Industry Report

2018 NFV Report Series Part 3: State of the VNF Ecosystem

The Trusted News and Resource Site for SDx, SDN, NFV, Cloud and Virtualization Infrastructure

Table of Contents

contents

Featured VNF Report Products

Acceleration, Optimization, Caching Products

Network Services

IMS and VoLTE Products

Mobile Packet Core / Gateways

SD-WAN and Virtual CPE (vCPE) Products

Security Products

Service Assurance and Monitoring Products

vRAN / cRAN Products

vRouters / vSwitches

Solution Suites (multi-function) or Other VNF Category

AVI Networks®

avinetworks.com

INTENT-BASED APPLICATION SERVICES PLATFORM

Software Load Balancer

Intelligent WAF

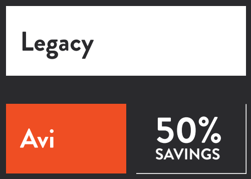
Elastic Service Mesh

Across Any Cloud

x86 / VM / Container / Public Cloud

90% Faster Provisioning

Built-in Analytics and Automation



50% Lower TCO

On-demand Auto Scaling

HIGH PERFORMANCE
FOR HIGH EXPECTATIONS

Executive Summary

Communication service providers (CSPs) worldwide continue to invest in virtualization of their network infrastructure, laying the groundwork for 5G and IoT services. Some have even taken the lead in accelerating service development on top of existing standards, thereby jumpstarting extensions to existing standards and defining new ones with their contributions. Moreover, CSPs continue pushing vendors to disaggregate specialized networking equipment in favor of open architectures.

This final installation in the NFV Report series covers the latest in network functions virtualization (NFV) virtual network functions (VNFs), the workhorse of NFV. These are the actual network functions that provide the desired network services. VNFs benefit from the underlying NFV Infrastructure (NFVI) that hosts these services and provides the appropriate virtualization capabilities as well as NFV MANO that orchestrates and manages the VNFs and the NFV Infrastructure to roll out NFV services.

CSPs and vendors have been working hard to build out new VNFs and enhancing existing ones with features and performance capabilities. They are also taking advantage of underlying capabilities in the NFVI and hardware where appropriate. However, new challenges have emerged like VNF silos, VNF onboarding, and VNF workload placement, the impact of which are being tackled by the standard bodies, CSPs and vendors alike.

In the meantime, CSPs are seeing more momentum in implementations as they migrate from proofs of concept into productions. CSPs are pushing their vendors to address these with alacrity. Some of the more popular VNFs continue to be virtual CPE/SD-WAN and virtual evolved packet core (vEPC). In addition, newer VNFs like vRAN/cRAN (virtual and cloud radio access networks) that can dramatically reduce the cost for an operator while giving them flexibility are gaining attention from CSPs and vendors alike.

On the business side, hardware vendors are still wary of over-investment in VNFs, especially if they currently have a profitable hardware offering consisting of similar capabilities. The VNF pricing and licensing is still work in progress and there is much more to be done. Accounting for VNF use and figuring out how to charge continues to be an area of active development.

The market in 2017 and early 2018 has moved forward rapidly. CSPs are taking charge of some of the slower moving standards and moving forward with gusto with their own implementations, and they are also moving forward from POCs to productions aggressively. The market has also seen successful exits of some NFV startups into larger vendor ecosystems along with the emergence of new VNF solutions. This all points to 2018 being a robust year for this market.

Introduction

Welcome to our 2018 network functions virtualization (NFV) report series covering NFV virtual network functions (VNF). NFV has proven to be compelling for communication service providers (CSPs) worldwide because of its promise to fulfill the networking needs of a service provider on standard server and storage infrastructures. New services only require simple software installation and no additional purchase of proprietary telecoms equipment.

Across our three-part NFV report series, we've covered how vendors and CSPs alike have made significant investment across the board, ranging from industry-standard commercial off-the-shelf (COTS) hardware, to hypervisors and virtualized infrastructure managers (VIMs), to VNFs and the management and orchestration (MANO) necessary to deploy these functions.

This report provides an update on the VNF market and key trends in 2018. If you missed the first part of the report (Part I – NFVI and VIM), or the second in the series, (Part II – MANO) you can download copies of the 2018 NFV Report series from our website at https://www.sdxcentral.com/reports.

Launched in January of 2013 by the ETSI ISG, NFV comprises of the following major components:

- **NFV Infrastructure (NFVI)**—The physical resources (compute, storage, network) and the virtual instantiations that make up the infrastructure.
- **VNFs**—The software implementation of a network function. This report will focus on this aspect.
- **NFV MANO**—The management and control layer that focuses on all the virtualization-specific management tasks required throughout the lifecycle of the VNF.

To bring you this report, we analyzed hundreds of our news and analysis articles, relied on in-depth interviews with technology vendors and end-users, and analyzed the results of the annual SDxCentral NFV Survey. In addition to an overview of the technology and an analysis of customer expectations, we also collected data from the leading NFV vendors. The product information from technology vendors is available at the end of this report.

What you can expect from this report:

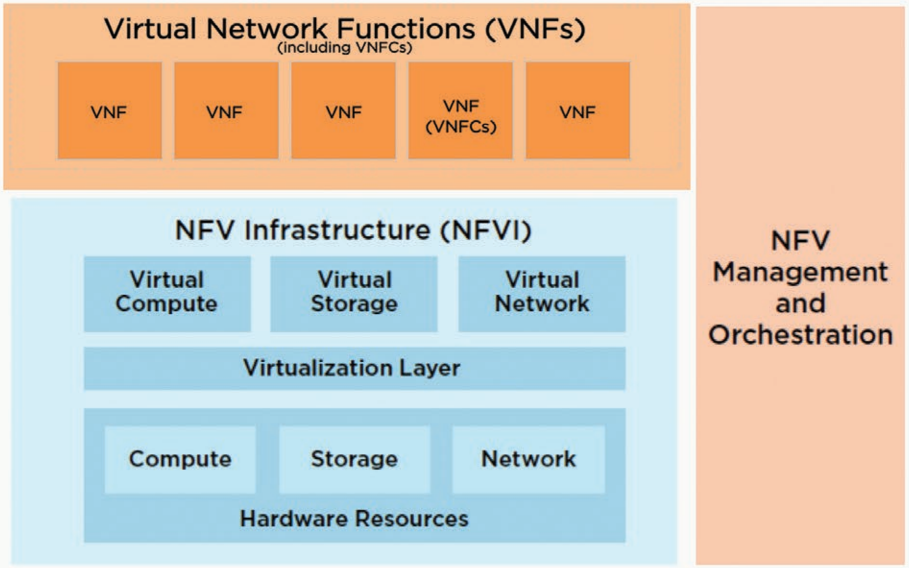
- A primer on VNF
- Business benefits from deploying VNFs
- A quick survey of the top VNF use cases
- Discussion around VNF migration challenges
- Market dynamics for VNFs and NFV survey results
- Conclusions and prognostication for 2018
- Details on popular VNF offerings from leading vendors

Thank you for reading or downloading this report, we hope you will find it a useful resource as you look to understand and adopt NFV technologies. Should you have feedback for our research team, feel free to reach out to us at research@sdxcentral.com.

A Quick VNF Primer–The Virtualization Framework

A lot of the terminology surrounding NFV can be confusing, and we hope this VNF primer will help with VNF basics. At the core of any NFV implementation is a set of application images that need to be managed. Each of those images is made up of elements known as VNF components (VNFCs). Those components can be combined in multiple ways to create a VNF that can be deployed anywhere to provide a networking service that previously would have required a dedicated physical appliance to deliver. In some instances, a VNFC is a discrete networking function, but a VNFC can also manifest itself as a more granular set of functions that could combine to create a larger VNF.

NFV FRAMEWORK AND ROLE OF VNFs



sdxcentral.com

Those VNFs are then centrally managed via a NFV framework that provides a layer of MANO that can be applied across multiple VNFs. That approach effectively creates a layer of isolation between the VNFs and the management and control planes employed to manage them that makes it simpler to both scale VNF deployments in addition to providing the control plane through which VNFs can interoperate with one another.

VNFs in VMs and Containers

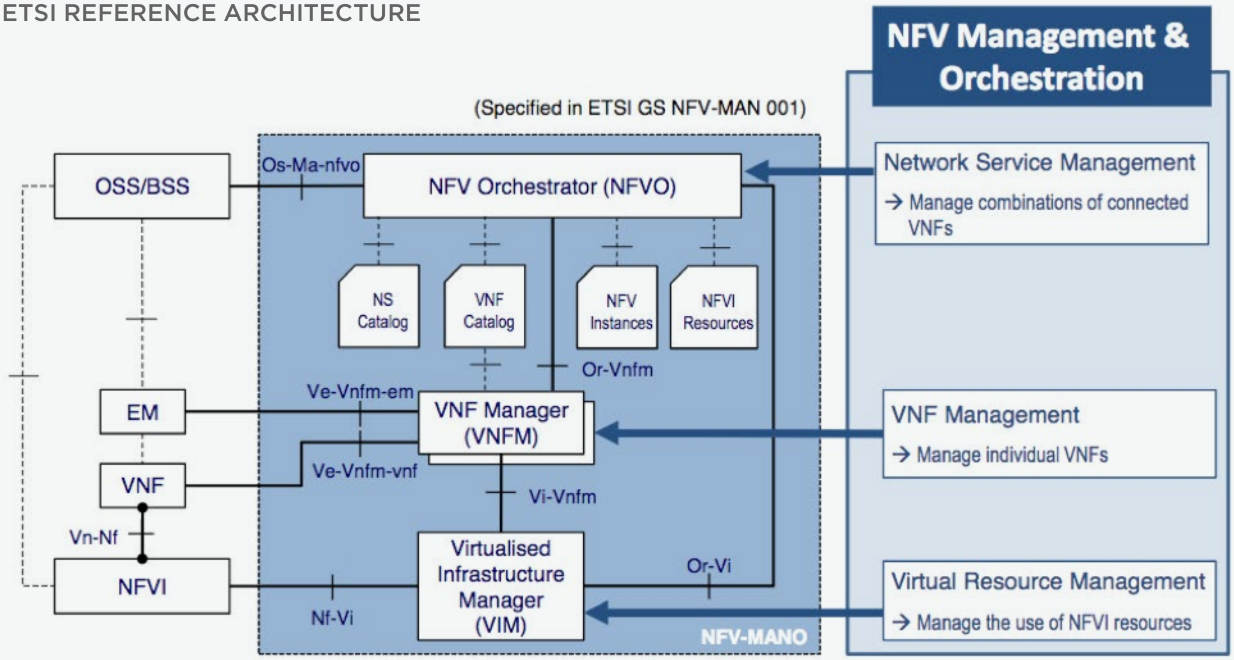
Generally speaking, in most NFV deployments, VNFs are hosted as individual or a collection of collaborating virtual machines (VMs). These VMs are hosted on the NFVI foundation, often in a combination of a hypervisor providing virtualization capabilities along with some NFVI orchestration and management (like OpenStack or VMware's vCloud NFV). These VNFs are managed by appropriate VNF managers (VNFMs) and coordinated through NFV orchestrators (NFV-O). However, we are seeing the emergence of Linux container technology as a viable alternative platform for these VNFs, reducing dependence on VM technology. Nevertheless, container technology for use in NFV is still relatively new and we expect to continue to see most NFV deployments using VM technology.

VNF Relationship to Software-Defined Networks (SDN)

The NFV framework is a virtualization framework that was initially aimed at telco workloads. Many organizations also deploy NFV frameworks in conjunction with software-defined networking (SDN) frameworks that span both physical and virtual appliances, including routers and switching gear. That approach not only makes it simpler to manage a heterogeneous networking environment, but also provides a consistent set of application programming interfaces (APIs) that can be invoked to programmatically control various elements of the network in a consistent manner.

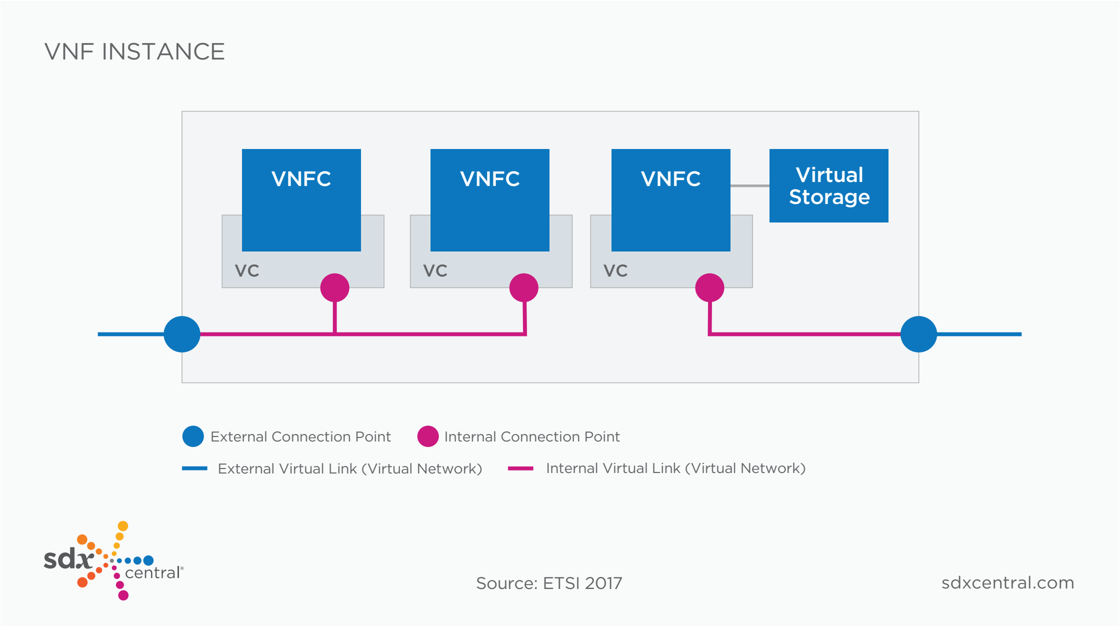
Let start with the ETSI reference architecture shown below.

ETSI REFERENCE ARCHITECTURE


NFV Management & Orchestration
(Specified in ETSI GS NFV-MAN 001)
OSS/BSS
Os-Ma-nfvo
NFV Orchestrator (NFVO)
Network Service Management
→ Manage combinations of connected VNFs
NS Catalog
VNF Catalog
NFV Instances
NFVI Resources
Or-Vnfm
Ve-Vnfm-em
EM
VNF Manager (VNFM)
VNF Management
→ Manage individual VNFs
VNF
Ve-Vnfm-vnf
Vi-Vnfm
Vn-Nf
Virtualised Infrastructure Manager (VIM)
Or-Vi
NFVI
Nf-Vi
Virtual Resource Management
→ Manage the use of NFVI resources
NFV-MANO

Source: ETSI 2017

As seen previously, the NFV instance (or VNF instance) is really one of three things - compute, network or storage. A VNF instance could be made up of a single or multiple VNFC or VNF components.

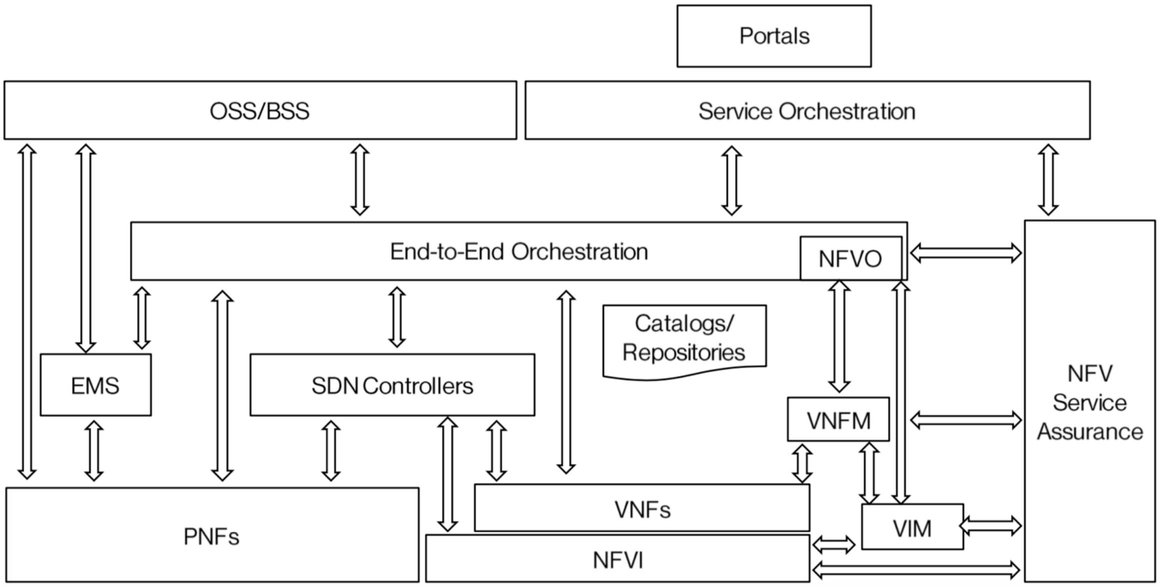

VNF INSTANCE
VNFC
VNFC
VNFC
Virtual Storage
VC
VC
VC
● External Connection Point
● Internal Connection Point
External Virtual Link (Virtual Network)
Internal Virtual Link (Virtual Network)
sdx central
sdxcentral.com

Source: ETSI 2017

The same function - say a Load Balancer or Application Delivery Controller - can be realized through a single VNFC by one vendor or through two VNFCs (one each for control or data plane) by another. The software architecture is very flexible and each vendor's NFV implementation is reflective of its architecture and competitive differentiation. In both situations, the VNFs have to be attached to the network in some fashion, and this is where SDN often comes in.

If we integrate VNF/VNFCs in an SDN reference architecture, we'll end up with a deployment similar to the following.

VERIZON SDN-NFV HIGH-LEVEL REFERENCE ARCHITECTURE



Source: Verizon

In this architecture, the SDN controller is used to direct the underlying network to drive traffic to the appropriate VNFs, often chaining these VNFs together as part of a service function chaining (SFC) implementation. SFC essentially provides the means, via SDN, to route traffic from one VNF to the next, creating a chain of inter-dependent functions that operate on a series of network flows. For example, one such SFC flow might include a firewall, followed by a carrier-grade network address translation (CG-NAT), and then some type of cache; all of those VNFs collaborate to provide secure, safe, and optimized traffic for fixed or mobile networks.

In the real-world, there has been some strong headway made by CSPs like AT&T, SK Telecom, Telefonica and Verizon to name just a few. They have taken these reference architectures and turned them it into monetizin business models.

NFV VNFs and ETSI

The interaction of VNFs with the overall NFV framework is defined by the European Telecommunications Standards Institute (ETSI). ETSI is currently working toward its Release 3 specification, which focuses on operationalizing NFV. ETSI is expected to finalize the specification in the first half of 2018.

ETSI's work builds on the published Release 2 specification, which focused on interoperability. In Release 2, ETSI added the requirements for the interfaces identified in the NFV architecture framework along with the interface specifications for information models to be employed in management and orchestration. Specific functional requirements applicable to the virtualized infrastructure management, the VNF manager and NFV orchestrator, were identified along with requirements, interfaces and information models associated with, for example, virtualized resources management and change notifications; virtualized resources fault and performance management; VNF packaging and software image management; VNF lifecycle management and change notifications; granting of VNF lifecycle operations; VNF fault, performance and configuration management, network services lifecycle and change notifications; and a VNF descriptor information model.

The latest version of the Release 3 of NFV specification that was released in the fall 2017, addresses the following elements:

- address information modeling end-to-end multi-site services management
- automated deployment of element management and other OSS functions
- additional aspects of management and orchestration
- NFV acceleration technologies
- management of NFV MANO
- management of network services and connectivity
- service orchestration and network service orchestration
- network acceleration for VNF
- security management and monitoring for NFV
- secure sensitive components in NFV framework
- update and upgrade of NFV software
- VNF snapshotting
- interoperability, conformance testing and benchmarking
- hardware environment for NFV
- hardware independent acceleration, policy management framework, application and service management, hypervisor-based virtualization
- license management

- NFV MANO admin domains
- NFV architecture PaaS
- cloud native VNF
- network slicing in NFV
- NFV reliability and availability
- identity management

That is an extensive list of addressed items and demonstrates how far the technology has matured since the original NFV framework was defined in 2013.

Finally, ETSI also works with external communities, including other standards bodies like the MEF, TMForum and open source projects, including many hosted by Linux Foundation, in addition to starting work on a framework for interoperability assessment.

As crucial as all this work is, however, service providers are not waiting for standards to be fully baked before taking advantage of VNFs and NFV frameworks that dramatically reduce their cost of operations while simultaneously injecting unprecedented amounts of flexibility. As we see later in this report, some forward-leaning operators have charged ahead by taking a version of the specification and making it their own as basis for further rapid development.

VNFs and NFV Advantages to Businesses–Myths and Reality

The business benefits defined at the outset were: the ability of the CSP to choose from a variety of standard VNFs (routers, switches, firewalls, caches, application delivery controllers, etc.); to mix and match VNFs at will using a standard service template for quick and easy deployment; add more complex service-chaining between these VNFs as desired according to deployment needs; and the ability to scale these out in response to the business demands. These are ambitious mandates. Five years from the point of the launch of NFV, not all these have been realized.

Regardless, VNF's business promise has always been threefold:

- Agility
- Cost
- Freedom from vendor lock-in

CSPs have achieved varying results across these main categories.

VNFs Help Drive Agility

Agility has always been a challenge for the traditional telco. This is due to the nature of the proprietary and hardware centric equipment that has dominated the industry until after the first decade of the 21st century. Vendors can now enable CSPs to not only benefit from VNFs themselves, but also to offer a broad range of VNFs to their customers (some of the tier 1 CSPs have as many as 50 VNFs in their marketplace today). These services span the gamut of L2 through L7 of the OSI stack - routing, firewall, load balancing, SD-WAN, etc. The competition has also changed. With AWS, Azure, Google, and IBM defining what agile means to the end customer (enterprises or end-users), customers demand the same efficiencies enjoyed by these software-centric, web-scale rivals, driving CSPs to adopt NFV as a means to that end.

However, it needs to be mentioned that the first cut of these VNFs was really 'recompiled' images of the hardware-based appliances from the incumbent appliance vendors. As expected, this left a lot to be desired in terms of efficiency and speed. But it was a start. Over the years, as the second-and third-generation of VNFs developed, these features have improved. Another 'agile' dimension is 'service-chaining'—the ability to stitch together VNFCs and VNFs into one cohesive service chain on-demand. The reality is still very far away. While manual pre-configured chains can be provisioned today, even a replacement of a single function — say a load-balancer from Vendor A with Vendor B — involves human intervention at most operators. While CSPs are more agile today than when they didn't have NFV and VNFs, they are certainly nowhere close to the cloud players like AWS, Azure, or Google.

Do VNFs Lower Cost?

The promise of VNF has been to replace costly monolithic, single-function appliances with commodity servers and run high VNF density for maximum efficiency. But this promise is only now starting to come to light. The grossly inefficient first generation of VNFs preempted any reasonable VNF density. While some purpose-built VNFs did deliver on that promise, an operator competing against the webscale and software centric giants in any reasonably sized marketplace, needed to have more than a few efficient. The situation is slowly improving with new VNF implementations that may yield higher density. With the advent of microservices, or containers, we anticipate that this will further amplify the density and lower capex for the CSP. Compared with VM deployments, containers are lightweight, considerably faster to provision, and can be programmed and configured through RESTful APIs. With a much smaller memory footprint, containers may run more efficiently and at higher density than VMs. Containers are also easier to scale up and down. This is not fully yet realized today, and the vast majority of VNFs are still VM-based and will be for the near future.

On the opex side of the equation, the challenge around MANO and managing these numerous VNFs (see the VNF onboarding section later in this report) have impacted the full potential savings from deploying these SW-based solutions versus the physical appliances. Interoperability challenges with VNFs and various VNFMs and difficulty in rolling out mature MANO stacks that can easily integrate with existing OSS/BSS systems at CSPs will continue to dog opex savings realization for the next 12-18 months, if not more.

Preventing Lock-In with VNF Marketplaces

If ‘agility’ and ‘cost’ objectives were truly met, this objective would have been fulfilled by definition. However, that is not the case. Yes, with a VNF marketplace, the customer can decide which firewall or vCPE they are going to choose. In theory, this should make the vendors of these VNFs more paranoid and give the CSPs better bargaining power, but that is far from today’s reality. The need for the CSP to characterize the performance, the footprint of each VNF to understand its limitations, the (still) manual provisioning steps that are involved (it is getting better with APIs and automation), the ‘yet-to-be-realized’ service chaining with on-demand swap of one vendor or service function with another — all still makes it very hard for the operator to truly gain the bargaining power against vendor incumbency. However, this remains an important tenet of the overall VNF business promise.

The bottom line around business benefits brought about by these VNFs, and in turn NFV, is that we are still in process of fully deploying NFV. Whether the full benefits will be realized is still an open question in some use cases. The industry as a whole still has rosy projections for the future and believe the eventual promise of NFV. Certainly, the original timeframes for achieving success were too optimistic. Nevertheless, CSPs and the overall ecosystem at large continue to have faith in NFV’s eventual success. Some regional carriers, for specific use cases (like SD-WAN), are projecting overall savings of 20-40% in opex, and large **carriers like AT&T and Verizon are predicting future savings** on the order of 40-50% but have yet to realize them.

VNFs Power Top NFV Use Cases

Beyond hybrid clouds, IoT and 5G networks, there are several NFV use cases emerging in both the short and long term. VNFs' original calling, and where they are most widely used today, is for providing a Layer 4 through 7 networking security service, including session border controllers, load balancers and application-delivery controllers, firewalls, intrusion detection devices, policy enforcement managers, DNS platforms, and WAN accelerators. In addition, software-centric network services like virtual IP multimedia subsystem (vIMS), vCPE/SD-WAN or even virtual evolved packet core (vEPC) suites have been viewed as good candidates for NFV.

CSP and enterprise IT organizations have already embraced virtual appliances to deliver these capabilities on top of virtual machines. A VNF implementation of these functions takes that concept to the next logical conclusion by making it possible to manage those functions as pure applications within a well-defined framework that can be deployed anywhere without concern as to what virtual machine platform is installed where.

Virtualization of Home and Business Gateways (vCPE, SD-WAN): Internet service providers (ISPs) rely heavily on residential gateways and set-top boxes based on embedded processors. The available bandwidth increase has given way to replacing these proprietary boxes with more industry standard CPU and VNFs. These vCPE implementations will help drive lower-cost white boxes into the picture while improving the agility. They will also provide a universal platform in residential and business gateways upon which VNFs, like security or optimization services, can be deployed on-demand as part of value-added services. SD-WAN continues to be one of the hottest market growth areas that is powered by replacing costly leased-line and MPLS connections with reliable Internet based broadband.

Virtualization of Mobile Core (vEPC, vIMS): Virtualization of the mobile core services helps with improving infrastructure efficiency to enable more flexible deployments of services and to accelerate 5G and IoT rollouts. As VoLTE implementations roll out today, CSPs are utilizing vEPC and vIMS in NFV frameworks to improve time-to-market and costs. vEPC and vIMS also provide the ability to roll out cost-effective network services in previously hard to reach places, like rural villages in undeveloped countries. Another driver for vEPC is the increasing popularity of private LTE networks, especially for industrial enterprises and other verticals that are increasingly reliant on a dedicated and customizable network for their critical infrastructure.

Virtualization of Content Delivery Networks (CDNs): Rather than having to build what amounts to separate dedicated networks for optimizing the delivery of multimedia traffic over the Web, VNFs allow service providers to embed that functionality within the same network used to deliver every other networking service they provide. That capability will, in many instances, eliminate the need for subcontractors to provide multimedia services.

Virtual Network Platform as a Service: Many enterprise IT organizations will also look to service providers to help them deploy applications at the edge of a virtual network. Just as enterprise IT organizations take advantage of PaaS environments in the cloud today, that same concept will be extended to deploying applications at the edge of a global network.

Virtualization of RAN - vRAN: Providers of mobile networking services should be able to replace large number of physical appliances at the edge of their networks with industry-standard servers running VNFs that effectively replace existing mobile base stations as RANs. We anticipate that cRAN/vRAN VNFs should enable those service providers to consolidate much of the infrastructure currently deployed within those mobile base stations. cRAN drives increased efficiency of the baseband unit, the brains of a cell site, by centralizing it back to a central location so the baseband can control more cells than just one driving efficiency.

Service Function Chaining (SFC): Once VNFs are widely deployed, service providers should be able to offer additional higher valued services by providing point-to-point connections between VNFs that allow for composable paths through these VNFs. Strictly speaking, SFC is not really a use-case, but a capability that is valuable for use cases like vCPE. That capability will require being able to granularly manage a virtual network using VNF forwarding graphs to set up those logical connections.

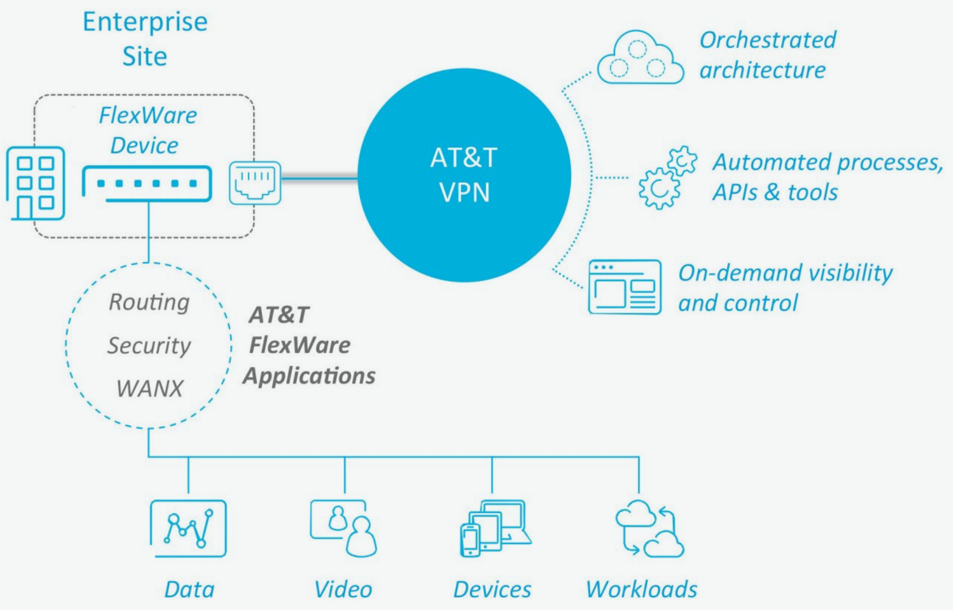
Real-World Carrier Deployments of VNFs

To get a flavor of VNFs in real-world NFV deployments, we take a brief look at three carriers that have been pushing NFV hard within their infrastructure.

AT&T - AT&T has its hand in just about every NFV pie. It has been one of the strongest proponents of NFV technology, and through its participation and contribution to numerous industry-standard initiatives (many of which involve open source), have established its NFV leadership in the CSP space. AT&T has contributed its ECOMP (Enhanced Control, Orchestration, Management & Policy) platform to the open-source Linux Foundation ONAP (Open Network Automation Platform) initiative for NFV MANO, its network operating system to the Linux Foundation DANOS (Disaggregated Network Operating System) project and has championed the use of open source in both OpenDaylight and ONOS SDN controllers. It is also involved in the CORD project.

In terms of end-user deployments, there is one area where we see VNFs feature prominently—in AT&T's FlexWare solution.

AT&T FLEXWARE SOLUTION

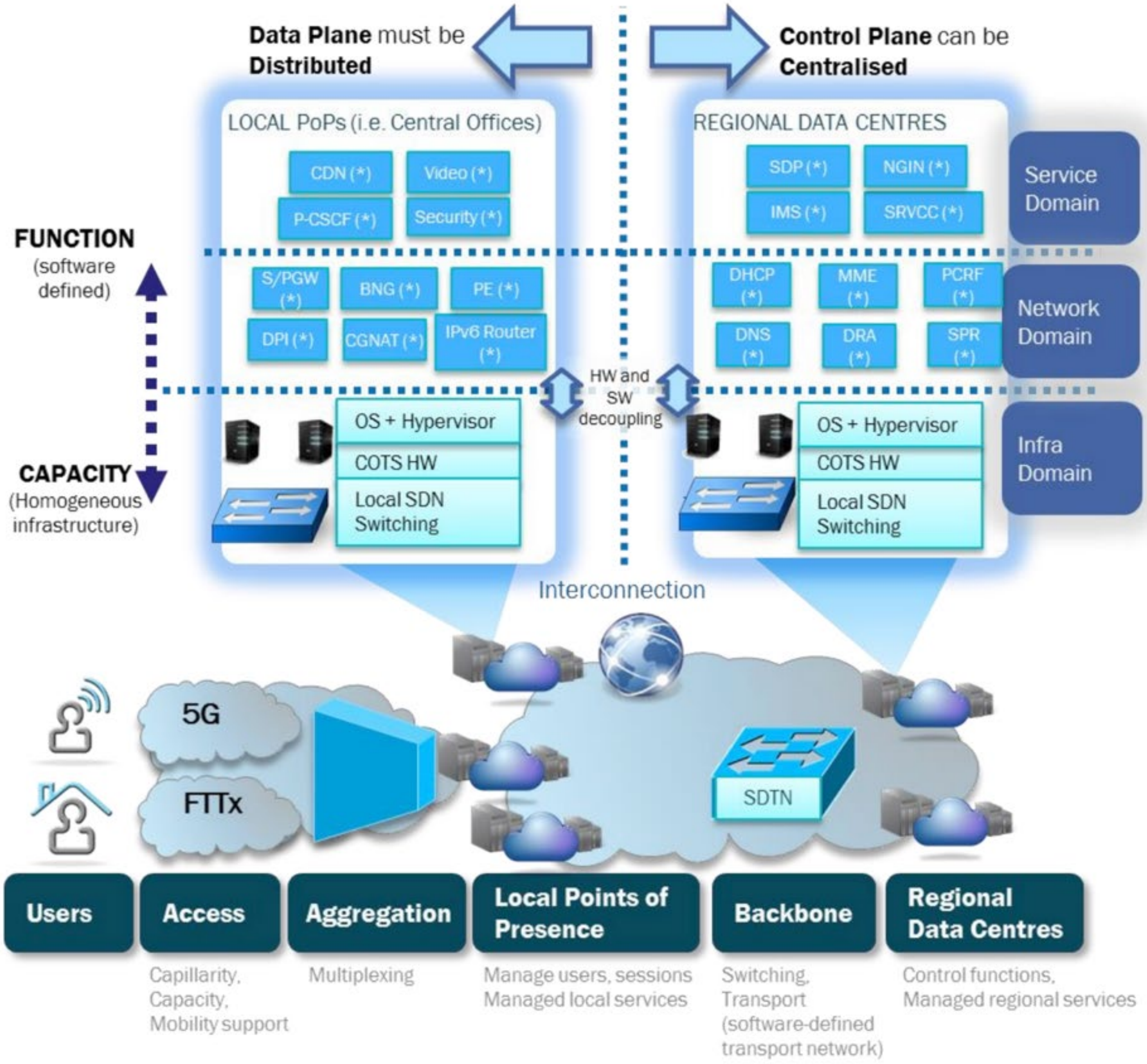

Enterprise Site
FlexWare Device
AT&T VPN
Orchestrated architecture
Automated processes, APIs & tools
On-demand visibility and control
Routing
Security
WANX
AT&T FlexWare Applications
Data
Video
Devices
Workloads

Source: AT&T

In AT&T's FlexWare solution, end-users get to choose from a variety of VNFs that are dynamically provisioned within a vCPE/SD-WAN framework. Ranging from basic routing to security and with VNFs from numerous leading vendors, its FlexWare platform has rolled out in more than 200 countries and territories, representing strong worldwide coverage through use of VNF and NFV technologies.

Telefónica UNICA - Telefónica's Unica initiative — when first unveiled in 2014 — was arguably the most ambitious among all the CSPs. Even after the sale of some assets, the Spanish operator's business empire spans countries in Latin America and Europe. It is still aggressively rolling out a variety of VNFs — core and edge — with many different vendors. China's Huawei Technologies supplies vEPC technology in Argentina and Peru, while ZTE contributes a vIMS in Peru. Nokia supports a virtualized service router for Unica, and Telefónica's Colombian subsidiary uses a virtual IMS from Ericsson. But more than 50 VNFs from 30 vendors are under evaluation.

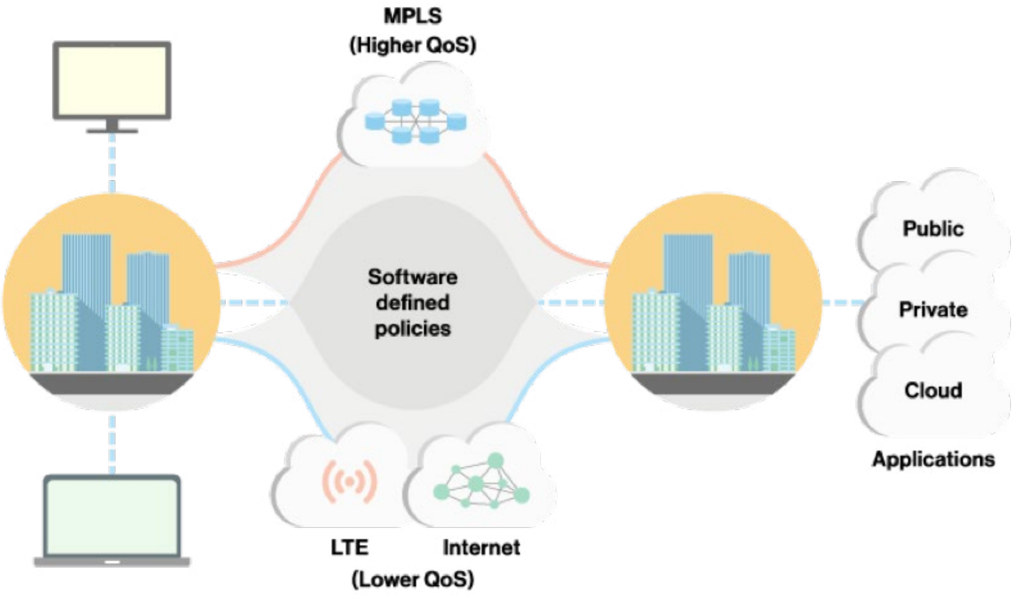
TELEFÓNICA'S END-TO-END VIRTUALIZED NETWORK VISION



Source: Telefónica

Verizon SD-WAN - Verizon has been active in deploying and offering SD-WAN as a service to its customers. In its product page, Verizon showcases a rich variety of services and vendors for its offerings as well as a managed services offering for less savvy customers. From routing to security, with choices from various vendors, Verizon has also demonstrated a commitment to using NFV and VNF solutions to improve edge connectivity options for its customers.

VERIZON SD-WAN



Source: Verizon

These are just samples of real-world VNFs in play. And they speak to the success of the SD-WAN/vCPE use-cases, which have proven to be the driving force across many carriers of NFV technology deployments.

VNF Major Challenges–VNF Onboarding and Monitoring

Despite the success of NFV and the SD-WAN/vCPE use case, NFV continues to face challenges in both widespread adoption across more use-cases, and also in operationalizing NFV to provide the full business benefits that carriers are looking for: agility, cost, and freedom from lock-in. In speaking with CSPs, there are a few areas of ongoing challenges, and in this section we'll highlight two that we hear about the most from CSPs and we'll cover the other challenges in the next section.

VNF Onboarding

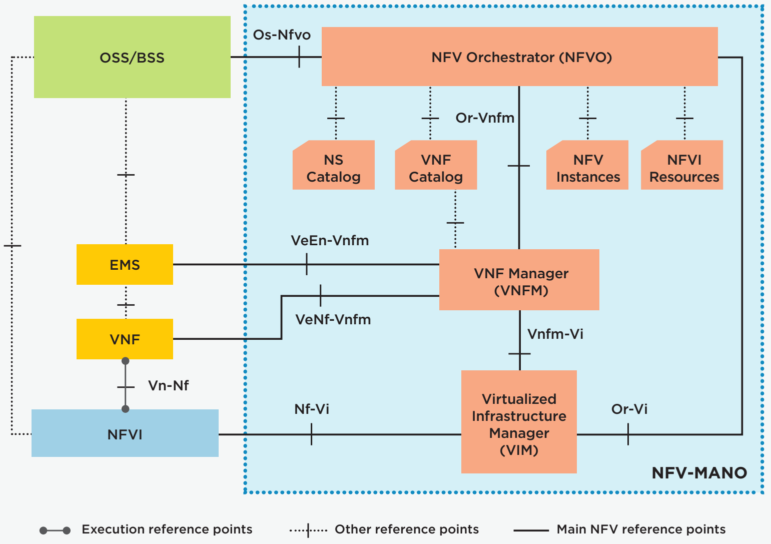
From a business perspective, there are really only two metrics that the CSP cares about — revenue and expense. In other words, CSPs care about bringing new services to market to grow the top line and reducing the cost of network services from both capex and opex perspectives. VNFs are the panacea to achieve this. However, once the CSP has decided to embark on the VNF journey, it must deal with a lot of logistical issues that are collectively referred to as "VNF onboarding." VNF onboarding consists of two stages. The first stage is the planning stage. This includes:

- Identification of the VNFs and VNF vendors
- Comprehending the licensing terms
- Procuring the VNFs from more than one vendor for testing
- Architecting the design-scale, heterogeneity, chaining, etc.

The second stage is the operationalizing stage. This includes:

- Onboarding the VNFs from various vendors
- Orchestrating them with service function chaining (SFC), VNF Forwarding Graph (VNFFG) and Physical Network Functions (PNFs)
- Testing the capacity and performance before advertising the service capabilities

NFV-MANO REFERENCE ARCHITECTURE



Source: ETSI

sdxcentral.com

As seen in the NFV-MANO reference architecture above, the onboarding process for any VNF involves:

A. Support for the underlying NFVI
B. Support for the VNFM that it brings along with it
C. Integration, by extension, of the VNFM into the NFVO
D. Optionally, direct integration into the existing EMS.

The biggest problem is that no standard way exists to instantiate, configure, and operationalize these multi-vendor VNFs. Each VNF has its own unique way of onboarding. There is a gap between what VNF vendors provide and the ability of the CSPs to easily consume these VNFs. Today, it is a very expensive, complex, and time-consuming effort to onboard VNFs.

The lack of standards is the reason that VNFs are difficult to onboard. Every VNF vendor has its own proprietary way to manage its VNFs, usually with a specialized VNF manager. But this is a cost and complexity challenge that both VNF vendors and CSPs face. VNF vendors have to test their VNFs against multiple virtualized infrastructure managers (VIMs), orchestrators, and sometimes even VNF managers. On the other side, CSPs have their own workflows and tools and want to integrate the VNF onboarding process with their existing workflows with little to no changes and ensure that the VNF onboards successfully in their environments.

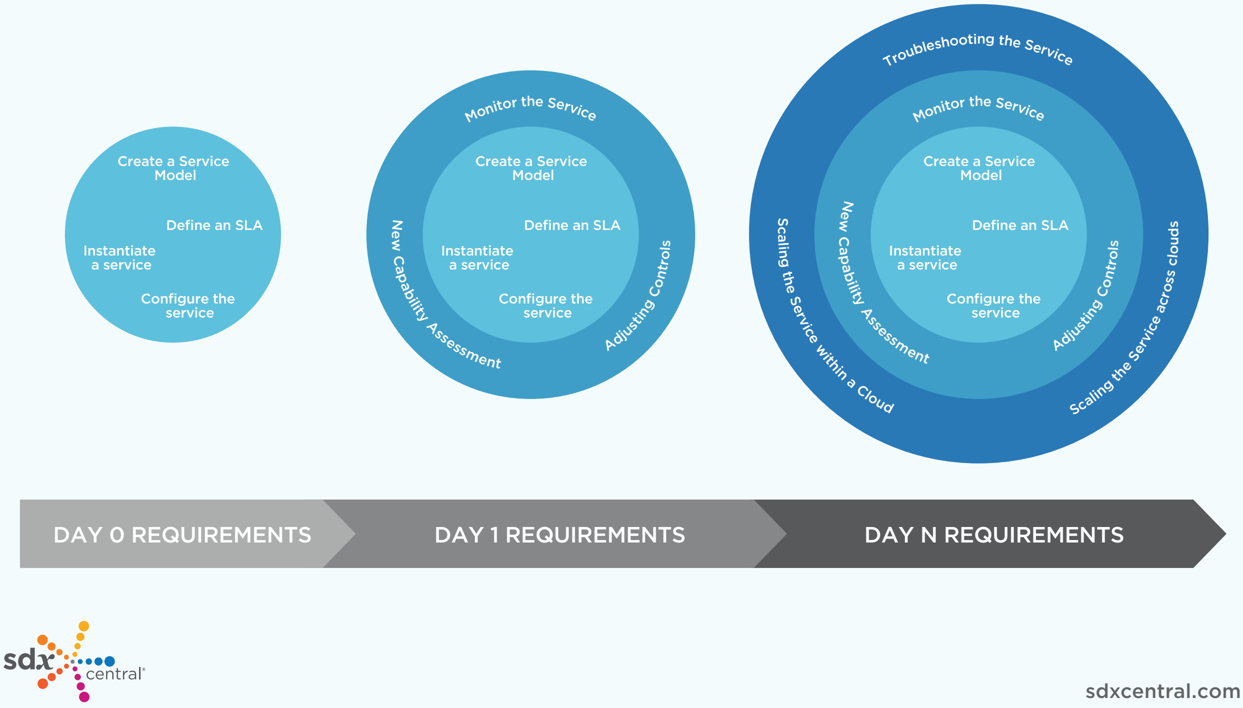
There are existing efforts to standardize on both the VNF descriptor (VNFD is a deployment template which describes a VNF in terms of its deployment and operational behavior), and its packaging format. The standards bodies — ETSI, IETF, OASIS-TOSCA, and open source communities, such as OPNFV, OpenDayLight, and ONAP, to name a few, all have a role in both defining and implementing these standards. But this also means it is incumbent upon vendors and CSPs to keep up with the rapid iteration in standards and open source projects as they gain traction.

VNF Monitoring

VNF monitoring is a key aspect of ensuring service availability and adjusting to changing conditions. Beyond onboarding VNFs, VNFs need to operate smoothly. Monitoring is what would be considered a ‘Day 1 requirement’. From a temporal perspective, this can be expanded and broken into ‘Day 0 requirements’, ‘Day 1 requirements’ and ‘Day N requirements’.

Day 0 requirements are essential to get the service up and running: creating a service model, defining an SLA, instantiating a service, and configuring the service. Day 1 requirements are essential to ensure continued uptime and adaptation. These include monitoring the deployed service, adjusting controls as needed and assessing new capabilities in the portfolio. Day N requirements are expanding, upgrading (downgrading). These involve troubleshooting the service, scaling the service inside a single region/cloud and expanding across regions and clouds.

MANO REQUIREMENTS – DAY 0 TO DAY N



sdxcentral.com

The need for VNF monitoring is manifold. It is good indicator for assessing the overall health of the network. Depending on the sophistication of the monitoring application, VNF monitoring can be customized to monitor groups of VNFs or specific VNFs that are updated or added for a period of time. Each group can be assessed based on pre-defined KPIs.

Often, VNF deployments focus on the Day 0 requirements, neglecting the Day 1 and beyond requirements. CSPs sometimes realize after initial deployment that they've neglected the remaining needs, resulting in much more expensive deployments after the fact. For more details on these requirements, read our **NFV Report Series Part II** which overs this issue and NFV MANO more comprehensively.

Other Challenges with VNFs

Beyond VNF onboarding and MANO, there are still other significant VNF migration challenges that exist. Some of these have been there since the beginning, others are new arrivals.

Curse of the Fake VNFs

Officially, a VNF is any combination of software that performs a discrete networking function. The challenge this creates is that a VNF can be written in almost any programming language and come in any software package, with arbitrary interfaces (which may or may not fully conform to ETSI NFV standards). Until all the interoperability specifications can be defined, VNFs essentially only offer an alternative to deploying a physical appliance. Due to competitive pressure and customer demands, every hardware vendor has been compelled to come up with a virtual edition of their hardware counterpart simply by porting a HW-based network product into a VM and declaring they have a full NFV VNF. Vendors often position offerings that require proprietary NFVI, or their own proprietary MANO, as an NFV VNF, when in truth that product is still more akin to a virtual appliance rather than a true NFV application. This is in contrast with VNFs that operate seamlessly on top of a NFVI with well-understood and stable performance characteristics that can be fully life-cycle managed by any standardized MANO implementation from multiple vendors.

However, to be fair to vendors, the NFV standards are still evolving and there is much we don't fully understand, nor have we solved all compatibility, deployment, or manageability issues. For example, the industry has been focused on VNFs as VMs, when in fact, because VNFs are more akin to applications, it may very well turn out that some subset of VNFs will be delivered in, for example, a Linux Container format. That format will not only make it easier to deploy a VNF across multiple platforms, but also the whole process of adding and updating additional functionality is greatly enhanced. Instead of patching the VNF, new functions are added by replacing discrete containers with a new container that then exposes that functionality to the network via a standard set of APIs. Certainly, work on the NFVI level is moving toward supporting these container deployments as well, but it remains to be seen how we manage VMs, containers, and in some cases, bare metal machines as hosts for VNFs in an effective manner.

VNF and Licensing—Still a Work in Progress

VNFs are not a panacea for every use case. There will be plenty of scenarios where performance requirements may dictate continued reliance on virtual or physical appliances. In fact, it's more than likely that both service providers and enterprise IT organizations will find themselves managing a medley of physical and virtual appliances alongside multiple types of VNFs for some time to come.

Vendors have also yet to work out anything that resembles a consistent approach to licensing VNFs. Most seem to be leaning toward a subscription model based on monthly usage that mirrors the models used by providers of software-as-a-service (SaaS) application providers. The reason for this is the demand from customers who are accustomed to pay-as-you-go models, even if vendors would prefer a more sustainable revenue model based on longer-term commitments. But these predetermined licensing models will not work. As network functions need to scale up and down more dynamically than an average SaaS application, more granular approaches to licensing based on actual usage are required. This will require significant investments in technologies ranging from monitoring tools to track availability and usage to chargeback tools that will enable organizations to allocate billing to specific departments.

To make matters more interesting, the same open source versus commercial software debate that has been going now for more than 10 years will also apply to VNFs. For every commercial VNF, a corollary open source project is likely to exist. CSPs and enterprise IT organizations are likely to have different levels of appetite for both the rate at which VNFs are upgraded over time and the level of support provided. That same conversation is now playing out across NFV management platforms as well. So, the pricing pressures that vendors will feel are from two ends of the spectrum. On one hand, vendors need to keep pricing competitive to compete with these open source cousins of their proprietary offerings. On the other hand, they need to keep pricing high so any cannibalization from their higher ASP hardware brethren doesn't impact their top lines too negatively.

VNF Performance—Value of HW acceleration

Physical network functions tend to take full advantage of the underlying hardware and, in some cases, depend on proprietary hardware to provide maximum performance per unit cost. In moving to NFV, we often achieve flexibility and may experience lower cost of the hardware platform, but sometimes give up software performance, resulting in high-cost per packet processed. NFV proponents argue that the opex savings will more than makeup for these increased hardware costs, but this might not apply in all cases. Acceleration techniques abound for VNFs, ranging from PCI-pass-through, to single-root input/output virtualization (SR-IOV) to software SDKs like DPDK for both x86 and ARM platforms. We're now seeing realization that using generic platforms might not make sense for all use cases (e.g. high-speed routing), and that HW acceleration in the form of Smart NICs and SSL/TLS assist might be necessary for some VNFs. There's still work to be done on this front as CSPs figure out the right underlying NFVI that best supports the varied flavors of VNFs.

Chaining VNFs—Missing links

One of the most common use cases for VNF roll out is service SFC to provide maximum flexibility for traffic processing. The promise of mixing and matching different VNFs from different vendors in flexible chains doesn't always materialize. Often CSPs find out that VNFs can be mixed and matched because they run on different NFVI flavors (specific versions of OpenStack, requirements for different hypervisors) or come under the control of different MANO stacks. Without the right span/scope of control across the VNFs, it becomes harder to orchestrate them to obtain the correct chain of functions. Work still needs to be done in standardizing these as related to the overall VNF onboarding challenges we covered earlier.

Generic VNFMs—Pipe-dream or Reality

One related problem to the chaining issue is standardized MANO. We also covered this a little in the VNF onboarding section. Fundamentally, what is still happening in the market (though improving) is that each vendor providing their VNF solution suites, which address a specific network service the CSPs want, also provide their own specialized VNF Manager (VNFM). Because the VNFs have unique capabilities, or because the service needs more fine-grained controls, these VNFs are tied to their own VNFMs resulting in an ability to mix and match more easily. In some cases, the VNFMs from the different vendors have different data models of capabilities, making this just as hard up the stack at the NFV orchestration (NFV-O) level, leading to more management nightmares as CSPs try to mix and match VNF solutions from different vendors.

Performance Characterization—Whose Job is it?

Another challenge that CSPs face in rolling out VNFs is understanding the performance characteristics of the VNFs so they can appropriately size the underlying NFVI to provide the right level of capacity and SLAs to their end-users.

There are efforts underway across vendors, test labs, standards bodies to try to find common ways of both testing and certifying NFV solutions. However, due to difficulties in performance characterizing a wide variety of network functions and the lack of common NFVI frameworks, these efforts are not as far along as CSPs would like. The question of who is ultimately responsible for ascertaining and certifying VNF performance remains. CSPs that can afford to do so run performance labs to characterize performance before rolling out NFV-based network services. But not all CSPs can do so, nor can they afford to for the diversity of VNFs that exist. In a desired world of mix-and-match VNFs on a universal NFVI platform with a universal MANO framework, we still come up short in terms of a common set of published and certified performance criteria across all VNFs from all NFV vendors.

Despite the above challenges, NFV continues to march along and its momentum will continue. SDxCentral believes that the overall benefits provided by virtualization and NFV are too great, and the pressure to compete with over-the-top (OTT) providers is so strong that the NFV ecosystem will find ways to overcome these challenges and make a significant part of NFV a reality.

Key VNF and NFV Market Trends in 2018

Consolidation of Players–M&A Continues to Roll

Two particular VNF areas that were in focus in 2017 and in early 2018 were the SD-WAN and the vCPE markets. SD-WAN had two large exits in 2017: Viptela was acquired by Cisco and VeloCloud was acquired by VMWare later in the year. Both of these acquisitions signal to the market that the SD-WAN market was real and that larger players were willing to pay a premium to get into the software WAN market. However, if one were to dig deeper, there is more to be gleaned from this market. First, the days of CSPs relying on MPLS circuits as a continued revenue stream were numbered. Second, the branch/SMB/SME was again becoming very interesting as the number of services deployed there started to mushroom and the need for reliable, cost-effective, and scalable solutions became paramount.

Large Players Disintegrated with Key Software Assets (VNFs) Acquired

One of the big stories of 2017 was the break-up of Brocade and the acquisition of its assets by various entities. The first sale was the software business unit of Brocade, and the two key assets of its VNF portfolio were the vRouter and the vADC. The vRouter was picked up by AT&T and the vADC by Pulse Secure. AT&T moved from being a customer of the vRouter to becoming the owner of that VNF asset. The acquisition further strengthened its asset base with one of the first commercial VNFs in the market and put it ahead of its top competitors in the US market when it came to owning and using technology.

NFV Players Grow Revenue After Years of Investments and False Starts

The last year was a watershed year when it came to NFV revenues. VMWare continued to lead the pack in terms of absolute license revenue, but, as expected, most of this was focused on the enterprise. However, VMWare did win a marquee account — Vodafone — although it was an NFVI win (vCloud NFV), we expect VMWare to start enabling its VNF portfolio on top of its platform through partnerships and acquisitions. Smaller players that also exited (like Viptela and VeloCloud described previously) reported double-digit revenues in 2017, showing healthy growth from the previous year. Some of the other startups in the SD-WAN space were also rumored to be growing revenues.

Net-Neutrality and Impact on the VNF market

One important market shift (somewhat underreported in the media) that will have a significant say in the use of VNFs by CSPs is the revocation of the 'net-neutrality' mandate late in 2017. In the past years or decades, CSPs in the US have had to treat all traffic alike, and the value of VNFs was predominantly one of cost-optimization and agility and not one of driving additional revenue opportunities. That changed in one fell swoop with the revocation of the net-neutrality rule, set to sunset on June 11, 2018. Now the CSPs in the US have free rein to treat the traffic as they please. What this implies is that services offered by them could be prioritized by those offered by the OTT providers like Google, Amazon, FaceBook, etc. And VNFs will start to assume a much bigger role in this evolution by allowing flexible and scalable service offerings like dynamic load balancing for a new service offered by AT&T, for example.

Network-As-A-Service (NaaS) becomes Real

As VNFs become more pervasive and their elusive promise of cost savings and agility finally start to bear fruit, the attractiveness of VNFs either as replacement of traditional hardware or as brand-new revenue opportunities for new CSPs brings forth with it the need to invest in people skills or retraining to take advantage of this trend. Strong software networking and cloud expertise are required. In addition, each VNF serving a different buyer has unique skill demands. ADC is different than routing and different than firewalling. That is not easy.

Hence, the network-as-a-service (NaaS) model. System integrators and service partners are all plunging into this practice. They hire the software experts with cloud and DevOps experience, have a collection of VNFs that they test and certify, and based on the requirements of the CSP they serve, these partners come in to set up the foundations of an NFV offering that the CSPs can sell on a subscription as-a-service model. In some cases, these partners will perform a build-operate-transfer model where the CSPs ultimately run the ongoing platform. In others, partners will continue to manage these services for the CSP.

DevOps and NFV

The impact of continuous integration/continuous delivery (CI/CD) — both in enterprise data centers as well as public cloud markets — has increased the pressure on service providers as they move to a software-based model to embrace DevOps to remain competitive. Because of the nature of some CSPs' operations — which might be slow rollouts like a cell site build out or an optical cable layout — there is an entrenched culture and legacy process gates that limit software delivery agility and adds redundant checkpoints while increasing latency thereby stymieing creativity and innovation. This is where DevOps can help by completely transforming the culture and delivery momentum. Experimenting, iterating, and deploying in a continuous and automated fashion will help CSPs compete and win. VNFs from some vendors are now available in a lightweight 'container' model to help with this CI/CD movement. But, migration to container architectures is still a work in progress, VMs are the bulk of deployments today and reality is that even bare metal network functions will have to be accommodated in NFV deployments. Most of the container implementations are early POCs and still being worked on by development teams.

Going Beyond Day 0 and Day 1 Operations to Day 'N' and Hyper-optimization

2017 and early 2018 finally saw some of the original promise of NFV start to come to light. As mentioned before, certain operators worldwide have been playing a leading role in this transformation. This is great news, but this also implies that the distinct nature of 'carrier grade' requirements compared to a large enterprise IT application starts to really manifest itself more pronouncedly. These include: CPU pinning, DPDK (which was called out earlier), SR-IOV, cache sharing maximization, etc. Some of these will limit agility but at 'Day N' — when a service is mature — the operator has a very good handle on the service requirements and can over-optimize on certain dimensions at the exclusion of others.

Sophistication in VNF Workload Placement

As the VNF market matures, there is more awareness about the impact of appropriate VNF workload placement. For example, there is increased recognition that a VNF that has significant scaling and performance needs may need to be appropriately placed on hardware that has available HW acceleration in the NFVI. This predicates that the infrastructure needs to advertise its capabilities beforehand — and on an ongoing basis as software and hardware updates happen — and so recognizing the needs for VNF acceleration and placing these workloads onto the right infrastructure is an area of ongoing research. As described earlier, there are existing efforts to standardize on the VNF Descriptor - a deployment template which describes a VNF in terms of its deployment and operational behavior). And the server hardware profile has several properties like Number of vCPUs, RAM size, CPU pinning, PCI pass-through, etc. which could be helpful in determining the match between the VNF requirements and the server capabilities.

Mitigating NFV Islands Caused by VNFs

An unforeseen side effect of the increase in vendor offerings in the VNF marketplace and the corresponding adoption of VNFs is the emergence of "VNF islands." Most vendor VNFs come with their own VNFMs that is mandatory in most cases, but often also extends into the MANO and NFVI dictates in order for the solution to work. In this situation, if an operator has three SD-WAN offerings in the marketplace, there could be three different VNFMs to deal with and possibly a MANO and NFVI requirement that could be different — even if the actual MANO and NFVI product is the same, a difference in the version that is supported could result in a completely new VNF+VNFM+MANO+NFVI. As CSPs roll-out NFV across different markets and use cases, they now find these disparate VNF islands, each of which might conform to the NFV framework, but which cannot interoperate much less mix and match VNFs. These VNF islands add to increased opex challenges, reducing the overall benefits of NFV. We're seeing a realization at some of the early adopters of NFV and efforts are underway to work with vendors to standardize at the NFVI and MANO level to drive a more cohesive and uniform approach to NFV roll-outs in the future.

More Self-service, Self-diagnosis, Self-remediation

The customer portal has started to evolve to a true 'self-service' selection of services. For example, an IP VPN service landing page for a customer could show three types of speeds — 10M, 100M or 500M that the customer can choose from. A service design portal on Google maps where the customer can mark the location of the VPN endpoints and hit 'buy'. If there is already a hardware CPE, the VNF simply gets deployed at those locations. If not, the customer gets directed to a list of partner hardware vendors that can ship pre-configured uCPE platforms. Once installed, the VNF/uCPE combination is managed by the service portal that shows key indicators such as performance latency and threats. Finally, we're also noticing increased roll-outs of an option to self-remediate if any of the SLA measures are not being met, showing improved maturity of NFV-based offerings, and a focus on reducing overall opex costs through NFV's SW-centric approach that improves flexibility and agility of VNF offerings.

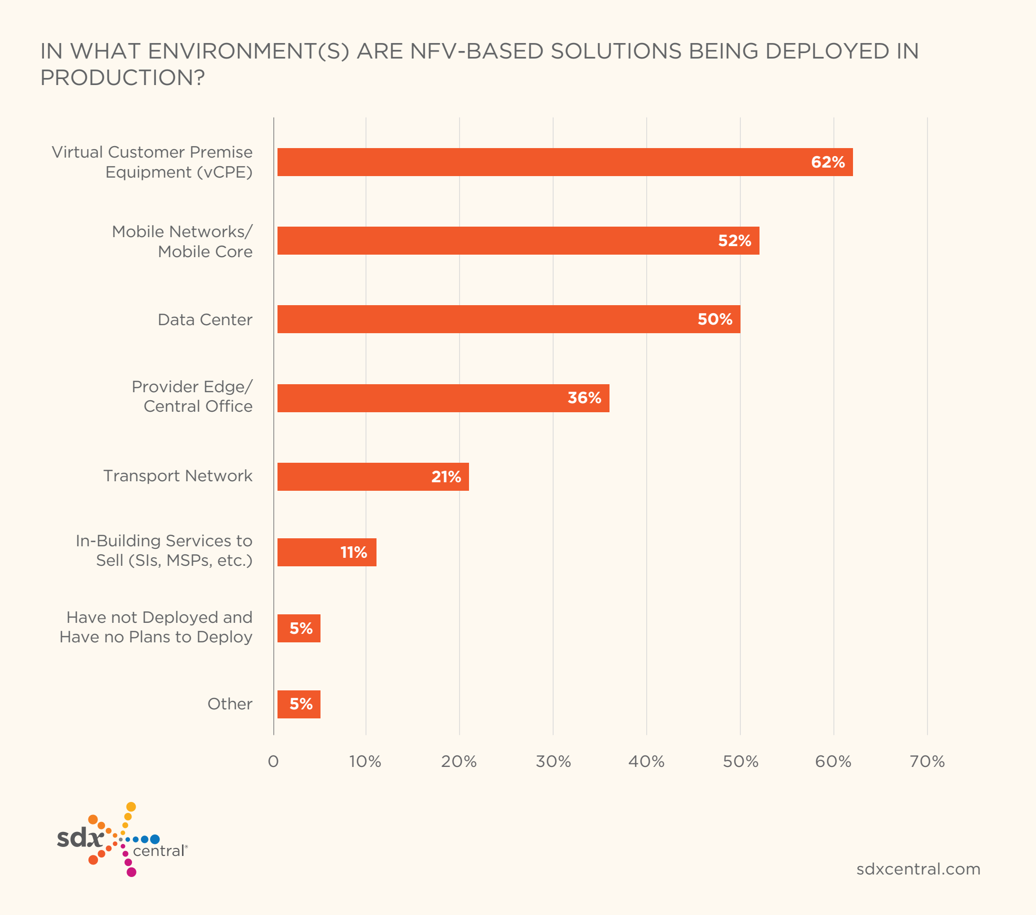
As 2018 progresses, we'll continue to observe new emergent trends and the SDxCentral research team will continue to track these updates for next year's updated NFV report series.

NFV Survey Results: VNF Report

The third annual network function virtualization (NFV) survey gives us a snapshot of how the market is developing and how virtualized architecture implementations and service delivery models are maturing. The SDxCentral Research team ran the survey on the SDxCentral site during the month of March 2018.[1] The 2018 results were compared to the 2017 and 2016 stats to try to identify trends or significant changes in perception or experiences that have occurred through the years. If you missed Part I and Part II of our NFV report series, then check those out as we've covered some other key survey findings in those reports.

VNF Deployments

Service providers indicated they deploy NFV-based solutions in a variety of production environments. When probed, with the ability to choose all the environments that applied to them, 62% of service providers said they had deployed NFV solutions in "virtual customer premises equipment (vCPE)," 52% in "mobile networks/mobile core," 50% in the "data center," and 36% in the "provider edge/central office." For the "transport network" and within "services to sell," only 21% and 11%, respectively, indicated they use NFV. Beyond these deployments, in an open-ended question, providers and vendors thought the evolved packet core (EPC), IP multimedia subsystem (IMS), and SD-WAN were also candidates for NFV solution deployments.



[1] There were 85 respondents

Top NFV Use Cases

When asked to name their top three use cases for NFV solutions, service providers responded with a wide range of options, including virtualizing security (firewall), automation, orchestration, and routing (load balancing) functions.

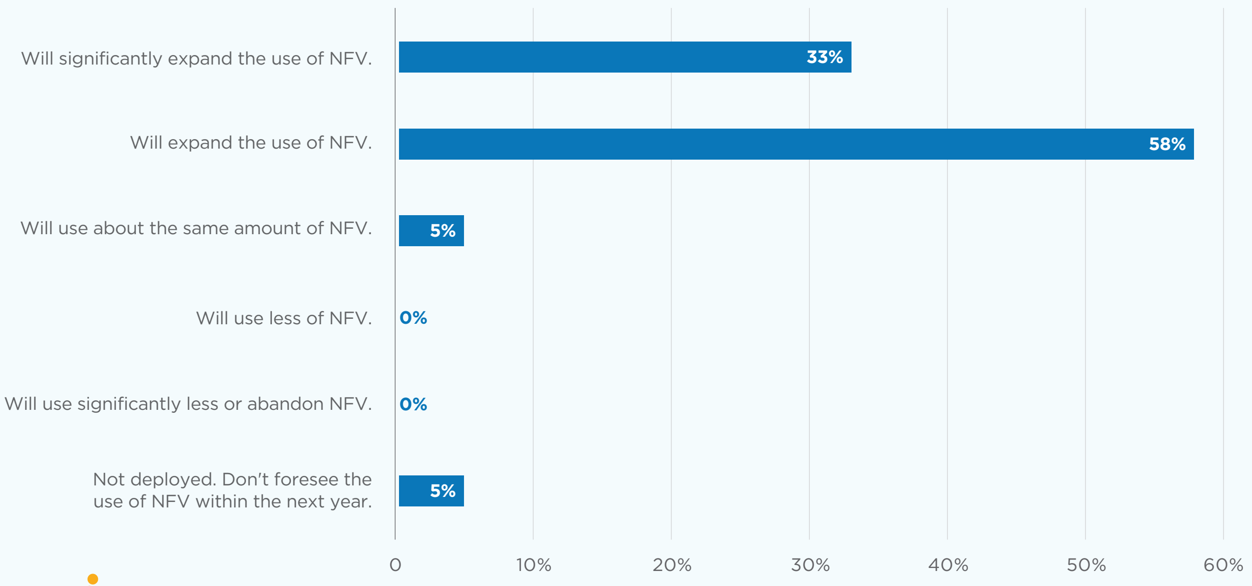
Lessons Learned in NFV Deployments

In an open-ended question, we asked providers and vendors to share what they had learned in their NFV trials and deployments. Most responses were a variation of "it's a little harder than anticipated." Getting the deployment right required some trial and error and learning on their part, however, it appears the potential and the benefits of the technology are worth the time, effort, and retooling.

NFV Plans for the Future

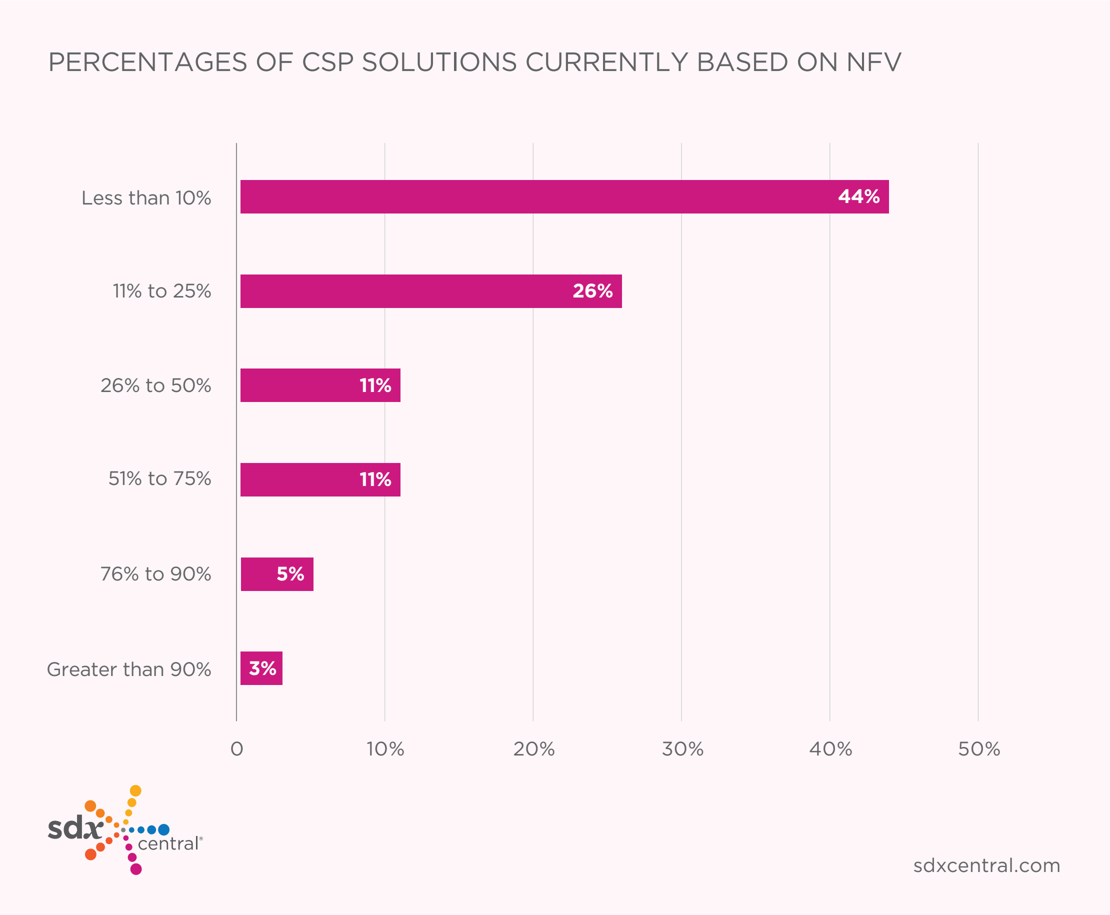
Service providers and vendors see the use of NFV "expanding" (58%) or "significantly expanding" (33%).

DO YOU SEE INCREASING, SUSTAINING, OR DECREASING USE OF NFV SOLUTIONS?



sdxcentral.com

They may not be starting with a large percentage — last year, 74% of those who indicated they were interested in NFV technologies said they expected 5-20% of their infrastructure to be based on NFV by the end of 2018. It appears customers probably hit that percentage, as 26% of service provider respondents thought NFV-based solutions probably made up between "11% and 25%" of a customer's environment, while 44% estimated it was probably "less than 10%."



This bodes well for NFV roll-outs over the next few years and is consistent with our own view that despite the various challenges that exist, NFV has a momentum that's virtually unstoppable at this point in time.

Conclusion – VNFs and NFV Power On

As 5G mobile computing and IoT applications come into the picture, and as the pressure from OTT players continues to rise, CSPs have no choice but to drive toward a virtualized and agile platform that allows them to compete effectively. SD-WAN and vCPE deployments have been a boon to CSPs worldwide, helping lead NFV deployments with real-world offerings that businesses and consumers alike are already benefiting from.

The good news is that as VNFs continue to proliferate, a lot of visibility and capabilities will be provided at the network level. That in turn should make enterprise IT organizations more comfortable with CSPs that are rapidly evolving into strategic business partners. This relationship transformation between CSPs and enterprise IT organizations is not going to occur overnight, but each new VNF that gets deployed is one more step in the right direction.

While a myriad challenges still face CSPs, from VNF onboarding to VNF islands to performance challenges, NFV will continue to pick up steam and expand its reach. In the early days of NFV, the overall ecosystem was perhaps too optimistic with the expected timelines for widespread deployment. However, as we've seen in technology adoption patterns in other industries, once we get past the proverbial chasm, the rate of uptake will increase significantly. And it feels that we're close to getting through that chasm in the next 12-18 months. The 2020 goals that CSPs are now touting as the year where we will see a majority of carrier infrastructures driven by NFV and virtualization seem much more achievable.

We hope you've found the analysis and insights in this report helpful. If you think we've missed a key trend, or have an area you'd like to see us cover in future reports, drop us a note at **research@sdxcentral.com**. We'd love to hear from you.

2018 VNF Report Products

The following section of this report profiles some of the more popular vendor offerings. At SDxCentral, we aim to cover a broad sampling across the space, but we welcome vendors to reach out to us. **Extended profiles of each product can be viewed online**. The information was gathered via a collaborative effort between SDxCentral's research team and the vendor's appropriate product experts. We welcome feedback, and if you believe we've missed a product, please contact the research team to start a conversation about having your products included in future editions of this report.

While every attempt has been made to validate the capabilities listed in the profiles, SDxCentral advises end-users to verify the accuracy of each claim for themselves in their actual deployment environments. SDxCentral cannot be held liable for unexpected operations, damages, or incorrect operation due to any inaccuracies listed here.

SDxCentral welcomes feedback and additional information from end-users based on their real-world experiences with the products and technologies listed. The SDxCentral Research Team can be reached at **research@sdxcentral.com**.

Organizations with listings in this report include: 6WIND, A10 Networks, Affirmed Networks, Airpsan, Alianza, Inc., Altiostar, AT&T, Avi Networks, CA Technologies, Cisco Systems, Enea, a Qosmos Division, Ericsson, F5, Fortinet, Ixia, Juniper Networks, Metaswitch Networks, NEC, netElastic Systems, NFWare, Nokia, Nuage Networks, Openwave Mobility, Palo Alto Networks, Pulse Secure, Radisys, Ribbon Communications, Silver Peak Systems, Telco Systems, Versa Networks

Qualified Vendors Not Listed

The following are additional organizations with products that we believe should be included in this report but were not submitted for various reasons. If you belong to one of these organizations, we'd love to hear from you and get your products listed in the future. Regardless of whether you belong to one of the following organizations, if you would like to submit to the report or to future versions of this report, please contact **research@sdxcentral.com**.

Allot Communications Ltd	Nominum Inc.
Benu Networks	Oracle
Check Point Software	Radware
Dialogic	Samsung
Hewlett Packard Enterprise	Viavi Solutions, Inc.
Huawei	ZTE Corporation
Infoblox	

Avi Vantage Platform

(Click to View More Details Online)

https://avinetworks.com/datasheet

Avi Networks
PUBLIC | **PRIVATE**
5155 Old Ironsides Drive
Santa Clara, CA, 95054, United States
chandra@avinetworks.com
408-628-1300
https://avinetworks.com/company/

Description of Company: Avi Networks delivers Intent-Based Application Services that automates elasticity and intelligence across any cloud. The Avi Vantage Platform provides a Software Load Balancer, Intelligent Web Application Firewall (iWAF) and Elastic Service Mesh to ensure a fast, scalable, and secure application experience. Customers enjoy 90% faster provisioning and 50% lower TCO.

Avi Networks in SDxCentral Company Directory

Description of Product: The Avi Vantage Platform delivers elastic load balancing, security, autoscaling, application performance monitoring, and acceleration for both traditional and cloud-native applications. Unlike legacy ADCs, Avi provides a software-defined, scale-out architecture delivering application services focused on outcomes instead of configuration parameters. The intent-based capabilities of the platform automate all aspects of application networking services across on-premises and cloud environments.

Avi Vantage Platform in SDxCentral Product Directory

Unique Value Proposition

Avi Vantage Platform uses a software-defined scale-out architecture that separates the central control plane (Avi Controller) from the distributed data plane (Avi Service Engines) that delivers application services such as load balancing and WAF. The software-only platform is ideally suited for NFV use cases since it can be deployed on bare metal server, virtual machines, containers, or in the public cloud. The platform delivers per-app and per-tenant application services.

Relevancy to VNFs

Avi Vantage is a software-only application services platform that delivers distributed load balancing and WAF with central management. It is ideally suited for VNF deployments needing dynamic services that are not tied to hardware appliances.

Product Differentiation

Avi Vantage is the only full-featured software-defined platform for application services. Unlike traditional ADCs which are over-provisioned on one hand or do not scale beyond the capacity of the appliance, Avi uses a scale-out software only architecture that elastically scales in real time in response to traffic patterns. The platform delivers rich application analytics that provide actionable insights to administrators who otherwise have to pore through log files and tcp dumps. Avi also delivers consistent application services across multi-cloud environments with a single central point of management. The platform enables networks administrators and DevOps teams to deliver per-app and per-tenant application services with self-service.

Analytics Support

Avi provides end-to-end visibility to round trip times and latency for individual application transactions. The platform delivers real time application performance, security, and end user insights.

Top Use Cases

Avi is used by enterprises to replace legacy ADCs with elastic, highly automated application services, to help deliver applications in multi-cloud environments, and to support modern application architectures such as container-based microservices.

VNF Solution Packaging

VNF (SW package), Containers, Bare Metal, Public Cloud

Supported OSes

Linux, AWS, Azure, GCP, Docker

Supported Hypervisors

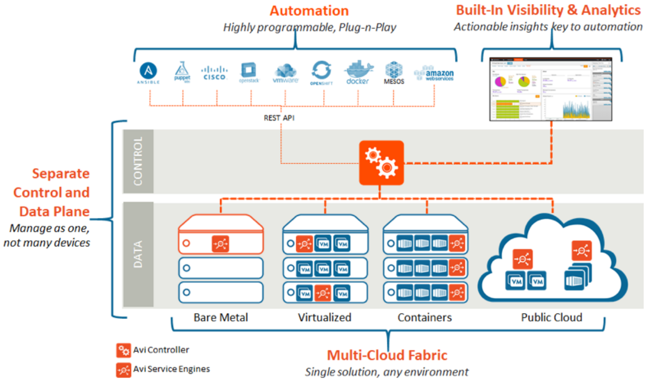
ESXi, KVM, Hyper-V, Nutanix Acropolis, Azure, AWS, GCP

Key Partners

https://avinetworks.com/partners

Key Customers

Adobe, Travelport, Zurich Airport, EBSCO, ZOLL Data



CATEGORY **Solution Suites (multi-function) or Other VNF**

F5 Virtual Network Functions (VNFs)

(Click to View More Details Online)

https://www.f5.com/pdf/solution-center/network-functions-virtualization-nfv-solution-overview.pdf

F5
PUBLIC | PRIVATE
401 Elliott Ave W
Seattle, Washington, 98119, United States
(206) 272-5555
http://www.f5.com/

Description of Company: All ten of the world's largest mobile operators and all of the top ten US telecommunications companies trust F5 to make their networks faster, smarter and safer. F5's broad portfolio of carrier-grade solutions improve signaling and data traffic management, ensure security at every level, and enable NFV and the evolution to 5G. Providers are empowered to more effectively grow their networks and deliver new revenue-generating services, while ensuring maximum quality of experience for subscribers.

F5 in SDxCentral Company Directory

Description of Product: F5 offers one of the broadest portfolios of software and hardware solutions in the industry, which allows maximum flexibility and choice as you virtualize your network. Leveraging F5's heritage and expertise in software applications, with F5 you can deploy a flexible, agile, and scalable network that will help you improve network efficiency and deliver services faster to market.

F5 Virtual Network Functions (VNFs) in SDxCentral Product Directory

VNF Categories

F5 has the broadest range of solutions - from traffic management and optimization, policy enforcement to firewall, DDoS and CGNAT and many others.

Unique Value Proposition

F5's history is rooted in software enabled application delivery and we can bring that history and expertise to the virtualization of network functions. All F5 VNF's are available and interoperable as either software, or hardware or hardware assisted, allowing for the most flexible and effective deployment. Pricing plans are designed to de-risk and ease transition to new software architectures.

Relevancy to VNFs

F5 offers one of the broadest portfolios of NFV solutions in the market today. That means you can introduce multiple VNF's into the SGi-LAN/Network Edge, EPC or Datacenter - load balancing, DDoS, DNS, CGNAT and more, with Service Function Chaining.

Product Differentiation

F5 has the broadest range of solutions - from traffic management and optimization, policy enforcement to firewall, DDoS and CGNAT and many others. Utilizing services from F5, as one vendor, eases management and reduces costs of operation. Our solutions are supported by our heritage and expertise in software application solutions.

API Support

F5 uses iControl REST API's. iControl is F5's open, web services-based API that allows complete, dynamic, and programmatic control of F5 configuration objects. With iControl you can add, modify, or configure your F5 device in real time. REST is a style of architectural principals with which you can design web services that focus on a system's resources. These interfaces are a method for performing automation and monitoring.

Top Use Cases

F5 traditionally focuses on services in the SGi-LAN, the Datacenter and EPC, so virtual load balancing, DDoS, DNS, CGNAT, network firewall, WAF, policy enforcement and others are typical use cases.

VNF Solution Packaging

VNF (SW package), Service-Based Offering (VNFaaS)

Supported Hypervisors

ESXi, KVM, Hyper-V

Supported VIMs

CloudStack, OpenStack, VMware vRealize/vCAC/vCD

Performance and Scalability

F5 VE's are available in a wide range of performance options and can be sized to suit the application services required. L4 throughput scales from 25Mbps to 40 Gbps.

Industry Association Participation

ETSI, Linux Foundation

Linux Foundation Projects

Cloud Native Computing Foundation, LFN

Key Partners

Atos, Tech Mahindra, Cloudify, Red Hat, Vasona

Key Customers

Large Service Providers in US, France, Australia

Virtual Broadband Network Gateway

(Click to View More Details Online)

https://www.netelastic.com/index.php/products/vbng/

netElastic Systems
PUBLIC | **PRIVATE**
2804 Mission College Blvd.
Santa Clara, California, 95054, United States
rsabin@netelastic.com
4087860453
http://www.netelastic.com

Description of Company: netElastic is a leading innovator of NFV software for carriers with a suite of products leveraging low-cost hardware. All netElastic VNFs are purpose-built to meet the needs of carriers, and include market-leading scalability and performance, massive multi-tenancy, core network integration, and always-on high availability clusters. By providing carrier-class performance and significant cost benefits, netElastic is helping to change the economics of networking.

netElastic Systems in SDxCentral Company Directory

Description of Product: netElastic vBNG delivers market-leading performance and scalability with advanced subscriber management. vBNG combines the capabilities and features of a traditional BNG solution along with the next-generation flexibility and cost benefits of an innovative virtualized solution. vBNG is purely software-based and works with low-cost x86 hardware to provide carriers with faster time-to-market and faster time-to-revenue.

Virtual Broadband Network Gateway in SDxCentral Product Directory

Unique Value Proposition

- A massively scalable network architecture with decoupled control and data planes that can be scaled independently based on network and end-user demands. This results in greater scalability and performance than hardware BNGs.
- A high performance x86 data plane delivers line-rate at 10 Gbps per core and scales linearly as ports and CPU cores are added.
- vBNG's software-based approach and industry-leading scalability helps carriers save up to 70% in costs compared to hardware BNG vendors.

Relevancy to VNFs

IP traffic is exploding and carriers are expected to provide increasing amounts of bandwidth at low costs. netElastic's vBNG enables carriers to meet rising bandwidth demand by delivering market leading performance and scalability at lower costs.

Product Differentiation

- Maximum deployment flexibility to deliver new services faster, whether you're deploying a new rural network or upgrading a large-scale metro POP, vBNG can be deployed for very small subscriber bases all the way up to millions of subscribers.
- vBNG's software can be re-used with future hardware purchases, which significantly lowers total cost of ownership.
- vBNG supports white box switching for greater scalability and lower costs.
- The flexibility and cost benefits of vBNG enables carriers to quickly address new market opportunities for increased revenue and profit.
- vBNG also takes advantage of the ever-increasing power of off-the-shelf x86 platforms to provide the elastic scalability that carriers need.

Key Partners

Intel, Advantech, Lanner, NoviFlow, and Red Hat

Top Use Cases

1. vBNG is ideal for subscriber management in FTTx and DSL access networks and supports VRF/MPLS integration for enterprise small-branch offerings.
2. High throughput makes vBNG a great choice for highly concentrated network environments that require high performance.

VNF Solution Packaging

VNF (SW package)

Supported OSes

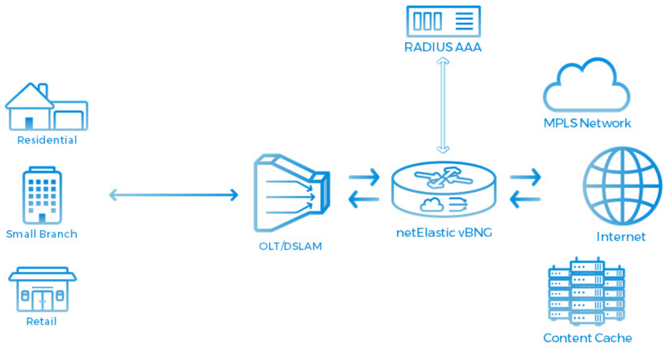
Linux, KVM

Key Customers

https://www.sdxcentral.com/articles/news/centurylink-trials-nfv-startup-netelastics-software/2018/03/

Pricing

netElastic vBNG is priced per session and has a perpetual one-time pricing structure for a given node. We also offer an Enterprise wide license structure that allows carriers the freedom to deploy sessions anywhere in their network environment.



Video Traffic Manager VNF

(Click to View More Details Online)

https://2nuzlzatrf-flywheel.netdna-ssl.com/uploads/MDO2017_Datasheet_Dec2017v2.pdf

Openwave Mobility
PUBLIC | PRIVATE
400 Seaport Court Suite 104
Redwood City, CA, 94063, United States
chris.goswami@owmobility.com
+1 (650) 480 7200
http://www.owmobility.com

Description of Company: Openwave Mobility, an Enea company, empowers mobile operators to manage and monetize encrypted traffic. Based on the industry's most scalable NFV platform, our solutions alleviate RAN congestion, create new revenue opportunities and unify data from virtualized applications. The company provides solutions for mobile video traffic management, cloud data management and targeted promotions.

Openwave Mobility in SDxCentral Company Directory

Description of Product: Video Traffic Manager is a Virtual Network Function (VNF) offering a single-point virtualized solution for all video management and QoE functionalities required on a mobile network. Over 60% of network traffic is video and over 80% of traffic is encrypted, so the challenge for mobile operators is to manage huge volumes of encrypted video while making the best use of precious radio assets. This widely proven VNF effectively enables users to watch more video without incurring RAN congestion.

Video Traffic Manager VNF in SDxCentral Product Directory

Unique Value Proposition

Video is arguably THE most important element of the mobile experience for many subscribers. Video Traffic Manager enables the operator to relieve network congestion in the cells where it is needed, while allowing operators to trade off subscriber QoE against cost of delivery. It accelerates at the TCP level, optimizes encrypted video and keeps up with changing video profiles. It has been deployed in many advanced NFV networks, including Vodafone, Orange, Zain, Reliance, AT&T and Telus.

Relevancy to VNFs

As a VNF, Video Traffic Manager enables intelligent virtualized optimization and TCP acceleration. It can be hosted in the cloud, in-network, or deployed in a NFV environment with dynamic scaling, complying with the industry's initiatives for NFV.

Product Differentiation

Our solution goes beyond simple brute-force optimization offered by others. We adapt to traffic in real-time so operators trade off cost against QoE. We provide flexible rules that vary with real-time conditions, and managed by a powerful NFV orchestration engine. This delivers improved experience to subscribers – quick start, no stutter – depending on costs and conditions the operator sets.

Our solution has won multiple industry awards including Best Product and Best Video Platform.

Openwave Mobility leads industry innovation in this area: we were FIRST to offer Google QUIC and Facebook 0RTT optimization; FIRST to optimize live gaming broadcasts, FIRST to manage encrypted video and 4K UHD; and FIRST to deploy in a fully virtualized network.

Pricing

Flexible pricing options available including per subs pricing and performance based pricing

Top Use Cases

1. Improved video Quality of Experience. QoE depends on quality of delivery (no stutter/buffering) AND quality of picture (eg std versus high def). Video Traffic Manager offers flexible rules dependent on real-time conditions to deliver the QoE you set.
2. RAN Congestion Management. Video Traffic Manager goes beyond the brute-force mobile data optimization offered by many companies and is invoked automatically, on a per location basis, whenever congestion in a specific cell exceeds set parameters
3. Monetizing mobile video as well as minimizing cost of delivery. Intelligent Video Traffic Management enables significant and proven increases in throughput. This can be over 80% and typically means more users can go on to hi-def video plans

VNF Solution Packaging

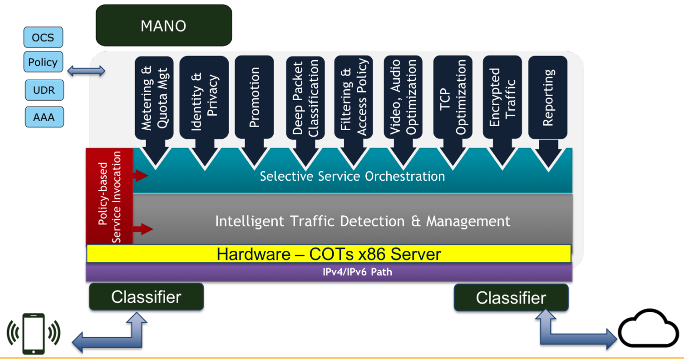
VNF (SW package)

Key Customers

Deployed in many advanced NFV networks, including Vodafone, Orange, AT&T, Reliance Jio, Telus

Key Partners

Huawei, Cisco, HP


MANO
OCS
Policy
UDR
AAA
Metering & Quota Mgt
Identity & Privacy
Promotion
Deep Packet Classification
Filtering & Access Policy
Video, Audio Optimization
TCP Optimization
Encrypted Traffic
Reporting
Policy-based Service Invocation
Selective Service Orchestration
Intelligent Traffic Detection & Management
Hardware – COTs x86 Server
IPv4/IPv6 Path
Classifier
Classifier

NFWare Virtual ADC

(Click to View More Details Online)

http://nfware.com/virtual-adc

NFWare
PUBLIC | **PRIVATE**
http://www.nfware.com

Description of Product: Virtual ADC is the fastest ADC solution on the market. It maximizes the availability, performance and safety of network applications through L4/L7 balancing, TCP-proxy mode, SSL-Offloading, DDoS-attacks prevention, Health Checking, DataPlane Scripting and many more. It also makes DevOps processes simple, with a customizable monitoring and management interface.

Unique Value Proposition

Compared to alternatives, NFWare vADC processes more traffic on up to 200 times less hardware. For virtual and cloud environments, it provides linear and run-time scaling capabilities for effective resource utilization. That is possible due to the Multicore Stack, powered by Dynamic Scheduler technology, developed by NFWare themselves.

Relevancy to VNFs

Designed from scratch based on the NFV concept, NFWare vADC works on commodity x86 servers and in cloud environments to provide cost of ownership optimization, easy integration with APIs and the ability for instant linear scalability.

Top Use Cases

1. LoadBalancer-as-a-service for cloud environment: vADC could be provided as a service to cloud providers' clients or within software-defined datacenters to ensure application availability, maximize performance and protect web-services from DDoS.
2. Improving application response: vADC provides custom rules for flexible traffic steering and, with the help of traffic compression and caching, reduces application response latency.
3. Improving security: vADC provides DDoS protection of backend servers and delivers effective protection through various approaches to ensure that your applications are run safely.

Key Customers

Mail.ru, Vallecas Telecom

Pulse Secure vADC

(Click to View More Details Online)

https://www.pulsesecure.net/vadc

Pulse Secure
PUBLIC | **PRIVATE**
https://www.pulsesecure.net/

Description of Product: Pulse vADC solutions provide fast, reliable application delivery across your virtual and cloud platforms at massive scale. Automated application delivery and centralized management speed and simplify service deployment, while application-level security protects your business.

Unique Value Proposition

The Pulse Secure Virtual Application Delivery Controller (Pulse vADC) has been designed from the ground up as a software-based VNF solution. With support for container-based architectures, Pulse vADC can run a large number of VNF instances, managed from a single control point. This highly automated ADC infrastructure makes it easy to manage ADC services over service lifecycles. This includes provisioning, metering, inventory management, and analytics, all via a software-defined architecture.

Relevancy to VNFs

Pulse vADC solutions enhance the performance, security and visibility of applications in virtual & cloud platforms at massive scale. Agile, lightweight services and open APIs help to automate service orchestration of multi-cloud applications.

Top Use Cases

1. Application Acceleration - Pulse vADC provides tools for intelligent caching, SSL acceleration, and content compression to increase application efficiency and reduce response time, enhancing user experience and application throughput.
2. Service Assurance - Pulse vADC can monitor service levels and route transactions automatically for service availability. Pulse vADC can even provide global load balancing across regions, and supports auto-scaling to adapt to changing workloads.
3. Policy Enforcement - Pulse vADC can monitor bidirectional traffic, and enforce security policies or business rules with traffic inspection, content-based routing, controlling application behavior or resolving security vulnerabilities on the fly.

Key Customers

https://www.pulsesecure.net/customer-success/

Cloud Voice Platform

(Click to View More Details Online)

http://sdx.io/2017-nfv-rpt-lnks-alianza-cloud-voice-platform

Alianza Inc.
PUBLIC | **PRIVATE**
http://www.alianza.com/

Description of Product: Alianza's Cloud Voice Platform is a web-scale, turnkey virtualized software solution that enables cable, telco, and other broadband providers to rapidly customize, launch, and profit from VoIP and UC services. Cloud Voice Platform provides all the elements (servers, virtualization layers, SBC, application servers, media servers, VoIP session control, etc.) required to deliver and manage VoIP services.

Unique Value Proposition

Service providers benefit from a "voice-network-as-a-service" delivered with a SaaS model. Lower overall cost (eliminates CAPEX and reduces OPEX by up to 50%. Simplified operations – APIs for back-office integration and a single interface to manage and troubleshoot voice reduces operational costs, accelerates time-to-revenue and improves customer experience. More rapid innovation (non- disruptive and regular feature releases) means better serving customer requirements.

Relevancy to VNFs

Cloud Voice Platform is a web-scale, turnkey virtualized software solution that powers VoIP and UC services for broadband providers. Alianza's SaaS solution provides the network elements required and makes VoIP easy to manage, agile, and high margin.

Top Use Cases

1. Replacing VoIP 1.0 solutions, softswitch or hosted softswitch white label
2. The system facilitates the launching new business VoIP and UC services, as well as new home phone services

Key Customers

Blue Ridge Communications, Co-Mo Connect, Service Electric Cablevision, Viasat, Xplornet

Metaswitch Voice over LTE

(Click to View More Details Online)

https://www.metaswitch.com/solutions/mobile-solutions/volte-vowifi

Metaswitch Networks
PUBLIC | **PRIVATE**
http://www.metaswitch.com

Description of Product: Only cloud native virtualized network functions running within highly orchestrated container clusters can deliver on the promise of cost-effective, agile, elastic, and resilient service infrastructures and applications. Metaswitch delivers the only complete VoLTE solution built from the ground up using cloud native microservices methodologies and deployable within public, private or hybrid cloud environments.

Unique Value Proposition

Metaswitch is the first company to deliver a complete VoLTE solution built using cloud native software methodologies that can be deployed in public, private or hybrid cloud environments using lightweight Containers. Virtualizing the OS, rather than at the hardware level as with hypervisor approaches, dramatically reduces overheads, thereby enabling our individual virtualized network functions to instantiate immediately, providing both capacity on-demand and resiliency only when required.

Relevancy to VNFs

Mobile network operators can deploy Metaswitch's VoLTE solution in public, private, or hybrid cloud environments using lightweight containers.

Top Use Cases

1. 1. VoLTE: The portfolio of virtualized network functions can be deployed to deliver a complete IR.92 and IR.94 Voice over LTE service infrastructure.
2. 2. VoWiFi: With Metaswitch products, mobile network operators can rapidly offload and extend high-quality mobile coverage by adopting IR.51 Voice over Wi-Fi.
3. 3. Metaswitch dramatically simplifies the process of establishing and maintaining IR.95 VoLTE peering and roaming interconnect services.

Key Customers

https://www.metaswitch.com/solutions/mobile-solutions/volte-vowifi

MediaEngine

(Click to View More Details Online)

http://www.radisys.com/mediaengine/mediaengine-products

Radisys
PUBLIC | PRIVATE
http://www.radisys.com/

Description of Product: The Radisys MediaEngine Virtualized MRF (vMRF) is a media processing powerhouse for a wide range of revenue-generating interactive HD audio and HD video services. The software-only solution is highly optimized to deliver exceptional performance in virtualized and cloud environments. With support for 3GPP IR.92, IR.94 and WebRTC, the vMRF is ideally suited for communication service providers deploying VoLTE, IMS and over-the-top (OTT) services.

Unique Value Proposition

The MediaEngine VNF provides service providers the ultimate flexibility in their choice of cloud and NFV management environments with OpenStack/ETSI-NFV compatibility. It has been engineered to achieve performance and capacity at par with bare metal configurations and it provides a holistic media processing platform for all real-time and non-real time media processing services and applications. Orange Labs Networks has integrated the Radisys media server VNF in the ONAP Amsterdam release.

Relevancy to VNFs

Radisys' cloud-native Virtualized Media Server solution delivers a pre-validated Virtual Network Function (VNF), integrated with Open NFV cloud infrastructure, providing the needed performance, reliability and scalable media processing.

Top Use Cases

1. The vMRF is used in NFV cloud architecture: serves as a common virtualized media processing platform for cloud-based offerings, helping operators accelerate deployment of HD audio and video services.
2. Provides high capacity IP audio & media processing.

Key Customers

Nokia, ZTE, Mavenir, Agnity, GENBAND (Ribbon Communications)

Affirmed Mobile Content Cloud

(Click to View More Details Online)

https://www.affirmednetworks.com/wp-content/uploads/2018/05/GlobalData_Affirmed-Market-DisruptorReport-2.pdf

Affirmed Networks
PUBLIC | **PRIVATE**
http://affirmednetworks.com/

Description of Product: Affirmed's 5G Mobile Core delivers rich set of capabilities including 5G NR, CUPS, optimized IoT access (NB-IoT/LTE-M/SCEF), network slicing, virtualized DPI and GiLAN services, integrated virtual probes, WiFi (ePDG and TWAG), and Service Automation. Combining the Affirmed vEPC with network slicing and the Affirmed Service Automation Platform, operators can rapidly deploy network slices and new revenue-generating services, reducing the time-to-market and operational costs by as much as 90%.

Unique Value Proposition

Affirmed's fully virtualized, cloud-native, 5G mobile core capabilities include 5G NR, CUPS, network slicing, integrated virtual probes, optimized IoT access(NB-IoT/LTE-M/SCEF), virtualized DPI and GiLAN services, WiFi and Service Automation, enabling operators to economically scale networks and take advantage of 5G capabilities today, delivering differentiated services tailored to specific use cases(Consumer, IoT, MVNO, Fixed Wireless) more quickly, and improve the overall customer experience.

Relevancy to VNFs

Affirmed's 5G mobile core(vEPC) solution offers CUPS, 5G NR, network slicing, optimized IoT access(NB-IoT/LTE-M/SCEF), virtualized DPI and GiLAN services, SFC, integrated virtual probes, WiFi(ePDG and TWAG) and Service Automation Platform.

Top Use Cases

1. Etisalat is using Affirmed to deliver broadband and voice services to both mobile and fixed users. Virtualization allows them to economically spin up mobile network cores for IoT, machine-to-machine(M2M), Wi-Fi* calling, and smart city initiatives.
2. Vodafone is using Affirmed Networks' vEPC to deliver M2M communications and connected-car services over their global network infrastructure.
3. Softbank is using Affirmed to deliver IoT services and mobile connectivity to enterprise customers over its nationwide network. Virtualization offers them the flexibility to rapidly deliver customized services over a common network infrastructure.

Key Customers

AT&T, Vodafone, Softbank, Three UK, Etisalat

Ericsson Virtual Evolved Packet Core

(Click to View More Details Online)

https://www.ericsson.com/ourportfolio/it-and-cloud-products/virtual-evolved-packet-core

Ericsson
PUBLIC | PRIVATE
http://www.ericsson.com

Description of Product: Ericsson is industrializing NFV for improved deployment flexibility, built for the most demanding environments. Ericsson's virtual Evolved Packet Core (EPC) provides tested and validated solutions addressing a large number of vertical use-cases thereby opening up new operator opportunities.

Unique Value Proposition

Ericsson virtual EPC is cloud native, with support for highest performance, including 60 Gbps per server with full DPI (SDN World Congress, 2017) and 50M connected devices (MWC 2016). Ericsson provides continuous delivery and deployment of software, full feature parity with native multi-access EPC, and is compatible with surrounding systems from devices and RAN to charging systems and services.

Relevancy to VNFs

Ericsson VNFs are used in 35+ Live commercial deployments, and has 160+ commercial NFV customers in 90+ countries.

Top Use Cases

1. IoT: Ericsson's virtual EPC offers a complete IoT Core slice. Measuring performance in terms of connection rates, 30 million devices can be attached per hour, with a CPU load of less than 30 percent.

Key Customers

Public vEPC commercial live networks include SoftBank, Vodafone and Telstra. 5G Core commercial contracts include Verizon and Swisscom.

Juniper vSRX Integrated Virtual Firewall

(Click to View More Details Online)

https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000489-en.pdf

Juniper Networks
PUBLIC | PRIVATE
http://www.juniper.net/us/en/

Description of Product: Designed for enterprises and service providers, the vSRX virtual firewall delivers core firewall, robust networking, advanced security services, and automated lifecycle management capabilities in a virtual machine. The vSRX gives users the power and control to deploy scalable firewall protection in highly dynamic environments.

Unique Value Proposition

The Juniper Networks vSRX delivers security services that scale to match network demand. It offers the same high-performance NGFW features as the SRX appliance, including core firewall, robust networking, next-generation firewalls (NGFW) and security capabilities such as unified threat management (UTM), intrusion detection services (IDS), Intrusion Protection Service (IPS), and antivirus. Handling speeds up to 100 Gbps, the vSRX is the industry's fastest virtual firewall.

Relevancy to VNFs

The vSRX is a virtual version of the Juniper Networks SRX Series firewalls. As a VNF it can be deployed at the customer premises on Universal CPE device, in the network, or in a a public or private cloud.

Top Use Cases

1. Contrail SD-WAN: vSRX provides integrated security at enpoints using NFX Series Network Services Platform. It offers a secure, flexible, & automated way to connect Enterprise locations together to the internet & multiple clouds, incl. AWS VPC.
2. Private/Public Cloud: vSRX protects against lateral spread of advanced threats b/w VMs within network borders. It provides scalable security for dynamic workloads, protecting apps, & can be a NGFW to extend private clouds into public.
3. Managed Security: vSRX can be deployed in the cloud or on premises to provide NGFW capabilities as part of a managed security service, offering capabilities such as UTM, IDS, IPS, antivirus, & advanced threat protection via integration w/ SKY ATP.

Key Customers

https://www.juniper.net/us/en/company/case-studies/

SD-WAN/vCPE

(Click to View More Details Online)

https://www.netelastic.com/index.php/products/vcpe/

netElastic Systems
PUBLIC | **PRIVATE**
http://www.netelastic.com

Description of Product: netElastic's SD-WAN/vCPE was built for carriers and provides faster time-to-market, market leading scalability and performance, and significantly lower costs. The end result is increased revenue, and greater customer satisfaction, and retention.

Unique Value Proposition

- netElastic SD-WAN/vCPE is a carrier-centric solution with native IP/MPLS support and massive scalability and multi-tenancy.
- Over 1,000 branches can be supported from a single 1RU server, which substantially lowers costs.
- netElastic's VNF marketplace allows carriers to offer new revenue-generating services quickly.
- netElastic's small branch SD-WAN option can be deployed for less than $500 per site and is easily deployed with zero-touch provisioning.

Relevancy to VNFs

netElastic SD-WAN/vCPE enables service providers to deliver secure enterprise networking and drive value-added VNF revenues quickly at high margins. High performance and scalability reduce hardware requirements and lower costs to less than $500/site.

Top Use Cases

1. Low Cost Solution: Small branch/retail locations can reduce costs while still having secure enterprise connectivity up to 100Mbps.
2. Single, Secure Solution: Carrier enterprise customers can have a single solution that works natively with their existing MPLS service and network.
3. Deliver Value-Added Services: Carriers that require secure enterprise networking have the ability to deliver value-added services via software VNFs at the edge or from the cloud.

Key Customers

https://www.sdxcentral.com/articles/news/centurylink-trials-nfv-startup-netelastics-software/2018/03/

Virtualized Network Services (VNS)

(Click to View More Details Online)

http://www.nuagenetworks.net/products/virtualized-network-services/

Nuage Networks
PUBLIC | PRIVATE
http://www.nuagenetworks.net/

Description of Product: Nuage Networks Virtualized Network Services (VNS) solution aligns the network service to the needs of the enterprise and provides the flexibility to deliver an unconstrained WAN experience that matches the dynamic cloud environment. Nuage Networks VNS is the only SD-WAN solution on the market that offers seamless and secure policy based connectivity between the branch, the datacenter and the cloud, as well as advanced security and analytics capabilities with a strong eco-system of partners.

Unique Value Proposition

Nuage Networks VNS is a multi-cloud, application aware virtual networking platform for the DC, WAN and public cloud. Running on commodity hardware, the solution improves business agility and enhances network security and flexibility to connect users to applications in a multi-cloud environment. It provides L2/L3 VPN connectivity as a vCPE on 3rd party uCPEs or as an x86 uCPE that can orchestrate and host multiple 3rd party VNFs in the branch or service chain to a VNF in a CO/POP/DC.

Relevancy to VNFs

The Nuage Networks VNS provides an open, API-driven, scalable, and high-performance virtual networking platform with policy based automation (DC, WAN, Cloud) and a growing ecosystem of technology partners with comprehensive VNF enablement tools.

Top Use Cases

1. Accelerate enterprise site-deployments with a highly-automated virtual network that combines resiliency & secure hybrid WAN support with application visibility and intelligence to optimize the network for high-performance & security.
2. Delivers intelligent, efficient & secure public cloud & SaaS connectivity that increases the availability and improves the performance of enterprise applications regardless of location, cloud provider or the underlay network.
3. Open, boundary-less policy based network automation solution delivering a flexible & high-performance NFV platform with embedded NFV functions with service chaining & NFV hosting capabilities, including orchestration & life-cycle management.

Key Customers

http://www.nuagenetworks.net/customers

Unity EdgeConnect SD-WAN

(Click to View More Details Online)

https://www.silver-peak.com/sites/default/files/infoctr/unity-edgeconnect-sd-wan-solution.pdf

Silver Peak Systems
PUBLIC | **PRIVATE**
https://www.silver-peak.com

Description of Product: EdgeConnect enables service providers to rapidly and cost-effectively bring new, differentiated tiered managed SD-WAN services to market to expand market reach and create new revenue streams in- and out-of-region. Unique application-aware capabilities, such as First-packet iQ, and centralized orchestration provide scalability to support large enterprise deployments. A single VNF integrates SD-WAN, WAN optimization, routing and security functions on vCPE platforms, simplifying WAN architecture.

Unique Value Proposition

The EdgeConnect SD-WAN solution is deployed using either physical vCPE or virtual appliances as a VNF. It's the industry's first fully integrated SD-WAN solution to combine SD-WAN, WAN optimization, routing and a stateful firewall to dramatically simplify management, consolidate branch office infrastructure and eliminate the requirement for conventional routers. EdgeConnect is centrally managed using Unity Orchestrator to quickly and cost effectively deploy new tiered managed SD-WAN services.

Relevancy to VNFs

The EdgeConnect SD-WAN solution uniquely integrates SD-WAN, WAN optimization, routing and a stateful firewall into a single VNF, delivering greater operational efficiency and simplicity of deployment and management than single-function VNF solutions.

Top Use Cases

1. Hybrid WAN: EdgeConnect delivers consistent network & app performance w/ policy-based control across SaaS & IaaS instances & DC applications, assuring service SLAs in & out of region & across any transport, incl. broadband.
2. Cloud Connect: EdgeConnect intelligently & securely directs SaaS & IaaS traffic to cloud providers via public internet or private cloud connect. The solution assures application SLAs & provides real-time visibility across all apps.
3. Local Internet Breakout: With First-packet iQ & Cloud Intelligence, EdgeConnect delivers the highest SaaS & IaaS performance, directing trusted traffic from branches directly to the cloud. An integrated stateful firewall secures sites from threats.

Key Customers

https://www.silver-peak.com/company/customers

NFVTime-Verge

(Click to View More Details Online)

http://www.telco.com/index.php?page=product-description&product=nfvtime-verge&category=sdn-nfv#.WwV38C_MxTa

Telco Systems
PUBLIC | **PRIVATE**
http://www.telco.com

Description of Product: NFVTime-Verge portfolio includes a powerful array of uCPE appliances installed with open NFVI-OS, supporting out-of-the-box and VNFs such as managed router, security and SD-WAN. Additional VNF can be added remotely with zero-touch service provisioning to enable the upselling of new services. The Verge hardware portfolio includes a wide range of Intel and ARM based CPUs, can address broad business and deployment models up to 10Gbps and for a variety complex service chains.

Unique Value Proposition

NFVTime addresses various market segments, including: Small business: secure managed Internet connectivity; Medium business: secure cloud and Internet connectivity, WAN optimization; Medium multi-location business: secure SD-WAN, managed cloud and Internet connectivity; WAN optimization, unified communication; Large enterprise: secure SD-WAN, managed cloud and Internet connectivity, WAN optimization, and unified communication; Education: Secure Internet including content filtering and monitoring

Relevancy to VNFs

NFVTime provides pre-integrated and optimized VNF service chains that addresses all major managed services use cases.

Top Use Cases

1. Open CPE: NFVTime NFVi turns any whitebox device into an open uCPE capable of running any VNF or application designed for KVM/OpenStack environment.
2. SD-WAN and secure SD-WAN: runs any SD-WAN software on its NFVi with out-of-the-box support and can be service chains to vSec to add robust security using best of bread solutions.
3. MEC: NFVi-OS supports Multi Access (Mobile) Edge Compute use cases, providing all the required hypervisor and device lifecycle management need for supporting vEDGE and MEC applications.

Key Customers

Not publicly available.

Versa Cloud IP Platform

(Click to View More Details Online)

https://www.versa-networks.com/products/

Versa Networks
PUBLIC | **PRIVATE**
http://www.versa-networks.com/

Description of Product: Versa Networks Cloud IP Platform is a cloud-native networking and security software platform. For service providers, it enables next-generation managed services with full multi-tenancy for software-defined WAN (SD-WAN), software-defined security (SD-Security) and software-defined branch (SD-Branch). For enterprises, it provides highly scalable Secure SD-WAN with integrated security for multi-cloud and enterprise branch connectivity.

Unique Value Proposition

Versa Cloud IP Platform is a multi-service, multi-tenant software platform built from ground up on cloud principles to deliver scale, segmentation, programmability and automation. It provides a broad set of networking and security functions (SD-WAN, routing, NGFW, UTM, etc) in a single software platform and managed via a single portal. The solution can software-define the entire branch through its ability to host third-party VNFs on its integrated hypervisor.

Relevancy to VNFs

The platform is a cloud-native multi-service & multi-tenant software platform for networking, SD-WAN, Security, and SD-Branch. It is a software solution for secure multi-cloud & branch connectivity for the enterprise and managed service providers.

Top Use Cases

1. Versa Secure SD-WAN enables enterprises and service providers to quickly deploy an application driven and secure hybrid enterprise WAN to improve costs, performance, and reliability.
2. Versa SD-Security enables enterprises & service providers to deploy advanced security to harden the branch & secure direct internet access while reducing the interoperability challenges and complexity of 3rd party security appliances.
3. The Versa SD-Branch combines SD-WAN, SD-Security, local branch networking & hosting of 3rd party VNF's as a unified services platform (uCPE). SD-Branch reduces appliance sprawl and simplifies operations with centralized management and automation.

Key Customers

https://www.versa-networks.com/customers

Carrier Grade NAT

(Click to View More Details Online)

https://www.zcorum.com/solutions/a10-solutions/

A10 Networks
PUBLIC | PRIVATE
http://www.a10networks.com/

Description of Product: The A10 Carrier Grade NAT solution provides high-performance, highly transparent address and protocol translation that allows service providers to extend their IPv4 network, while simultaneously making the transition to IPv6. Operators can preserve the existing IPv4 address allocation and the investment of IPv4-based infrastructure, saving cost and gaining time to plan your IPv6 transition strategy.

Unique Value Proposition

The A10 Thunder CGN proactively solves IPv4 address exhaustion to overcome the challenges associated with the rapid increase of IP address demands for internet-connected devices and BYOD roll out. Thunder CGN delivers advanced features to help service providers and enterprises extend IPv4 connectivity, transition to IPv6 and reduce TCO.

Relevancy to VNFs

For virtual deployments, vThunder Carrier Grade Nat provides the full set of NAT features that run atop leading hypervisors, such as VMware ESXi, KVM and Microsoft Hyper-V, on your choice of virtualized infrastructure.

Top Use Cases

1. IPv6 migration - For example, a deployment at one of the nation's largest mobile carriers uses A10's CGN solution to maintain IPv4 connectivity for the ever growing mobile and smartphone market.
2. High Availability (HA) - Because of active session synchronization, the A10 Carrier Grade Nat solution maintains all active sessions intact if a single A10 device were to lose its power.
3. Cost reduction programs - A10 CGN is cost-efficient (typically 10x to 100x less per subscriber cost versus traditional network vendors). One single A10 device provides more power than multiple hyper-expensive, chassis-based processing cards.

Key Customers

Box, KDDI Corporation, Intermax, CRC Health Group, Micron21 Datacentre Pty. Ltd.

FortiGate VM

(Click to View More Details Online)

https://www.fortinet.com/products/virtualized-security-products/fortigate-virtual-appliances.html

Fortinet
PUBLIC | PRIVATE
http://www.fortinet.com/

Description of Product: FortiGate VM is the VNF version of Fortinet's flagship FortiGate hardware appliances, suitable for, virtual, cloud and NFV deployments. It also offers a rich set of management and orchestration interfaces to support standard-based NFV service insertion and chaining, in addition to interoperability with many NFV MANO and NFVi vendor platforms

Unique Value Proposition

FortiGate VM is the VNF version of Fortinet's flagship FortiGate hardware appliances. It is suitable for virtual, cloud, and NFV deployments. A common FortiOS operating system and FortiGuard services provide the same rich firewall, security functions, and manageability as physical FortiGate appliances.

Relevancy to VNFs

Fortinet’s Security VNFs support the deployment of key security functions in SDN and NFV environments. Our VNF security ensures consistent application of security across heterogeneous networks.

Top Use Cases

1. IaaS Cloud Provides north-south and east-west security for enterprise workloads.
2. SD-WAN Secures traffic at managed enterprise site/branch office when WAN used as network.
3. Virtual CPE Provides gateway.

Key Customers

Fortinet VM solutions are orchestrated in a large number of service provider NFV deployments worldwide designed to scale to tens of thousands of VNFs. Included in the broad range of customers that use FortiGate VM technology are: AT&T (FlexWare), Verizon (VNS), Orange (Easy Go Network), AWS, Microsoft Azure.

Palo Alto Networks Virtualized Next Generation Firewall (VM-Series)

Palo Alto Networks
PUBLIC | PRIVATE
http://www.paloaltonetworks.com/

(Click to View More Details Online)

https://www.paloaltonetworks.com/resources/datasheets/vm-series-specsheet

Description of Product: The VM-Series is a virtualized form factor of our next-generation firewall deployable in a range of service provider networks and private / public cloud environments based on technologies from Openstack, VMware, Amazon Web Services, Microsoft, Citrix, and KVM.

The VM-Series natively analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity, enabling you to improve your security efficacy across all network peering points and ports

Unique Value Proposition

The VM-Series natively analyzes all traffic in a single pass to determine the application identity, the content within, and the user identity. This enables teams to improve security efficacy through a positive control model and reduce incident response time though complete visibility into applications across all network peering points and ports.The VM-Series supports the same next-generation firewall and advanced threat prevention features available in PaloAlto security appliances.

Relevancy to VNFs

The PaloAlto VM-Series Next Generation Firewall can be deployed across multiple service provider NFV/SDN deployment scenarios, as a perimeter gateway, an IPsec VPN termination point, and a segmentation gateway.

Top Use Cases

1. Protect Any Cloud - Enable teams to move toward a cloud-first deployment model that better supports the business.
2. Application Visibility for Better Security Decisions - Provide application visibility across all ports, giving teams far more relevant information about the cloud environment.
3. Improve overall Security Posture - Integrate with a wide range of user repositories.

Key Customers

https://www.paloaltonetworks.com/customers

Session Border Controller Software Edition (SBC SWe)

Ribbon Communications
PUBLIC | PRIVATE
http://www.ribboncommunications.com

(Click to View More Details Online)

https://ribboncommunications.com/products/enterprise-products/session-border-controllers/sbc-software-edition-sbc-swe

Description of Product: The Ribbon Session Border Controller Software Edition (SBC SWe) is a virtual cloud native session border controller. The SBC SWe's architecture is designed to deliver performance and scalability with the same advanced security and interworking features and functionality of Ribbon's SBC hardware portfolio.

Unique Value Proposition

Although the SBC SWe shares common application software w/ the HW versions, it differs from the physical version by leveraging the adoption of a microservices architecture & support for the NFV framework. The SBC SWe can be optimized through technology choices & dynamically orchestrated for lifecycle management of signaling, media & transcoding VNFCs, for interconnect & access SBC use cases. All while delivering carrier-grade security & reliability.

Relevancy to VNFs

Real-time communications continues its migration to the cloud, thus the need for secure interworking between networks must also migrate to the cloud. Ribbon's SBC SWe, meets the security, scalability, and reliability requirements of this migration.

Top Use Cases

1. Virtual Access SBC for SIP Trunking, applicable to cloud-based call centers, unified communications, or Enterprise connectivity.
2. Virtual interconnect SBC for network peering. Highly scaleable solution that rapidly increases service reach and service velocity, especially in new markets
3. SBC-as-a-Service, deployed as a VNF on virtual customer premise equipment (vCPE) in a service provider's cloud domain or as a VNF on universal CPE (uCPE) on the customer premise

Key Customers

Verizon Enterprise Services, Telegate, Veracity, Arrow SI (now part of ConvergeOne)

Network Operations and Analytics

CA Technologies
PUBLIC | PRIVATE
http://www.ca.com

(Click to View More Details Online)

https://www.ca.com/content/dam/ca/us/files/data-sheet/ca-performance-management.PDF

Description of Product: Network Operations and Analytics from CA Technologies is a big data, converged network monitoring platform with full-stack analytics for assuring traditional and SDx networks. This network monitoring platform converts inventory, topology, device metrics, faults, flow and packet analysis into actionable intelligence for NetOps. Customers can troubleshoot issues, optimize resources, demonstrate accountability, analyze anomalies and ensure application and service performance.

Unique Value Proposition

Network Operations and Analytics from CA Technologies is a big data, converged network monitoring platform with full-stack analytics for assuring traditional and SDx networks. This network monitoring platform converts inventory, topology, device metrics, faults, flow and packet analysis into actionable intelligence for NetOps. Customers can troubleshoot issues, optimize resources, demonstrate accountability, analyze anomalies, and ensure application and service performance.

Relevancy to VNFs

The Network Operations and Analytics Platform contains broad capabilities to acquire, present, and analyze network performance metrics across traditional SDN, SDDC, SD-WAN, NFV, and hybrid-could architectures.

Top Use Cases

1. Service Chain Building Block Analytics - Monitor performance of underlying resource components such as virtual machines and vSwitch.
2. vCPE Assurance - Monitoring inventory instantiation as well as performance and fault.
3. Underlay and Overlay Correlation - Mapping overlay exceptions to underlay network faults.

Key Customers

https://www.ca.com/us/company/customer-success.html

Qosmos NFV Probe

Enea, Qosmos Division
PUBLIC | PRIVATE
http://www.qosmos.com

(Click to View More Details Online)

http://qosmos.com/wp-content/uploads/2018/03/Enea-Qosmos-Probe-Datasheet-180215.pdf

Description of Product: The Qosmos NFV Probe provides visibility into virtualized infrastructure. At the heart of this technology is Qosmos ixEngine, the market leading deep packet inspection engine providing detailed real-time IP traffic classification and metadata extraction. The Qosmos NFV Probe can be integrated in two ways:
1. Software instance on a hypervisor monitoring the entire NFVI layer (resources and network)
2. VNF running on a virtual machine to monitor specific VNFs

Unique Value Proposition

At the heart of the Qosmos NFV Probe is Qosmos ixEngine, as well as the company's Deep Packet Inspection (DPI) engine, providing 3000+ protocols classified and 5000 application metadata extracted. Qosmos NFV Probe features include a cloud native solution, with ability to add and remove processing cores and memory at runtime, and virtual network adaptors, support for OVS-DPDK and VPP, and a centralized NETCONF management solution.

Relevancy to VNFs

Physical probes cannot access the logical interfaces between internal VM-to-VM communication to monitor functions hosted on the same server. The Qosmos NFV Probe has been specifically developed to provide visibility into a virtualized infrastructure.

Top Use Cases

1. Trouble shooting: High-degree of information granularity for advanced troubleshooting of faults and performance issues.
2. Service Assurance: Examples of available metadata is Packet loss, Round Trip Time (RTT), Latency, Retransmission count, Application error codes, Jitter delay, Mean Opinion Score (MOS), Individual call flow messages
3. Security: The Qosmos Probe, a Deep Packet Inspection (DPI) sensor, is a perfect complement to signature-based detection tools, such as IDS/IDPS, and full packet capture (FPC), enabling faster, more accurate detection of network infiltration.

Key Customers

Not publicly available.

CloudLens Private with MobileStack

Ixia
PUBLIC | PRIVATE
http://www.ixiacom.com/

(Click to View More Details Online)

https://www.ixiacom.com/resources/cloudlens-private-mobilestack-data-sheet

Description of Product: CloudLens Ixia's platform for public, private, and hybrid cloud visibility addresses the challenges subscriber-aware visibility. CloudLens Private, the arm that supports private cloud technologies, provides mobile carrier-specialized packet-level visibility capabilities tailored to provide them the information needed provide a positive user experience by delivering optimized data to passive, specialized QoS monitoring probes.

Unique Value Proposition

Ixia offers specialized visibility for physical and virtual environments, tailored for the mobile operator evolved packet core through its CloudLens platform. The solution is scalable, subscriber-aware and is multi-platform capable meeting the need of hybrid deployments. CloudLens Private also offers virtual tapping, virtual packet processing, and advanced, Layer 7-based application filtering for applications such as Central Office Rearchitected as a Datacenter.

Relevancy to VNFs

Ixia CloudLens Private provides a complete cloud-based visibility solution for virtual networks, providing total visibility into all inter-VM traffic.

Top Use Cases

1. Allows providers to scale-out monitoring for the evolved packet core.
2. Lowers total cost of ownership (TCO) of monitoring solutions and cost per packet.
3. Is multi-platform capable - works for physical, virtual, and hybrid transitional deployment models.

Key Customers

Not publicly available.

AirSymphony

(Click to View More Details Online)

https://www.airspan.com/wp-content/uploads/2017/02/AirSymphony-Product-Spec-Sheet.pdf

Airspan
PUBLIC | PRIVATE
https://www.airspan.com

Description of Product: Traditional network planning has its limitations when it comes to large and rapid deployments. Connecting Airspan's Small-Cell Controller (SCC) into the existing infrastructure of the operator, improves user experience and maximized network capacity also in extreme hyper dense femto deployments. Centralized AirSymphony platforms complement local virtualized Clusters of Airspan eNodeBs, giving flexibility in the rollout of next generation architectures.

Unique Value Proposition

AirSymphony provides mobile operators the ability to combine different small-cells into a single super cell. Multiple 2x2 small-cells can combine their transmit paths to create a 4x4 MIMO transmission or even higher (8x8) MIMO schemes towards a single UE in the network. Same technics can be used to enhance capacity, increase gain or reduce interference improving user experience, maximizing network capacity and simplifying management.

Relevancy to VNFs

Airspan's Airsymphony centralized processing platform allows the creation and managment of "Virtual" or "Cloud" LTE Radio Access Networks giving big flexibility in the rollout of next generation architectures.

Top Use Cases

1. S1 Aggregation - Terminate all small cell S1 connections and proxies them as a single connection to the MME.
2. X2 Aggregation - Aggregate all X2 interfaces from individual small cells, and present a single X2 for the entire E-SCN to each macro eNB.
3. Enhanced MIMO schemes - Combine different small-cells to create a 4×4 MIMO transmission or even higher MIMO schemes towards a single UE in the network.

Key Customers

Afrimax, Vodafone, Sprint, NFL

Altiostar vRAN solution

(Click to View More Details Online)

http://www.altiostar.com/solution/

Altiostar
PUBLIC | **PRIVATE**
http://www.altiostar.com/

Description of Product: Altiostar's vRAN solution connects the intelligent remote radio heads with the virtualized compute nodes over any transport, including dark fiber, lit fiber, WDM, FTTx, carrier ethernet, microwave, mmWave, or anything else carriers have. If transport is economically and readily available, carriers can use it.

Unique Value Proposition

Altiostar is a mobile broadband provider of Virtual RAN (vRAN) with Ethernet front haul, for software-intensive LTE eNodeB applications. Altiostar's unique solution is designed to improve quality of experience, enhance spectral efficiency and significantly reduce Total Cost of Ownership (TCO) via any existing transport that is economically and readily available giving operators full scale C-RAN ability on all parts of the network.

Relevancy to VNFs

The vRAN solution connects the intelligent remote radio heads with the virtualized compute nodes over any transport providing a carrier grade platform that can provide high availability, ultra low latency and massive scalability.

Top Use Cases

1. Capacity and Performance Gain - Increase the spectral efficiency of the LTE systems to implement LTE Advanced features such as CoMP and Carrier Aggregation.
2. Application Intelligence - Deploy intelligent eNodeBs that understand applications and application states to intelligently.
3. 5G Network Build-out - The vRAN solution is the step towards realization of 5G vision. Software programmability of bearers as per use case is required to create 5G network slices.

Key Customers

Dali Wireless, Corning, SK Telecom

6WIND Turbo Router

(Click to View More Details Online)

http://www.6wind.com/products/6wind-turbo-router/

6WIND
PUBLIC | **PRIVATE**
http://www.6wind.com/

Description of Product: 6WIND Turbo Router provides a high performance, ready-to-use software network appliance for bare metal or virtual machine environments that comprise virtual edge solutions. Turbo Router delivers routing and firewall features with 12 million packets per second per core of IP forwarding throughput, scaling linearly with the number of cores on standard x86 servers. It leverages DPDK for high performance I/Os with multi-vendor NIC support.

Unique Value Proposition

6WIND's vRouter delivers routing and IPsec VPN performance in software that was previously only available in hardware solutions. Customers gain 5x performance increase for software-based IPsec VPNs while using only 1/3 of server resources. Based on DPDK for performance, 6WIND's vRouter separates its full-featured data plane and control plane for use case flexibility. Management options include CLI, NETCONF, RESTCONF and Linux-based tools.

Relevancy to VNFs

6WIND's vRouter is a high performance routing and IPsec VPN software appliance that is ready-to-use in bare metal or virtual machine configurations on x86 and Arm processors inside COTS servers.

Top Use Cases

1. Software Appliances for Network Builders: Use Cases include BGP routing, security gateways, uCPE, PE, BNG, IPsec VPN, CG-NAT, SD-WAN Route Reflector.
2. Source Code for OEMs: Equipment manufacturers can use 6WIND's vRouter in source code to build equipment such as uCPE, BNG, security gateways, IPsec VPNs, CG-NAT devices, and more.
3. Virtual Infrastructure / Hypervisor Networking: OEMs and platform vendors can integrate 6WIND's vRouter software to accelerate hypervisor networking. Software packages are deployed directly into the KVM hypervisor domain for routing and switching.

Key Customers

http://www.6wind.com/company-profile/customers/

ProgrammableFlow Controller PF6800

(Click to View More Details Online)

https://www.necam.com/Docs/?id=6b0e78dc-7d60-4e2e-b550-d456a95da499

NEC
PUBLIC | PRIVATE
http://www.necam.com/sdn

Description of Product: NEC ProgrammableFlow Networking Suite is the first commercially available Software-Defined Network solution to leverage the OpenFlow protocol. It enables full network virtualization and allows enterprises, data centers, and service providers to easily and cost-effectively deploy, control, monitor and manage secure multi-tenant networks.

Unique Value Proposition

ProgrammableFlow PF6800 Controller centralizes control of network services simplifying network management and providing granular, end-to-end network visibility and control, policy-based network management featuring advanced automation and a full set of APIs. Network-wide virtualization, featuring a high performance, resilient network fabric with high availability. Best-in-Class interoperability and investment protection, including support of the 1.3 OpenFlow standard.

Relevancy to VNFs

NEC ProgrammableFlow has multi-tenant capabilities which enable isolated, secure networking to meet stringent compliance and regulatory requirements.

Top Use Cases

1. Centralized Network Administration - simplified network management.
2. Network Automation Multi-tenant Network Segmentation - highly secure, simple to provision network isolation.
3. Service chaining of virtual network functions.

Key Customers

https://www.nec.com/en/global/solutions/sdn/case/index.html

AT&T FlexWare

(Click to View More Details Online)

https://www.business.att.com/content/productbrochures/network-function-virtualization-product-brief.pdf

AT&T
PUBLIC | PRIVATE
http://www.att.com/

Description of Product: AT&T FlexWare, designed and deployed on the AT&T Integrated Cloud platform leveraging Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies.

Unique Value Proposition

Designed and deployed on the AT&T Integrated Cloud platform that leverages Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies, AT&T FlexWare simplifies network infrastructure while potentially lowering capital investments. Customers only need a single AT&T FlexWare Device at each site to run multiple AT&T-certified virtual functions from the best-of-breed vendors (AT&T FlexWare Applications).

Relevancy to VNFs

AT&T FlexWare eliminates the need to buy individual pieces of equipment for firewalls, routers, and other network functions. Customers can download network functions as software to an AT&T FlexWare device. Customers then can scale networks.

Top Use Cases

1. MPLS/global networking - AT&T FlexWare is available in over 200 territories and countries.
2. Flexible service deployments - AT&T FlexWare is modular: you can mix and match FlexWare Devices and Applications and deploy them to your various global locations much quicker than with traditional single purpose built network equipment models.
3. Secure connectivity - Fortinet, Juniper, Palo Alto, and Check Point Virtual Security Options. Help secure your environment with a virtual security solution that offers best-in-class intrusion prevention, virus protection, and Web filtering.

Key Customers

Tech Mahindra, Ericsson, IBM, Pulse Music.

Cisco Virtual Managed Services

(Click to View More Details Online)

http://www.cisco.com/go/vms

Cisco Systems
PUBLIC | PRIVATE
http://www.cisco.com

Description of Product: Cisco Virtual Managed Services (VMS) is a service creation platform that helps service providers easily create and deliver managed network, security, and business services to enterprises. Using VMS, they can create new services or leverage pre-built service packs, such as Cisco SD-WAN and vBranch (vCPE). VMS is a highly extensible API-driven platform, enabling an unlimited range of personalized, differentiated services based on virtual or physical network functions from Cisco and third-parties.

Unique Value Proposition

Unlike do-it-yourself solutions that require large IT budgets and long lead times, Cisco VMS provides a common framework between a business service and service provider's OSS/BSS systems, allowing for rapid and cost-effective delivery of new business services. Unlike point solutions, service providers can go to market quickly with Cisco's pre-built service packs and also develop fully-customized and differentiated services that deliver higher value and command higher prices.

Relevancy to VNFs

Cisco VMS provides provisioning, management and orchestration of business services delivered on physical hardware devices and VNFs, from Cisco and third-parties. VMS delivers automated and secure lifecycle management, provisioning and configuration.

Top Use Cases

1. SD-WAN -- VMS SD-WAN provides a framework of automation and simplification for Managed Service Providers to quickly deploy the Cisco SD-WAN service to multiple tenants at scale.
2. vBranch – VMS vBranch provides a highly customizable framework from which to accelerate service creation and automate deployment for branch-based VNF services.
3. Managed Devices – VMS Managed Devices provides automated device provisioning, management, and monitoring across multiple network elements like routers, switches, and access points.

Key Customers

Verizon, Vodafone

Nokia AirGile cloud-native core

(Click to View More Details Online)

https://networks.nokia.com/solutions/cloud-native-core-network

Nokia

PUBLIC | PRIVATE

http://networks.nokia.com/

Description of Product: The Nokia AirGile cloud-native core network offers the flexibility, responsiveness and adaptability needed to deliver the high performance, ultra-reliability and low latency demanded by the 5G programmable world. Nokia AirGile solution is based on new, modular software architecture built with cloud capabilities and technologies to achieve improved cloud redundancy and software overload protection.

Unique Value Proposition

Nokia AirGile offers unique VNF features such as: Supports a wide variety of business models using multiple fixed and mobile access technologies, meeting the needs of new industry and enterprise customers; Delivers faster new services that depend on extremely low latency, massive connectivity, full mobility and high service availability; As it is built for cloud, it adapts in real-time to dynamic traffic changes it, providing flexibility and automation to manage increasingly complex networks

Relevancy to VNFs

AirGile is built and optimized for the cloud deliver service agility, performance, scale and flexible resiliency. Using cloud-native design principles such as stateless and micro-services architecture to cope with the demands of IoT and 5G.

Top Use Cases

1. VoX (incl. VoLTE, VoWiFi, etc.)
2. Mobile data for broadband and IoT applications
3. Subscriber data management

Key Customers

3UK, Altan Redes (Mex), Reliance Jio, Elisa, Telia

SDxCentral, LLC
3511 Ringsby Ct, #101
Denver, CO 80216 USA
www.sdxcentral.com

Rev A