injected into the system using the mce-inject tool to simulate a failing DIMM; these synthetic errors are injected at the software level to test machine check handling code. All of these issues can be picked up via Intel® platform telemetry plugins for Collectd that sends the metrics and events to Splunk to ingest and generate graphs, reports, and alerts visible on Splunk dashboards for use in operations centers. The end goal is to enable an automated closed loop workflow that takes real-time action based on operational needs.

**Use Case 2: Responding to Malicious Activity:** This use case utilizes the Fortinet FortiGate VNF, which has a Splunk forwarder. A malicious attack is simulated with the event log pushed to Splunk. Splunk then determines that a new firewall rule must be created in order to respond to the attack. Examples of rules updates include blacklisting of specific source MAC addresses in the event of denial-of-service attack. Splunk pushes this back to the FortiGate, which implements the new rule. Splunk continues to receive information from the forwarder and monitors the firewall to determine the impact of the new rule.

The use cases are illustrated in Figure 2.

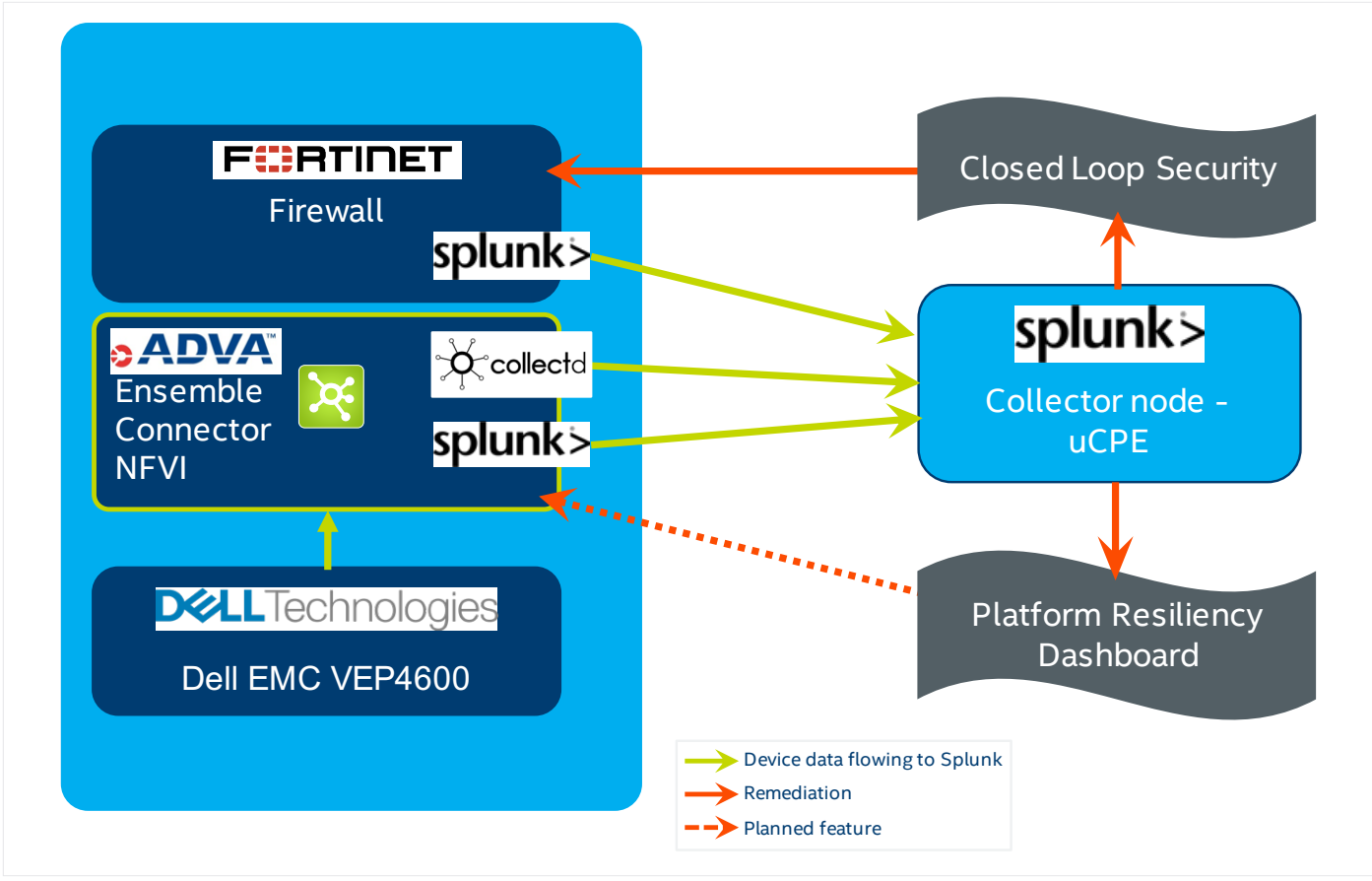


**Figure 2.** Use case block diagram

As shown in these two use cases, analytics from Splunk facilitate direct action when network conditions violate business rules and policies. Overall, the system showed how Splunk can be integrated with an NFVI OS from ADVA and a wide range of VNFs, including Fortinet, to simplify network deployment and manage service lifecycles.

## Conclusion

Capturing insights to trigger near-real-time data-driven decisions at the edge is a game changer. This partnership delivers on that vision. To drive new revenue opportunities, CommSPs can look to high levels of integration with this combined uCPE solution to support trends in growth of IOT devices and 5G wireless networks as well as many other expansions of technology across their customers' networks. At the same time, this solution can address CommSPs' need to continue to support and expand NFV for cost-effective ways to deploy uCPE and manage the lifecycles of edge-delivered services for their own networks, as well as offering this solution to their enterprise customers.

## For More Information

ADVA Ensemble Connector: https://www.adva.com/en/products/network-virtualization/ensemble-connector

Nuage SD-WAN 2.0: https://www.nuagenetworks.net/products/virtualized-network-services/

Fortinet FortiGate VNF: https://www.fortinet.com/products/next-generation-firewall.html

Splunk: https://www.splunk.com/

Intel® Platform Telemetry: https://wiki.opnfv.org/display/fastpath/Barometer+Home

Dell EMC Virtual Edge Platform 4600: https://www.dell.com/en-us/work/shop/povw/virtual-edge-platform-4600

Intel® Network Builders: https://networkbuilders.intel.com

Intel Xeon D 2100 processor: https://www.intel.com/xeond


0220/DO/H09/PDF ♻ Please Recycle 342627-001US