Market Report

2016 Mega NFV Report Pt. 2: VNFs

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

Table of Contents

NEXT-GENERATION WAN & BRANCH NETWORKS

Network and security functions in software

Versa transforms how service providers and large enterprises build and secure branch networks

VERSA NETWORKS

Learn more about Versa VNF solutions at versa-networks.com

Be Open to the Ideas that Matter Most

Your success with NFV is our concern.

We deliver packaged, independently verified OpenStack NFV infrastructure.

We have a broad set of VNFs to cover your use cases.

We offer management and orchestration to control your multivendor network with its virtual and physical elements.

Take your next step toward NFV success at cisco.com/go/nfv or scan the QR code.

cisco

BROCADE

BREAK THE STATUS QUO:

THINK BIG. START NOW.

When it's time to modernize your network, Brocade NFV and SDN solutions help you and your customers thrive.

The Brocade vRouter improves performance, flexibility, and automation in virtual environments. The Brocade vADC streamlines application delivery. And the Brocade SDN Controller gives you a fully supported controller to run a new wave of SDN apps.

Together, they bring you one step closer to the network of the future.

Start your journey to the New IP today.

www.brocade.com
#NewIP

Introduction – NFV and VNFs Get Commercial

Welcome to the 2016 Mega NFV Report Pt. 2: VNFs, which gives you a full update into the trends and progress in the market for Virtual Network Functions (VNFs). Since our NFV report in 2015, the NFV market is progressing, with operator deployments beginning in earnest. Their primary goal is to create new revenue-generating services on an open, interoperable NFV platform.

For more background, see our **2016 Mega NFV Report Pt. 1: MANO and NFVI**. This report contains some of that information as well as more details and specifics about VNFs.

The main goal of NFV is that it can deliver network functionality via software running on industry-standard commercial off-the-shelf (COTS) hardware. The advantages are that it can provide networking needs of a service provider or enterprises' application on standard server and storage infrastructures. New services do not require new hardware infrastructure – simply software installation.

An open NFV market enables network features and functions to be delivered in the form of software-only VNFs, which can provide the same functionality of just about any specialized hardware device of the past. As a result, functions, such as network address translation (NAT), firewalling, intrusion detection, domain name service (DNS), and even complete suites like EPC (Evolved Packet Core) services can be delivered in software and deployed on general purpose appliances. This gives organizations a lot more flexibility in the way they design, deploy and manage their network services.

How ETSI ISG Created VNFs

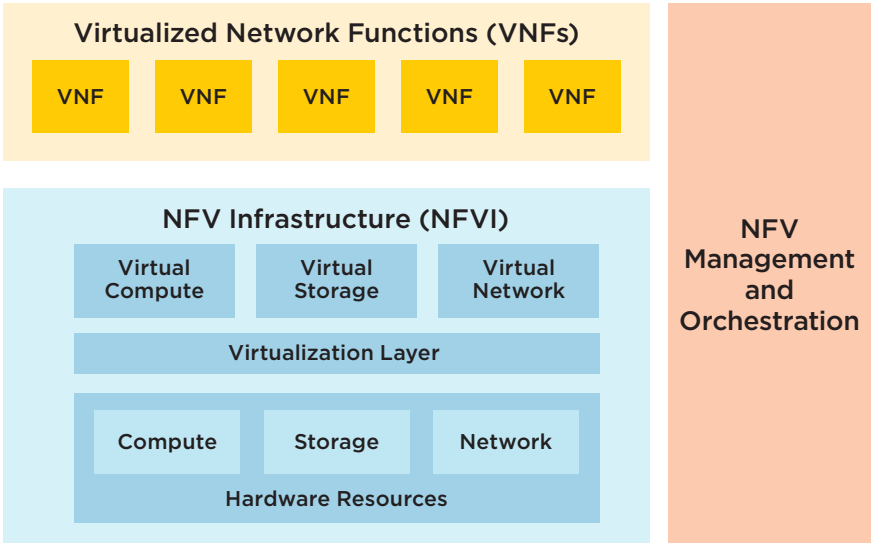
The European Telecommunications Standards Institute's (ETSI) created the Industry Specification Group (ISG) for NFV to accelerate the progress of VNFs. Launched in January of 2013, the ETSI ISG for NFV has been working to develop the requirements and architecture of virtualized network functions in a telecommunication's network.

ETSI created the ISG for NFV to accelerate the progress of virtualizing network functions. The project was driven by the service provider community as operators looked for ways to cut costs and accelerate the roll out of profitable services to monetize their networks and grow their revenues. Hardware-based network appliances, which are typically expensive and complex to deploy and manage, were limiting the providers' ability to consolidate functionality and quickly trial new services.

The ETSI ISG for NFV model includes these components of the NFV framework:

- **Virtualized Network Functions (VNFs)** – The software implementation of a network function.
- **NFV Infrastructure (NFVI)** – The physical resources (compute, storage, network) and the virtual instantiations that make up the infrastructure.
- **NFV Management and Orchestration (NFV MANO)** - The management and control layer that focuses on all the virtualization-specific management tasks required throughout the lifecycle of the VNF.

market summary



Adapted from ETSI publication GS NFV 002: Network Functions Virtualization (NFV); Architectural Framework

HIGH LEVEL NFV FRAMEWORK

As you can see, a number of NFV technologies are needed for customers to achieve the flexibility, scalability, and efficiencies they require.

The establishment of a standardized NFV model has been crucial to the development of VNFs. Nearly all the networking and software players that built specific networking functionality in the past are now focused on building VNFs for NFV platforms. This might include, for example, security companies that previously built specific hardware platforms now turning their focus to software-only VNFs. Later in this report, we'll focus on the VNFs that users are looking for and where the market has the most momentum.

NFV, VNFs, and Beyond

This report presents an overview of the emerging NFV architectures and designs, leading use cases applications, and which VNFs are likely to be particularly hot as the trend gathers momentum.

Our analysis includes examination of hundreds of our news and analysis articles, in-depth interviews we have conducted with technology vendors and end users, and the results of the SDxCentral NFV Survey, which was posted on the SDxCentral site. This survey had 79 end-user respondents, including service providers, (46%), cloud service providers (14%), enterprise end users (14%) and a variety of others (24%) from user communities.

In addition to an overview of VNF technology and an analysis of customer expectations, we also collected data from almost 100 companies. The product information from technology vendors is available at the end of this report

(Editor's note: This is the second part of the series. Part 1 of our 2016 Mega NFV Report covers MANO and NFVI)

What you can expect from this report:

- An overview of NFV and VNFs, describing the evolution of architectural components and potential benefits.
- General use cases and applications for NFV technologies, including feedback from our users in our 2016 NFV Survey.
- Details on different vendor offerings for VNFs, providing insights into the capabilities and maturity of different solutions.

Thank you for downloading this report, we hope you will find it a useful resource, as you look to understand and adopt NFV technologies.

Investment Benefits of VNFs

Network operators and cloud providers want to move to an NFV architecture so that they can deploy new services using VNFs. This means building a business case that they can accelerate revenue while reducing costs associated with service deployment and operations.

Making the move to an NFV architecture is a huge shift. It's a complete change from how services have been deployed for decades, whereby proprietary systems were installed for each service rollout (for example, DSL and mobile services were each built with new hardware architectures). Operators worldwide are currently evaluating the Return on Investment (ROI) for NFV. The goal is a reduction in expenditures (both capex and opex) and by new revenue generated by NFV-related services.

In identifying the business case for NFV, key questions include:

- What are the specific revenue-generating services enabled by NFV?
- Which network elements are good candidates for virtualization?
- How does NFV reduce capital and operating costs?

The Business Case for VNFs

In order to determine the business case for NFV, organizations will likely be looking closely at which VNFs they would be likely to deploy, and how this would alter their business.

Here are some of the potential benefits of deploying VNFs:

Reduce capital expenditures for new VNF deployments:

- The use of commercial off-the-shelf (COTS) hardware and servers reduces hardware costs. A wide variety of providers can offer these servers, increasing the volume and competition in the marketplace and, ultimately, driving down costs.
- By delivering the services in software, organizations are no longer forced to rely on specialized hardware to run network functions. This means the premium that a handful of vendors could charge for their proprietary hardware is no longer applicable or justifiable.
- A single, common server architecture can be used to build in the redundancy and availability organizations require within their data center environment. No longer do organizations need to purchase and maintain expensive equipment to keep as spares; in the event of a failure, the shared virtualized infrastructure can simply move workloads to ensure ongoing capacity and performance.
- The ability to use a shared infrastructure from a cloud provider(s) to run the functions required by an organization turns the capital expense to an operational one to increase capital efficiencies. By renting instead of buying the equipment outright, organizations can take advantage of pay-as-you-grow models and avoid costly and wasteful overprovisioning.
- A side benefit of using less expensive commodity hardware is that an organization can potentially cycle the hardware more often to improve the overall performance of the network. By upgrading the network every 2 to 3 years, instead of the traditional 5 to 7, an organization can continue to effectively address the changing demands placed on their network and increase the value captured throughout the lifetime of those servers.

Accelerate time-to-market for new services:

- Virtualized functions can be easily installed and provisioned to enable an organization to quickly deploy services when, and where they are needed.
- Virtualized functions are conducive to enabling organizations to trial new services, without incurring much risk. Standardized frameworks and the ability to dynamically recover from failures by using an orchestrating

framework enables organizations to dramatically decrease the risk of deploying new products from vendors. The low costs and flexibility of being able to move and scale functionality, as needed, drives service innovation. Proof of Concepts (POCs) and trials can be run faster, in smaller scale environments; "fail fast" prototyping can be achieved, so the organization can adjust and fine-tune their offerings to be confident in wide-scale deployments.

- The ability to run virtual services on top of physical underlay networks means organizations do not need to incur the time or costs of having to forklift upgrade their existing systems to add new services.

Deliver Agility and Flexibility:

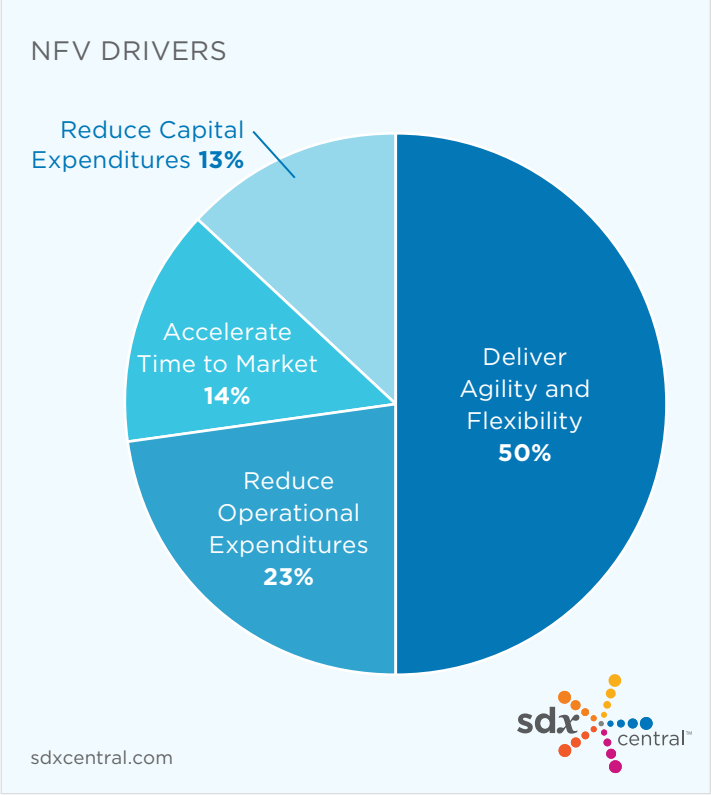
- Because organizations don't have to amortize the cost of expensive equipment or handle "step-function" capital equipment acquisitions (e.g. where they need to make a $M investment to bring up a new service for a single customer), they can quickly and easily address customers' demands. Now, they can provision a couple of servers to offer one-time use or short-term use services.
- The ability to easily tear down, move, scale and configure services as the demands of customers or the business changes gives organizations the ability to bring up services anywhere in the world, any time.

These trends are confirmed from our discussions with industry experts as well as some of the survey data we have collected.

Top Drivers for VNFs

So, we've determined that operators like the VNF model for deploying new services because it offers agility and flexibility, faster time to market, reduced capital expenditures, and reduced operational expenditures. We have also gathered some feedback from end-users about particular VNFs that are of interest in this early stage of the market.

The drivers for VNFs require that NFV technology be adopted first – so the initial needs will be the same. As described in Pt. 1 of our Mega NFV Report, the majority of respondents (50%) to our NFV Survey said it was NFV's ability to "Deliver Agility and Flexibility." "Accelerate Time-to-Market" was identified by 14%, while the remainder of the respondents chose savings as the primary reason to adopt NFV – 23% focused on the operational savings of NFV, while 13% said it was NFV's ability to reduce capital expenditures that was so attractive.



VNFs in the NFV Architecture

The NFV architecture enables network functions to be standardized, allowing for the construction and management of function or functions that best support the organization's environment.

This makes it easy for service providers and enterprises to deploy new services faster, while maximizing their investments in existing platforms.

VNFs in the NFV Framework

As described in the introduction, there are three major components to an NFV framework:

1. VNFs – the virtual implementation of a physical network function.
2. NFVI – the physical resources (compute, storage, network) and the virtual instantiations that make up the infrastructure.
3. NFV MANO – the management and control layer that focuses on all the virtualization-specific management tasks required throughout the lifecycle of the VNF.

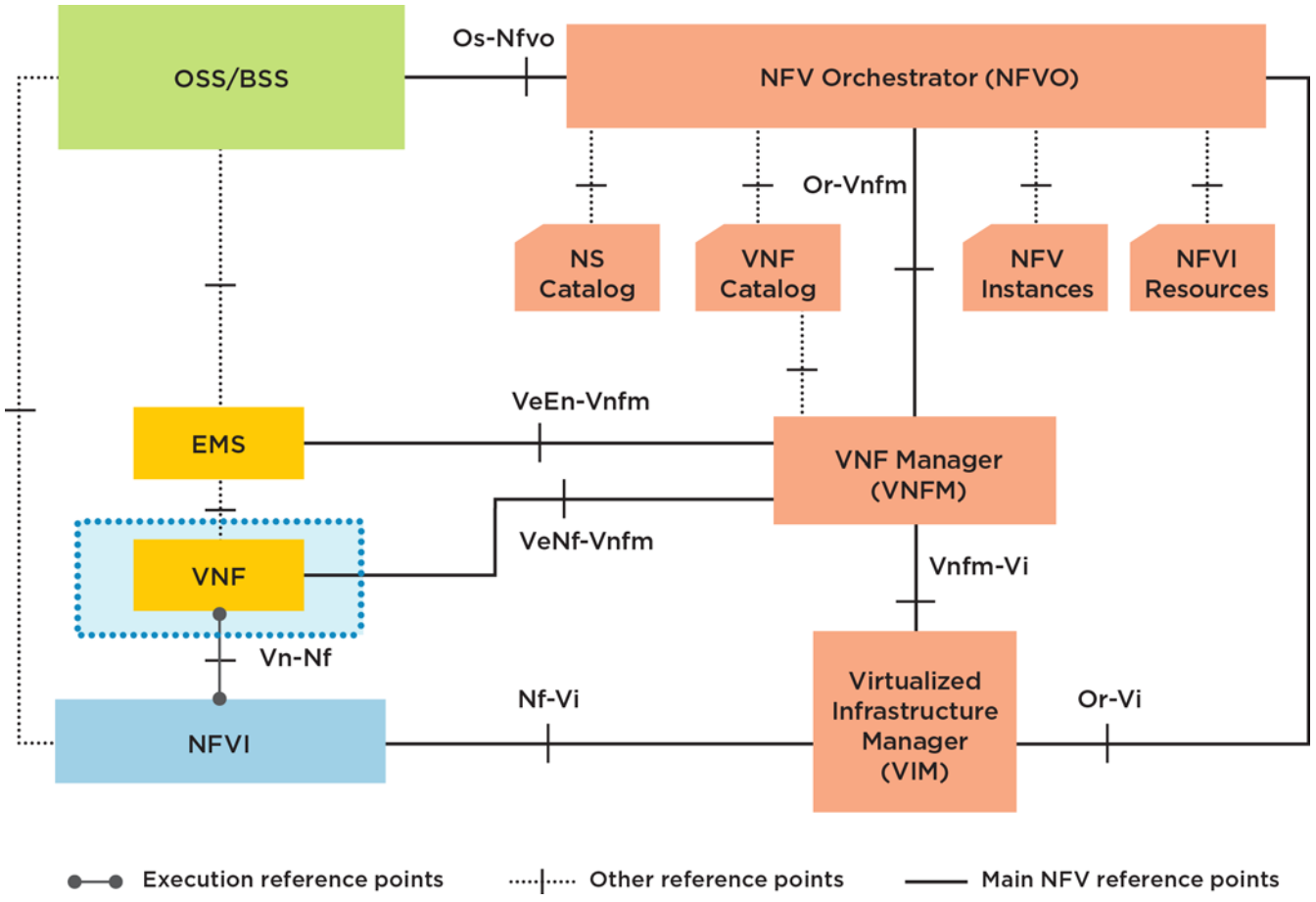
These components fit together in the architecture depicted in the diagram below. Specifically, for this report, we will be focusing on the VNF portion of the infrastructure, which includes VNFs (the actual network functions running as pure software implementations) and VNFCs (VNF components, often library or subcomponents that can be used to modularly build up VNFs).

VNFs are essentially the "stars" of the NFV show as they represent the key functions that service providers are trying to migrate into a virtualized environment. Some examples of common VNFs include vEPC services, routing, caching, security, etc. Most of the VNFs are provided in the form of VMs (Virtual Machines) that run on the NFVI which often includes a hypervisor like Linux KVM or VMware's ESXi. However, we are seeing some more recent implementations that use Linux Containers as their execution environment, addressing some of the performance and memory footprint overhead that VMs have to contend with.

The other elements that come tightly coupled with VNFs are the EMS (element management system) that provide either a programmatic or User Interface to each distinct VNF.

A representation of the key components in any NFV system, including the VNF and its EMS, as well as the other critical pieces is shown here:

market summary



A graphical depiction of the NFV architecture, with the VNF components on the left side in blue.

The VNFs are certainly important to the overall NFV ecosystem, but there are other critical elements of the NFV architecture as well.

The other components depicted in the diagram each contain a number of different NFV technologies which organizations can deploy to achieve the flexibility, scalability and efficiencies they require. Let's look at the elements in the MANO that integrate closely with VNFs including the VIM, the VNFM, and the NFVO.

Based on user feedback, this ETSI NFV architecture has become the roadmap for the NFV industry. When our survey asked if the ETSI ISG architecture was seen as the primary source of standards for the NFV ecosystem, respondents overwhelming replied "Yes" (91%).

VIM Functions and Importance

The virtualized infrastructure manager (VIM) is a key component of the NFV-MANO architectural framework. It is responsible for controlling and managing the NFVI compute, storage, and network resources, usually within one operator's infrastructure domain.

The functional blocks help standardize the functions of virtual networking to increase interoperability of software-defined networking elements. VIMs can also handle hardware in a multidomain environment or may be optimized for a specific NFVI environment.

The VIM is responsible for managing the virtualized infrastructure of an NFV-based solution. VIM operations include:

- Keeping an inventory of the allocation of virtual resources to physical resources. This allows the VIM to orchestrate the allocation, upgrade, release, and reclamation of NFVI resources and optimize their use.
- Supporting the management of VNF forwarding graphs by organizing virtual links, networks, subnets, and ports. The VIM also manages security group policies to ensure access control.
- Managing a repository of NFVI hardware resources (compute, storage, networking) and software resources (hypervisors), along with the discovery of the capabilities and features to optimize the use of such resources.

The VIM performs other functions as well – such as collecting performance and fault information via notifications; managing software images (add, delete, update, query, copy) as requested by other NFV-MANO functional blocks; and managing catalogues of virtualized resources that can be consumed from the NFVI. In summary, the VIM is the management glue between hardware and software in the NFV world.

VIMs are critical to realizing the business benefits enabled by the NFV architecture. They coordinate the physical resources necessary to deliver network services. This is particularly visible for infrastructure-as-a-service (IaaS) providers. The IaaS providers have to ensure that their servers, networks, and storage work smoothly with those onsite. They must ensure that resources can be dynamically allocated based on requirements, which is a key feature of cloud computing.

When a VIM is described, many think of OpenStack VIM software. It's been tested and is in use in provider networks, such as NTT, South Korea Telecom, Deutsche Telekom, AT&T and Verizon. There has been some industry criticism of OpenStack and whether it can be a "carrier class" platform for NFV. There are other major competing VIMs including VMware's vRealize suite and to a lesser extent, CloudStack. As we will detail later, a number of open source projects have been founded to add improved functionality to OpenStack and other NFV platforms to make them "carrier class."

Our survey asked users about the maturity of the OpenStack VIM, and 66% of respondents to the survey said it was "Coming to Maturity, But Needs More Work"; 26% felt the software was "Not Mature at All", while 8% were on the other side of the spectrum, believing it was "Complete and Mature".

The Role of the VNFM

The VNFM is responsible for the lifecycle management of VNFs under the control of the NFVO, which it achieves by instructing the VIM. VNFM operations include:

- Instantiation of VNFs
- Scaling of VNFs
- Updating and/or upgrading VNFs
- Termination of VNFs

VNFs are critical to realizing the business benefits outlined by the NFV architecture. They deliver the actual network functions that create value. But they aren't autonomous. They require VNFMs. VNFMs are critical for scaling, changing operations, adding new resources, and communicating the states of VNFs to other functional blocks in the NFV MANO architecture.

The VNFM also works in concert with other NFV MANO functional blocks, such as the VIM and the NFVO, to help increase the interoperability of software-defined networking elements.

A VNFM may be assigned the management of a single VNF instance or multiple VNF instances. The managed VNFs can be of the same or different types. In the original design, VNF manager functions are assumed to be generic and can be applied to any VNF.

Ultimately, the VNFM maintains the virtualized resources that support the VNF functionality without interfering with the logical functions performed by the VNFs. The services provided by the VNFM can be employed by authenticated and properly authorized NFV management and orchestration functions (e.g., functions that manage network services).

Inside the NFVO

The NFV Orchestrator performs two primary functions including resource orchestration and network service orchestration, as well as other functions.

Resource orchestration is important to ensure there are adequate compute, storage and network resources available to provide a network service. To meet that objective NFV Orchestrator (NFVO) can work either with the VIM or directly with NFVI resources depending on the requirements and architecture as it has the ability to coordinate, authorize, release and engage NFVI resources independently of any specific VIM. It also provides governance of VNF instances sharing resources of the NFVI infrastructure.

This capability is important to solve the new challenges faced by providers as they create new architectures. For example, it might be more important to deploy an NFV-based solution across different points of presence (POPs) or within one POP – but across multiple resources. This would not be easily implemented or perhaps not possible. But with NFV MANO and NFV Orchestrator, service providers now have this capability.

To provide service orchestration, the NFVO creates end-to-end service among different VNFs (that may be managed by different VNFMs) by coordinating with VNFMs as well as the VIMs through their northbound APIs.

VNF Market Landscape

As we have described, network operators and cloud providers are looking at using NFV software and industry-standard hardware to deploy networking applications as VNFs rather than using integrated, proprietary hardware and software systems. This means that just about any application can be deployed with NFV software on top of a standard hardware platform.

This makes the possibilities somewhat endless, and the market for network functions –most of which can conceivably be migrated to software – quite large. It is certainly billions of dollars, if you take a look at traditional network applications such as firewalls, load balancing VPNs, application delivery, mobile evolved packet core (EPC), WAN connectivity, many types of security applications, and IP routing – all of which could be moved (and are being moved) into a VNF model.

VNFs vs. Purpose-built Hardware

The standard question that a network operator might ask about VNFs vs. traditional hardware-based functions is “does it scale” and “is it carrier-class.” The proprietary hardware industry has been formed for many decades and many companies have spent years optimizing their gear, including using custom chipsets, to boost performance. In addition, existing OSS and BSS systems are geared towards physical systems, with the use of VNFs, automation and orchestration play a significantly bigger role with managing the entire lifecycle of VNFs, including creating new instances as and when performance demands it.

Organizations looking at VNFs will have to make careful evaluations about whether or not the VNF measures up to the performance and stability of the function they are targeting as it runs on a purpose-built box. In early POCs, we’ve heard from end-users that some VNFs are poorly-executed as simple ports from physical boxes to a virtualized instance with capacity, throughput and stability issues. As well, the many variations of architectures to extract maximal performance from the underlying NFVI, ranging from PCI pass-through, SR-IOV (single root I/O virtualization on PCI buses), DPDK (Intel’s Data Plane Development Kit), specialized off-loading to NICs (network interface cards) and other acceleration techniques create a lot more complexity than most organizations are willing to sign up for. We expect these teething pains to eventually be overcome. In the

meantime, organizations should also examine the feature-set and performance characteristics of VNFs and how they compare with their physical counterparts.

Key Criteria in Selecting NFV Components and Solutions

Below we have created a chart showing the key criteria that will be used to select an NFV platform and its components. There are different aspects based on the type of product it is – you evaluate MANO component different from VNFs, for instance. However, some general capabilities to consider that have surfaced from our conversations with service providers include:

Capability	Consideration
Conformance with the ETSI Framework	To ensure ongoing interoperability, the solution should conform to the ETSI framework and standards being adopted by the industry.
Performance and Reliability	The solution needs to support the environment in which it will be deployed. In the migration towards a virtualized NFVI and replacing what exists today as physical infrastructure, it is critical to understand the limits, bottlenecks that might exist in the virtualization layer.
Scalability	What kind of scale does the overall system provide – does it scale up (consume more cores) out (run across multiple virtual CPUs) or both? Does it have its own management system that can handle multiple instances? How is load managed?
Compatibility	Many organizations have selected a hypervisor platform for strategic or cost reasons. Organizations need to understand if the NFV solution will be compatible with the environment selected. Likewise, what other elements in the infrastructure will this NFV platform need to interact with. Are there any legacy systems that need to be integrated? How will that integration be achieved.
Programmability	Understanding how easy it is to integrate the NFV solution within an organization's existing environment and program the functionality is key to its success. What type of management stack does the solution integrate with today? What type of APIs are provided and are they sufficiently rich to support business goals?
Security	Given that NFV environments are comprised of multiple vendors, who will be involved in the set up and delivery of different NFV elements, it is important to ensure security doesn't suffer. Organizations should understand the security capabilities offered by each and every component of their NFV deployment to ensure best practices are being followed. (Look to understand the communication protocols, hardening capabilities and patch management tools and processes used to secure functionality.)
Any Specialized Hardware Requirements	Are there any specialized hardware requirements, which could limit the NFV benefits achievable with the system? Examples include requirements for specific NIC hardware or accelerated NICs.

Supported Orchestration Stacks and Management Stacks	What type of EMS is provided with the system and how does it integrate into the existing management frameworks already deployed for NFVI? Does it provide a VNF Manager or integrate with an existing one? How complete is the VNFM feature-set and what hypervisor or OSes does the VNF run on? Bare-metal? What is the maturity of the NFVO? What OSS system does it integrate with and what APIs are provided?
Support	Not all service providers have the luxury of having their own development teams with the right level of expertise. Is the vendor providing the solution capable of providing development and integration services? If open source based, who is responsible for fixing bugs and issues that come up? Is there an SLA that makes business sense?

VNF Market Leaders & Insurgents

Many established networking players sell purpose-built equipment that delivers functions in the process of being converged to VNFs. At the same time, there are insurgents and startups looking to replace legacy hardware with a pure VNF solution.

This will make this market interesting to watch – to see if the incumbents are successful at fending off more nimble competitors offering software-only solutions. Some of the larger incumbents, including the likes of Cisco, Ericsson, and Nokia, are building naturally hedged portfolios that include both purpose-built appliances and VNFs. They see a day when many network functions can be delivered as VNFs, but they will likely try to stall development of these markets to give them time to migrate their products to a VNF model.

Just as in the larger NFV market, the competitive forces in the VNF market can be characterized by three major components: 1) Intra-industry rivals (incumbents) 2) New entrants and 3) Low-cost or free alternatives (open source).

The usual cast of Cisco, Ericsson, HPE, NEC/Netcracker, Nokia, and Huawei are looking with their existing hardware and software management offerings. At the same time, a large number of specialty appliance vendors such as Brocade, CA Technologies, F5 Networks, Juniper, Metaswitch, Oracle, Sonus are taking expertise in their specific markets and converting it to VNFs to expand their competitive portfolios.

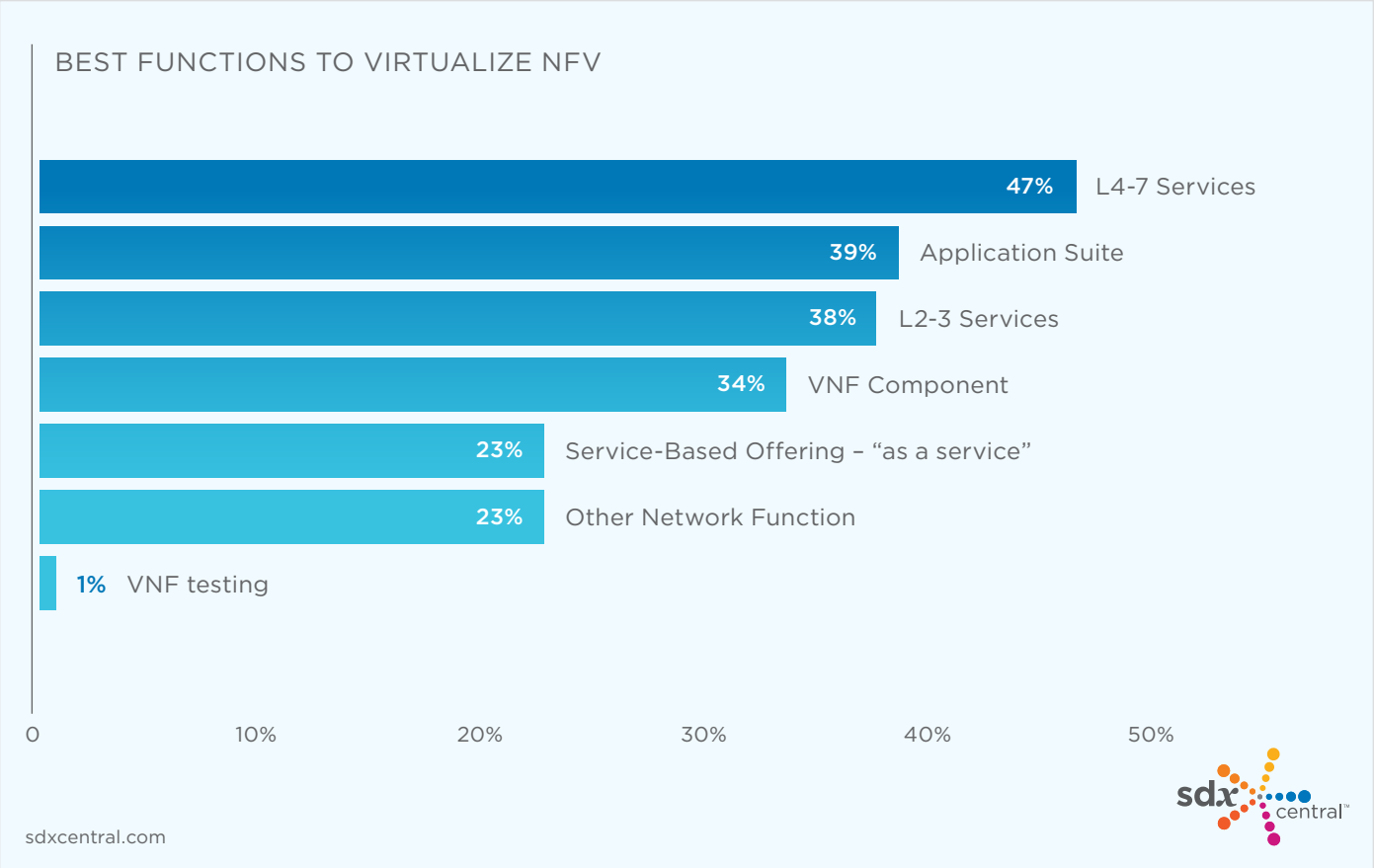
Competition is also coming from the startup world, with companies such as Affirmed Networks and Versa Networks tackling individual VNFs.

Hot VNFs from Our Readers

So what kinds of functions would benefit from being virtualized the most? According to respondents to the SDxCentral survey, L4-7 Services, such as firewalling and intrusion detection and intrusion prevention (IDS/IPS), are the best candidates, receiving 47% of the vote (respondents could pick two). Application suites, such as virtual evolved packet core (vEPC), virtual customer premises equipment (vCPE) and IP Multimedia Core Network Subsystems (IMS) received the second most votes, at 39%, followed by L2-3 Services, such as DHCP, DNS, routing, etc., at 38%.

Service -based offerings, which have been described by the industry as good candidates for NFV (think Virtual Network Function as a Service (VNFaaS) and Virtual Network Platform as a Service (VNPaaS)) were chosen by less than a quarter (23%) of respondents.

market summary

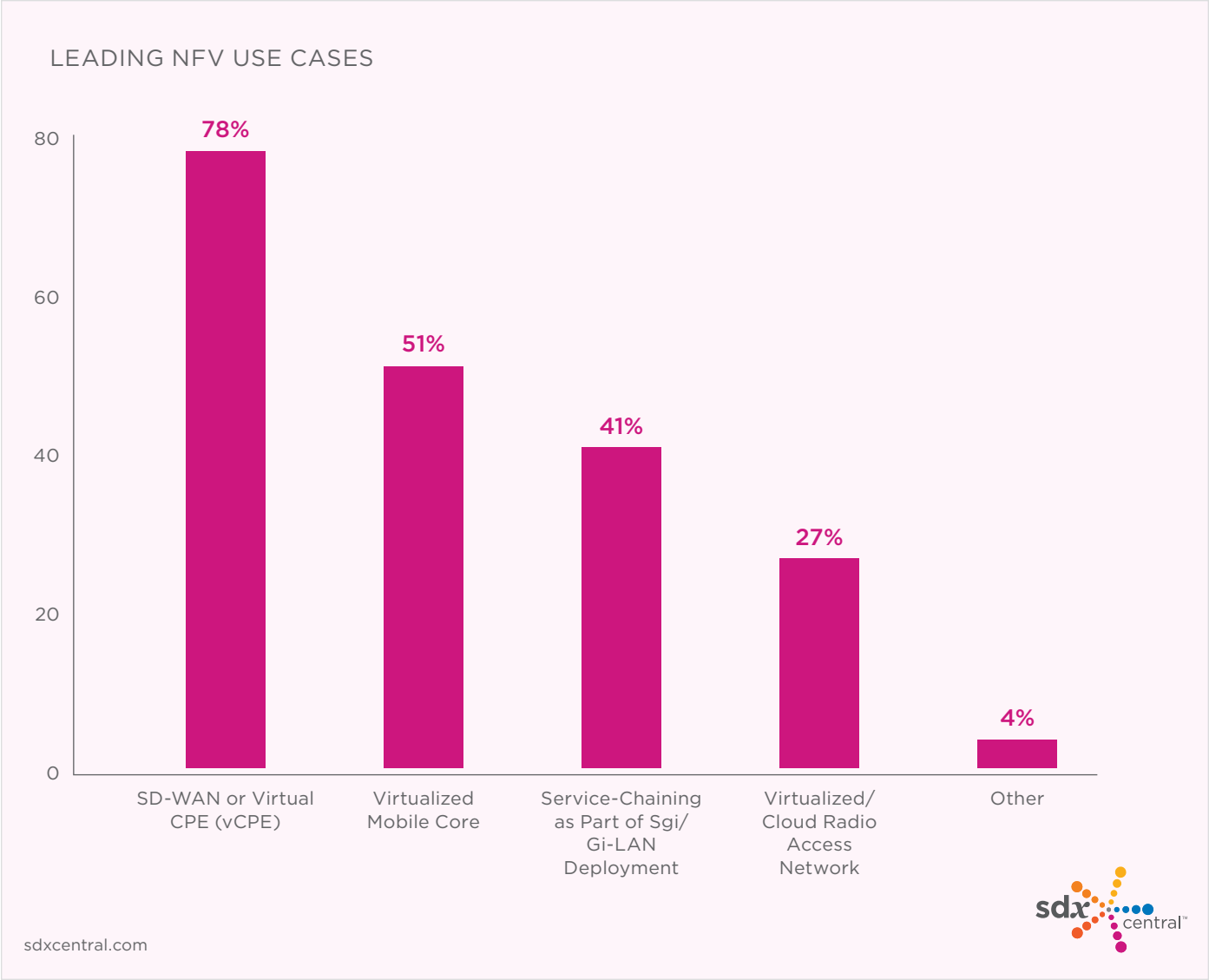


Leading NFV Use Cases

Another way to look at the popularity of VNFs is to ask about specific use cases. Here, the data backs up what we have been seeing in the market, which is broad interest in WAN, VOIP, and mobile connectivity applications.

When probed on the use cases (respondents could pick two) that were most appealing for NFV, an overwhelming 78% of respondents cited the **software-defined wide area network (SD-WAN)** or vCPE. Fifty-one percent identified the virtualized mobile core (vEPC, vIMS, etc.), while 41% noted service-chaining as part of an SGi/Gi-LAN deployment as a good fit.

market summary



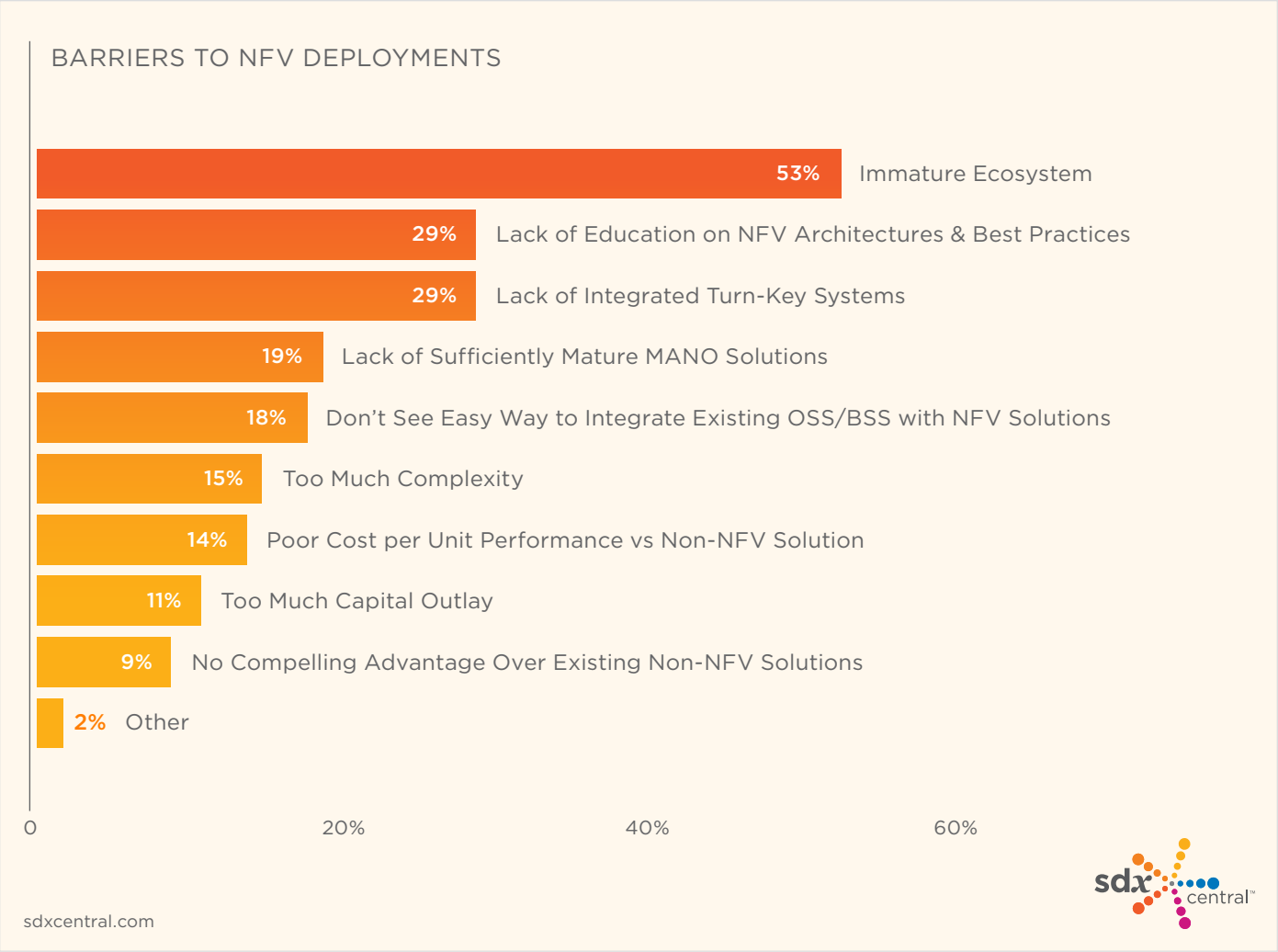
VNF Market Barriers

The market adoption barriers to VNFs are largely the same as with NFV. The market still perceives the stability and maturity of NFV as being a challenge to more rapid adoption.

As described in Pt. 1 of this report series, 78% of respondents to our end-user survey said that they feel NFV technology is starting to mature, but still needs more work. Eighteen percent feel it is “Not Mature at All and Needs a Lot of Work”.

Respondents noted there were a variety of factors that are impeding the faster rollout of NFV. Fifty-three percent said the difficulty certifying and integrating multi-vendor solutions was a barrier, which speaks to the immaturity of the overall NFV ecosystem.

market summary



Twenty-nine percent of respondents said a lack of turn-key NFV integrated systems and general education on NFV architectures and best practices were hindering deployments, which also indicates how early the market still is.

Nine percent of respondents felt they couldn't see a compelling advantage for NFV over existing solutions. With such a minority doubting the validity of the VNF approach, the market will likely continue to invest in developing standards and building out the capabilities of their services.

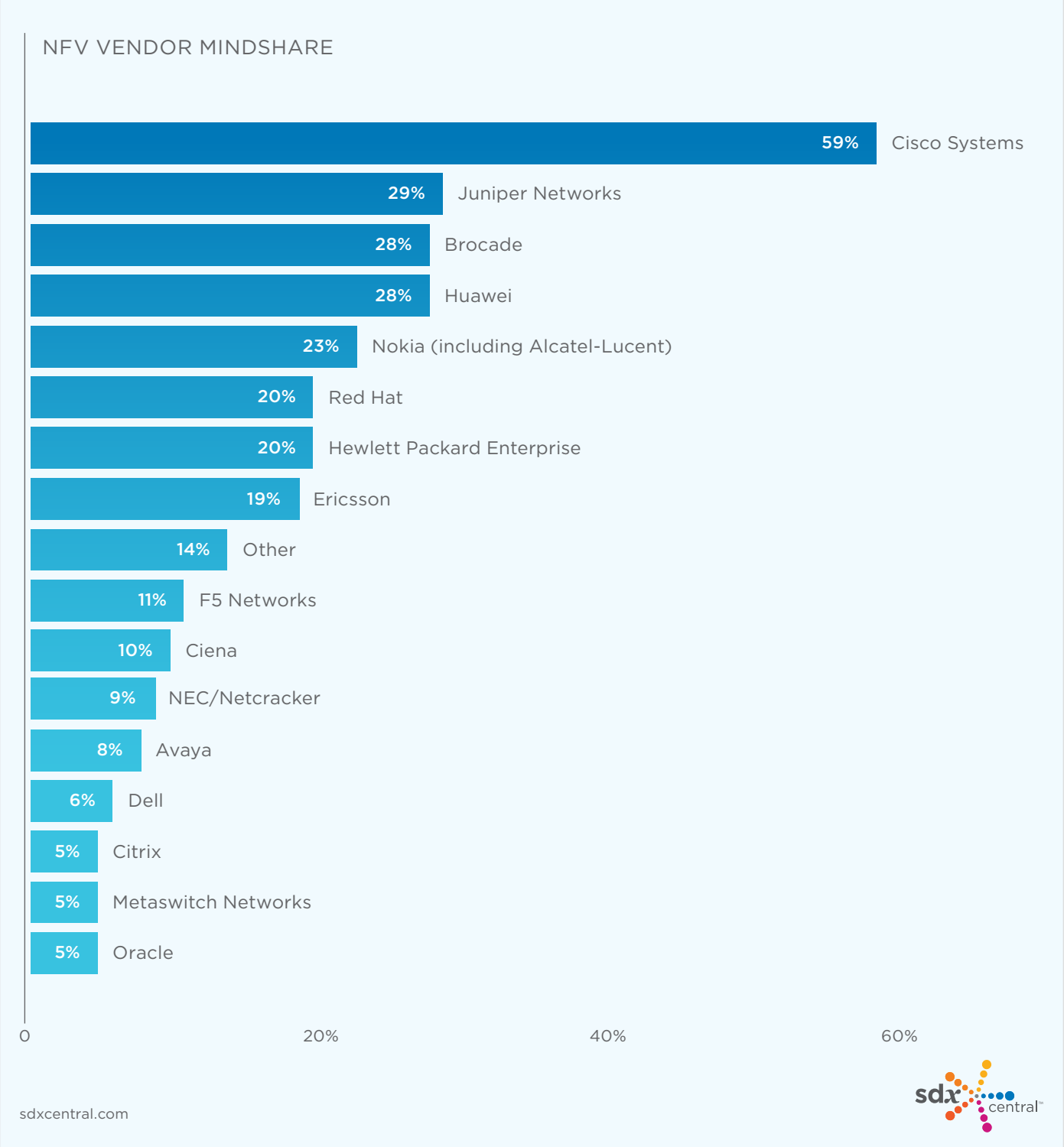
Conclusion: VNF Market Offers Opportunity

While the relative immaturity of existing NFV solutions is still in question, it's clear from our research that the end-user market embraces the need to move to a software defined model for deploying new network applications, which requires VNFs. Because it is still early in the development stage of the market, there is plenty of time for both incumbents and insurgents alike to develop compelling, high-performance VNFs that will work on an NFV platform.

As we discussed in Pt. 1 of this report series, our research indicates that users are looking at solutions from many vendors and are open to many different products. The nature of the NFV movement encourages interoperability, which means users will be able to consider many different vendors. Respondents to the SDxCentral survey showed that many vendors are in the mix, with few dominating the conversation. Only Cisco

market summary

received a majority of the vote, at 59%. Other leading NFV vendors include Juniper Networks with 29% of the vote, followed by Brocade and Huawei, who were each chosen as leaders by 28% of respondents. Nokia (including Alcatel-Lucent) and Hewlett Packard Enterprise received 23% and 20% respectively.



There is a lot of opportunity for both established players and new entrants to make noise and gain share with compelling VNFs.

VNF Products

VNFs are software-only applications designed to run network services on an NFV platform. A VNF is designed to consolidate and deliver the networking components necessary to support a full virtualized environment.

VNFs work with the key components described in **2016 Mega NFV Report Pt. 1: MANO and NFVI**, including the NFVI, VNFM, VIM, and MANO. These are the key technology pieces needed to build a NFV platform to run VNFs, yet other technology integration is usually required. In order to properly deploy a VNF, integration with a network operators OSS and billing systems or Business Support Systems (BSS) is usually required.

Once installed, a VNF runs the specific network functions that run on one or more virtual machines (VMs) on top of the hardware networking infrastructure – routers, switches, etc. Individual virtual network functions can be connected or combined together as building blocks to offer a full-scale networking communication service.

Because of the wide range of VNFs possible, the market for VNFs is quite large and many companies are looking to convert traditional networking functions into VNFs. It includes companies converting existing, hardware- or appliance-based functions into software-only functions. Some companies, including startups, are targeting specific VNFs such as vEPC, IMS, and vCPE with their VNFs.

VNF Service Offerings

In addition to VNFs being offered as discrete software functions that can be deployed on an NFV platform, VNFs can also be offered in the cloud in an "as-a-service" format, thus begetting NFVaaS (fun with acronyms!)

Although most VNFs being marketed today are sold as software VNFs, we expect that areas such as security, voice, and WAN will offer many opportunities for an NFVaaS cloud services model. There are already some interesting new business models evolving for players that want to offer NFVaaS.

It's early days, but expect this category to grow over time.

Vendor Profiles

The following sections profile many of the vendors in the NFV market. The individual profiles were created through a collaborative effort between SDNCentral's Research Team and the Vendor's product experts. SDNCentral worked under the assumption the information provided by the vendors was factual, auditing the submissions only to remove unverifiable claims and hyperbole. Extended profiles can **be viewed online**.

While every attempt has been made to validate the capabilities listed in the profiles, SDNCentral advises end users to verify the veracity of each claim for themselves in their actual deployment environments. SDNCentral cannot be held liable for unexpected operations, damages or incorrect operation due to any inaccuracies listed here. SDNCentral welcomes feedback and additional information from end users based on their real-world experiences with the products and technologies listed. The SDNCentral research team can be reached at **research@sdxcentral.com**.

POWERING NETWORK TRANSFORMATION AND SERVICE INNOVATION

PIONEERING OPEN NFV SOLUTIONS FOR COMMUNICATIONS PROVIDERS

- » Session Border Controllers
- » IP Multimedia Subsystem
- » Voice / Video App Servers
- » Complete VoLTE Offering

TO LEARN MORE, VISIT METSWITCH.COM

Metaswitch Networks


WHAT'S THE BIG NFV IDEA?
Endless possibilities now actually possible.
Build more ideas, more quickly with NFV that's open, flexible and automated. www.juniper.net/big-nfv-idea
JUNIPER NETWORKS

Next Generation VNFs for Intelligent and Secure Real Time Communications

Sonus Solutions: Session Border Control, Policy Management, Diameter Signaling Control.

Sonus™
Cloud communications made smarter

To learn more about Sonus' NFV initiatives visit us online at sonusnet.com or call 1-855-GO-SONUS

BROCADE

130 Holger Way
San Jose, CA 95134
www.brocade.com
1.888.BROCADE

Brocade 5600 vRouter

(Click for Online Version)

www.brocade.com/en/products-services/software-networking/network-functions-virtualization/5600-vrouter.html

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: vRouters, Security (NAT, SBC, Policy, Identity and DPI Solutions), Service Assurance & Monitoring (Tapping, NPB)

Description: Built for Network Functions Virtualization (NFV), the Brocade 5600 vRouter is the first virtual router capable of providing advanced routing in software without sacrificing the reliability and performance of hardware networking solutions. It offers advanced routing, stateful firewall, and VPN capabilities in a high-performance software form factor. This platform utilizes innovative Brocade vPlane technology, enabling hardware-like routing performance in a software-based network appliance. By offering carrier-class performance and reliability in a software solution, the Brocade 5600 vRouter changes the economics of networking while driving innovation inside and outside the data center.

Uniqueness: The Brocade Vyatta vRouter has been optimized and engineered with specific focus on virtualization, and has been tuned appropriately to operate at high performance levels and scale in a virtual form factor. The highly tuned and optimized platform utilizes the underlying compute and memory resources for high speed packet processing functions while also maintaining a highly optimized and reduced virtual footprint. The combination of a low virtual footprint, it's capabilities of driving high throughput per physical core and a development strategy of focusing on virtual optimization are some of the unique capabilities and differentiators the platform provides for NFV adopters.

Supported Hypervisors
ESXi, KVM, Hyper-V. The Brocade 5600 vRouter supports the integrated hypervisor within the Brocade Vyatta Network OS for vCPE deployments. The Brocade 5600 vRouter also supports Xen based hypervisors.
Supported OS
Linux (Red Hat Enterprise Linux, Ubuntu and Cent OS)
Supported CMP
OpenStack. The Brocade Vyatta Network OS supports any CMP that utilizes NETCONF/YANG models as the method for orchestration and instantiation of VNFs
Supported HW Acceleration
The VNF leverages Intel DPDK for the creation of a high speed packet pipeline within the data plane. The VNF also supports the use of SR-IOV and PCI pass through for dedicated NIC assignment and higher performance.
Management Framework
The Brocade vRouter has been integrated into MANO tools from partners such as Ciena and is supported by the Brocade VNF Manager. The Brocade vRouter supports most MANO frameworks which leverage NETCONF and YANG
Pricing and License Model
The Brocade vRouter is offered in a Capacity Based deployment model offered in a subscription, perpetual and monthly consumption based model.

Use Cases Supported
Virtual Edge (vCPE, vCE, SD-WAN)
Customer Use Case #1: vCE
The Layer 3 service is moved from the physical premises and brought inside of the xSP infrastructure and simplifies the on-premises to be a NID and the VNFs are deployed to the POP/CO. The POP/CO has the opportunity to host and share servers amongst customers, and leveraging the efficient footprint of the vRouter VNF can co-locate a high density of vCE routers in a single platform – offering up reduction in power and cooling www.sdxcentral.com/brocade/building-the-virtual-customer-edge-vce
Customer Use Case #2: vCPE
The on-premises device is replaced with a whitebox or white label compute platform capable of housing multiple VNF's to provide the networking services necessary. Offers a high degree of automation and flexibility and reduce CAPex and OPex by minimizing truck rolls for new service insertion www.sdxcentral.com/brocade/virtual-cpe-on-premise-vcpe
Product Datasheet
www.brocade.com/en/backend-content/pdf-page.html?/content/dam/common/documents/content-types/datasheet/brocade-5600-vrouter-ds.pdf

category: ■ VNF

FEATURED

BROCADE

130 Holger Way
San Jose, CA 95134
www.brocade.com
1.888.BROCADE

Brocade VCM

(Click for Online Version)

http://www.brocade.com/en/products-services/mobile-networking.html

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Packet Core / Gateways

Description: Brocade® VCM is a full-function Evolved Packet Core (EPC) solution designed for virtualized environments. Organized in independent slices of the control, user, and management plane, Brocade VCM is free of the redundant functionalities and inter-node dependencies that increase costs and reduce performance in physical node-based packet cores. Brocade VCM, running on Intel x86 servers, provides linear-scaling performance to support any size network for cost-effective business growth.

Uniqueness:

- Significantly reduces infrastructure deployment costs with a micro service based modular architecture, allowing throughput, transaction, and session capacity to be added independently
- Optimizes resource usage and increases business agility through on-demand scalability
- Leverages a highly optimized architecture with full Evolved Packet Core (EPC) functionality to achieve maximum performance across the separate control plane and user plane
- 5G ready architecture that can support low-latency use cases through a portable user plane that can be placed at the network edge
- Eliminates overhead and latency in processing user data on Virtual Machines (VMs), providing line-rate performance on an Intel x86-based platform

Supported Hypervisors	Supported OS
ESXi, KVM	Linux (CentOS 6.4)

Supported CMP

OpenStack, VMware vRealize/vCAC/vCD, Ciena BluePlanet, Amdocs Network Cloud Service Orchestrator, Nokia CloudBand

Supported HW Acceleration

Brocade VCM has a modular architecture with independent control and user plane. Brocade VCM's user plane is optimized with Intel DPDK and provides line rate performance on virtual machines with small size packets. Brocade VCM is also tested with PCI pass-through, SR-IOV, and OVS.

Management Framework

In ETSI NFV reference architecture, Brocade VCM acts as a VNF and a part of VNFM so monitor and manage the VNFCs inside VNF. Brocade VCM provides all aspects of FCAPS information to an external orchestrator and/or NMS using various APIs, including REST, SNMP, XML, and CLI.

Scalability and Performance

- Independent control and user plane scaling with on-demand, linear scalability
- Control plane: TPS, number of SAUs/bearers
- User plane: Throughput, TPS

Use Cases Supported

MVNO (Mobile Virtual Networks), Virtual Mobile Core (vEPC), 5G, IoT, Private LTE for Industrial, Enterprise, or public safety

Customers

There are many trial and production customer engagements but we cannot share the names at this point. Two of the public announcements include Smartsky and Telefonica.

Customer Use Case #1: MVNO/MVNE: Delivers a flexible & cost effective mobile core solution

- Multiple deployment models to enable the network: Brocade VCM can be deployed as vPGW or vPGW+HSS for a turnkey solution
- Increased service velocity to deploy, test and enhance new services quickly
- Lower introduction and operational costs to maximize revenue margins

Pricing and License Model

Brocade VCM provides simple, disruptive, and value-based perpetual licensing model. It provides incremental usage based pricing that is not tied with number of attached users, subscribers, or bearers. This model can be applied to both consumer and IoT use cases without any penalty of overpaying for either case.

FEATURED

CISCO SYSTEMS, INC.

170 West Tasman Drive
San Jose, California 95134
800.553.6387
www.cisco.com

OPNFV: Y **ETSI NFV ISG:** Y

Cisco Ultra Services Platform

(Click for Online Version)

www.cisco.com/go/ultra

Sub-Category: Packet Core / Gateways, Policy, Gi-LAN services
Description: Cisco Ultra Services Platform is the first and only solution that delivers multi-G packet core functions, Gi-LAN services with service chaining, and Policy, operating as a single VNF. It is 5G-ready, offers unmatched TCO savings, and opens new market opportunities.
Uniqueness: Cisco Ultra supports control and user plane separation (CUPS). Its architecture allows you to centralize the control and management planes and distribute its SDN-enabled user plane closer to the RAN to scale efficiently and lower latency. Remote DCs can fail over with zero impact to customers. End-to-end network slicing enables service innovation and acceleration.

Supported Hypervisors	Supported CMP
KVM	OpenStack
Supported OS	**Use Cases Supported**
Linux (RHEL)	MVNO, vEPC, 5G, IoT

Cisco Adaptive Security Virtual Appliance (ASAv)

(Click for Online Version)

www.cisco.com/c/en/us/products/security/virtual-adaptive-security-appliance-firewall/index.html

Sub-Category: Security (NAT, SBC, Policy, Identity and DPI Solutions)
Description: Cisco ASAv offers the same security features as the ASA appliance. It is designed to work in multiple hypervisor environments with multiple vSwitches to secure DC traffic and multi-tenant deployments, increasing flexibility and operational efficiency.
Uniqueness: Cisco ASAv supports fabric-based deployment with Cisco ACI and traditional tiered deployment. With ACI ASAv services are managed as a pool of security resources you select and attach to specific applications or transactions, providing dynamic, scalable, policy-based security. A common policy works across physical, virtual, application-centric, and cloud resources.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V	OpenStack, VMware vRealize/vCAC/vCD

Cisco CSR 1000v, IOS XRv 9000 and Nexus 1000v

(Click for Online Version)

www.cisco.com/c/en/us/products/switches/virtual-networking/index.html#~Products

Sub-Category: vRouters, vSwitches
Description: CSR 1000v (IOS XE), IOS XRv 9000 (IOS XR) and Nexus 1000v (NX-OS) use the same operating systems as their related physical routers and switches, minimizing impact to operational processes.
Uniqueness: IOS XRv 9000 maximizes forwarding with Cisco Vector Packet Processor (VPP) for Intel x86 and delivers advanced classification using Intel SSE2 and AVX instructions. Nexus 1000v port profiles ease assignment and portability of networking and security policies. With VPath Nexus 1000v enables movement of VMs among servers in different L2 domains.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V (Nexus 1000v only)	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Use Cases Supported**
Linux (multiple), Windows (Windows Server 2012)	vCE, vCPE, vPE, vRR, DC Switching

Cisco Virtualized Video Processing (V2P)

(Click for Online Version)

www.cisco.com/go/v2p

Sub-Category: Video / Media / Messaging
Description: Cisco V2P offers programmable and elastic application infrastructure for video data plane functions – acquisition, ingest, encoding, transcoding, recording, packaging, storage, and publishing for multiscreen.
Uniqueness: V2P is a unique open platform to host, configure and manage Cisco or 3rd-party standard media data plane functions. Via open APIs, it manages the life cycle of these virtualized media apps, deploys them across hybrid infrastructures (bare-metal, cloud OS platforms, and docker/containers) and dynamically chains them for use cases into complex workflows.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD

FEATURED

category: ■ VNF

JUNIPER NETWORKS, INC.

1133 Innovation Way
Sunnyvale, CA 94089
www.juniper.net
vmx-lead-gen@juniper.net

vMX/vSRX

(Click for Online Version)

www.juniper.net/uk/en/products-services/routing/mx-series/vmx
www.juniper.net/us/en/products-services/security/srx-series/vsrx
OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: vRouters, Security (NAT, SBC, Policy, Identity and DPI Solutions),, Network Services (DHCP, DNS), L2-3 services (DHCP, DNS, Routing), L4-7 services (Firewall, IDS/IPS, etc), Application Suite (vCPE, other), IPSec VPN, FW, IDS, URL Filtering, Anti-Virus, Anti-Spam, AppSecure, AppTrack, AppQoS, AppFW

Description: The vMX is a virtual MX Series 3D Universal Edge Router with full-featured, carrier-grade capabilities including complete control, forwarding and management planes, making it an ideal platform ideal for service providers and enterprises. The vSRX is a virtual firewall featuring robust networking, advance security (built on AppSecure 2.0 services that deliver a comprehensive threat management framework such as Firewall, IPsec VPN, NAT, IDS, UTM and Application visibility), and automated lifecycle management.

Uniqueness: The vMX uniquely brings the Junos control plane and the programmable Junos Trio chipset to the virtual world, enabling rapid deployment and easy scale-out options. The vSRX uniquely bundles networking and advance security services that leverage analytics to stop threats faster. Juniper has flexible and open automation and management expertise with NETCONF, Virtual Director and integration with Contrail Cloud. For service providers, new services can deliver faster into new markets with lower risk and costs. For enterprises, this solution will adapt to new workloads, increase operational efficiencies and drive greater business outcomes for their core business.

Supported Hypervisors
ESXi, KVM. vMX also supports XEN PV
Supported OS
Linux (Ubuntu/CentOS)
Supported CMP
OpenStack, VMware vRealize/vCAC/vCD, CloudStack, Juniper's Contrail OpenStack
Scalability and Performance
vMX: 1) Flexible and efficient license options provide scale starting from 100Mbps. 2) Validated throughput through 160Gbps. 3) Performance optimization using Intel DPDK, SR-IOV vSRX: 1) Optimized to leverage multiple CPUs to maximize packet process and overall throughput. 2) Leading price to performance. 3) Upcoming performance optimization using Intel DPDK and SR-IOV With the vMX, the innovations of Junos and vTrio are leveraged to deliver the best packet forwarding engine in a virtual device. With the vSRX, performance and advance security features are combined to deliver agile and scalable security solution. Managed with the Contrail Cloud, virtualized resources can be scaled up or down on demand and scale beyond the cloud/data center boundaries to deliver tremendous versatility and operational efficiency empowered with Juniper automation.

Use Cases Supported
MVNO (Mobile Virtual Networks), Virtual Edge (vCPE, vCE, SD-WAN), VoLTE, Virtual Broadband Network Gateway (vBNG); Virtual Route Reflector (vRR); Virtual L2TP network server (vLNS), Virtual Traffic Detection Function (vTDF)
Customer Use Case: Juniper vCPE Solution
Juniper vCPE overcomes the cost, delay and inflexibility associated with physical CPE deployments and opens opportunities to automate current deployments and tap into new markets with rapid, customizable implementations. The vMX and vSRX provide centralized control and low touch deployments, and value added services such as firewall, IDS, DPI and other L4-7 applications can be chained together to offer a rich and highly customizable service catalog.
Ecosystem Partners
Juniper has a comprehensive and ever-expanding set of Ecosystem partners, www.juniper.net/us/en/partners/technology-alliances/data-center/#vnf-technology-developers
Pricing and License Model
The vMX is priced based on throughput, permitting capitally efficient 'pay as you grow' scale. The vSRX provides a base package and optional advanced security services via perpetual, subscription or utility based models.

METASWITCH NETWORKS

201 Potrero Ave
San Francisco, CA 94103
www.metaswitch.com
www.metaswitch.com/contact
415.513.1500

Clearwater Core

(Click for Online Version)

www.metaswitch.com/resources/clearwater-core-ims-in-the-cloud-datasheet

ETSI NFV ISG: Y

Sub-Category: Video / Media / Messaging

Description: vIMS Core

Uniqueness: Clearwater was the first vIMS implementation designed specifically for the cloud and features technological breakthroughs to enable unmatched scalability and resiliency in highly distributed compute environments.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V, Xen	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (CentOS, Fedora, RHEL, Ubuntu, Wind River Linux)	
Management Framework	
Clearwater has been onboarded in numerous NFV infrastructures using various orchestrators and VNF managers. Metaswitch does not mandate a specific VNFM.	
Scalability and Performance	
Clearwater components can be elastically scaled-up, independently, to meet any signaling demands.	

Ecosystem Partners
Hewlett Packard Enterprise, IBM, Intel, Red Hat & VMware
Use Cases Supported
Virtual IMS (vIMS), Virtual Mobile Core (vEPC), VoLTE,
Customer Use Case #1: Mobile
Clearwater Core is a complete cloud-based, NFV-proven, IMS Core implementation; supporting standards based IR.92 VoLTE, IR.94 Conversational Video over LTE, IR.51 IMS over Wi-Fi and Rich Communications Suite (RCS) services.
Customer Use Case #2: Fixed Line
Customer Use Case #3: OTT

Perimeta

(Click for Online Version)

www.metaswitch.com/perimeta

Sub-Category: Security (NAT, SBC, Policy, Identity and DPI Solutions)

Description: Session Border Controller

Uniqueness: Featuring optional integrated real-time analytics, Perimeta was the first and according to external testing is the most resilient session border controller in the market.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V, Xen	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (CentOS, Fedora, RHEL, Ubuntu, Wind River Linux)	
Management Framework	
Perimeta has been onboarded in numerous NFV infrastructures using various orchestrators and VNF managers. Metaswitch does not mandate a specific VNFM	
Use Cases Supported	
Virtual IMS (vIMS), Virtual Mobile Core (vEPC), Virtual Edge (vCPE, vCE, SD-WAN), VoLTE,	

Customer Use Case #1: Security
SIP-based communications, and by default Port 5060, are increasingly becoming a target of mainstream attacks. With the advent of more advanced and sophisticated hacking techniques, coupled with the increase in VoIP traffic, ensuring the security of VoIP networks is emerging as a looming concern for Service Providers worldwide. This concern is intensified if the communications network is deployed in a virtual environment, as the security complexity is only further increased. Fortify your multimedia communications edge and protect your core with the Metaswitch Perimeta SBC.
Customer Use Case #2: Interworking

FEATURED

category: ■ VNF

SONUS NETWORKS

4 Technology Park Dr.
Westford, MA 01886
United States
www.sonus.net
855.GO.SONUS

Virtualized SBC (SWe)

(Click for Online Version)

www.sonus.net/products/session-border-controllers/virtualized-sbc-swe

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Security (NAT, SBC, Policy, Identity and DPI Solutions)

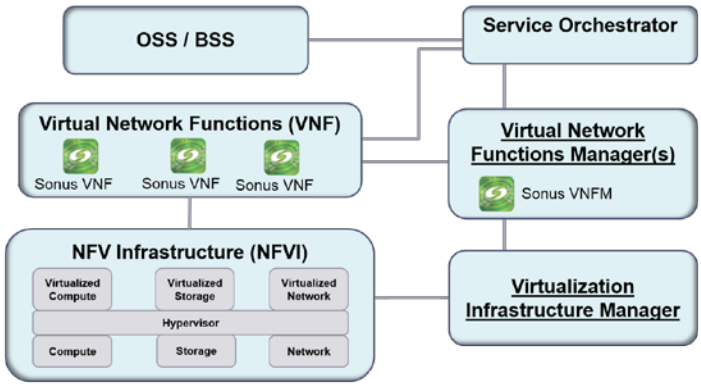
Description: User-defined real-time scalability and proven performance have merged to create Sonus' first virtualized Session Border Controller (SBC). The Sonus SBC SWe uses identical software to Sonus' award winning SBC 5000 Series. The only difference is the box – there isn't one. The SBC SWe is the industry's only software-based SBC architected to deliver unmatched scalability with the same advanced functionality of hardware on a virtualized platform.

Uniqueness: Designed to be simple but robust, and agile but predictable, the Sonus SBC SWe makes it very easy and affordable for customers to reach new markets and new revenues with secure SIP and Unified Communications (UC) services. The Sonus SBC SWe:

- Delivers hosted SBC services in a virtual environment for scalable performance based on simple network-wide licensing
- Seamlessly fits into the migration to a Cloud-services delivery model
- Designed to evolve into a microservices architecture

Supported Hypervisors	Supported OS
ESXi, KVM, Hyper-V	Linux (Debian v6 Linux with the SBC VNF)
Supported CMP	
OpenStack, VMware vRealize/vCAC/vCD, OpenStack, VMware vRealize/vCAC/vCD, AWS	
Management Framework	
The Sonus SBC VNF can be scaled and managed using many ETSI compliant 3rd party MANO solutions. Optionally, Sonus provides a VNFM for SBC VNF scaling and management.	
Supported HW Acceleration	
The Sonus solution has an accelerated data plane powered by DPDK. The product also can take advantage of VMware Direct I/O and SR-IOV. No specialized NICs are required.	
Scalability and Performance	
A single SBC SWe instance is scalable from 25 to 10s of thousands of sessions. Capacity can be elastically scaled up or down using network-wide licensing.	
Ecosystem Partners	
More information can be found at www.sonus.net/products/sonus-product-interoperability-testing/sbc-swe-nfv-orchestration-interoperability-testing	
Use Cases Supported	
Virtual IMS (vIMS), Virtual Edge (vCPE, vCE, SD-WAN), VoLTE, SIP Peering, SIP Trunking for Contact Centers, SBC-as-a-Service	

Customer Use Case #1: SBC as a Service
Service providers can now deliver 'SBC as a Service' to enterprise customers by leveraging their virtualization and cloud infrastructure. SBCaaS is a more efficient business model that eliminates the need to install, deploy and maintain SBCs at the customer premise. SBCaaS makes it far easier to serve enterprises that have seasonal business or high variability in traffic and enables a pay-as-you-grow revenue model. Instead of buying and managing their own SBCs, enterprises benefit by eliminating capital expenses, the need to carry and manage spare physical inventory, having to deal with equipment space, power, installation and configuration issues, and CPE obsolescence. More information can be found at www.sonus.net/solutions/cloud-and-virtualization-solutions/virtual-cpe-vcpe



2953 Bunker Hill Lane, Suite 210
Santa Clara, CA 95054
www.versa-networks.com
408.385.7660

Versa VNF Solution

(Click for Online Version)

www.versa-networks.com/products

OPNFV: N **ETSI NFV ISG:** Y

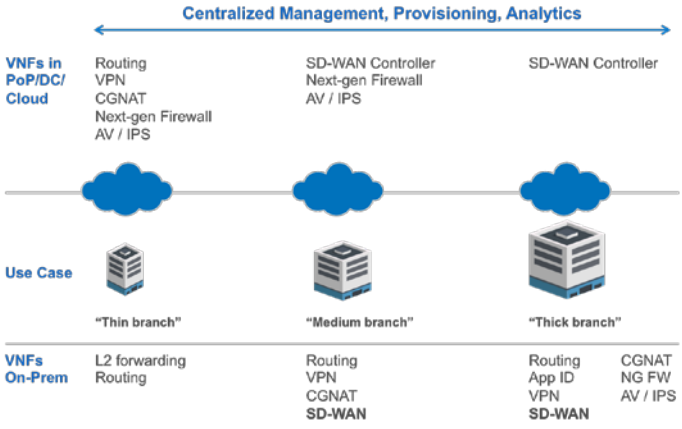
Sub-Category: vRouters, Security, Network Services, SD-WAN, vCPE

Description: Versa FlexVNF is the Versa Networks platform that simplifies the creation, automation and delivery of network services, along with Versa Director and management and Analytics for big data analysis. Together they provide a highly flexible, scalable and carrier-grade software solution to deliver VNF-based network and security services for a variety of use cases, including software-defined WAN (SD-WAN), software-defined security (SD-Security), and virtual CPE (vCPE).

Uniqueness: Versa FlexVNF + Director + Analytics provides a unique carrier-grade and system-level solution, including the following unique capabilities:

1. Complete multi-tenancy – VNFs + controller at head-end, VNFs at branch (for multi-tenant buildings), Director management and Analytics big data platforms
2. Elasticity – Versa VNFs can be dynamically scaled up or down in capacity via Versa Director w/o truck rolls or hardware replacement
3. Complete service chaining – greatly simplify the integration of multiple services (both Versa and 3rd party) with automated service chaining
4. Broadest set of networking and security VNFs – from carrier-grade BGP routing to CGNAT to SD-WAN to next-gen firewall/AV/IPS/secure web gateway – all service-chained
5. Big data analytics – Versa Analytics provide a real-time analytics engine for control, visibility, prediction and a feedback loop for adaptability
6. Wide set of deployment options – bare metal, VMs, containers
7. True zero-touch provisioning

Supported Hypervisors	Supported OS
ESXi, KVM	Linux (Ubuntu 14.04)
Supported CMP	
OpenStack, VMware vRealize/vCAC/vCD	
Management Framework	
Versa Director is a comprehensive VNFM, and manages all aspects of FlexVNF.	
Supported HW Acceleration	
DPDK, SR-IOV, AES NI, Cave Creek/Coleto Creek	



Use Cases Supported
Virtual Edge (vCPE, vCE, SD-WAN)
Customer Use Case #1: SD-WAN (both managed service and enterprise DIY)
The Versa SD-WAN solution enables service providers and large companies to re-architect enterprise WANs and branch office networks through a carrier-grade and software-based approach to SD-WAN – leveraging commodity appliances vs. proprietary network hardware, and better enabling network and security functions to seamlessly interoperate.
Customer Use Case #2: SD-Security (both managed service and enterprise DIY)
The Versa SD-Security solution provides a broad set of software-based security VNFs, including stateful and next-generation firewalls, malware protection, URL and content filtering, IPS and anti-virus, DDoS and VPN/ next-generation VPN. Versa SD-Security maximizes cost efficiency by using commodity appliances vs. proprietary hardware, and simplifies operations through zero-touch provisioning and automatic service chaining.

A10 Networks Thunder ADC

(Click for online version)

www.a10networks.com/sites/default/files/A10-DS-15100-EN.pdf

A10 NETWORKS

www.a10networks.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Acceleration, Security. The vThunder ADC provides advanced L4-7 ADC services (including security) and server load balancing (SLB) and vThunder CGN provides IPv4 scaling with carrier grade NAT (CGNAT) and IPv6 migration capabilities.

Description: Thunder ADC is A10's premier ADC product line, delivering performance scalability up to 150 Gbps, the broadest range of form factors (physical, virtual and hybrid), and expanded system resources designed to support future feature needs.

Uniqueness: A10 Thunder ADC product line is built upon A10's Advanced Core Operating System platform, with Symmetric Scalable Multi-Core Processing software architecture that delivers high performance and a range of deployment options for dedicated, hosted or cloud data centers.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V, Xen Hypervisor. Additionally vThunder ADC is available for AWS and Azure.	OpenStack, VMware vRealize/vCAC/vCD, A10 aGalaxy Management System, Microsoft SCVMM
Supported OS	
Not provided	

APG/80 Active Programmable Gateway

(Click for online version)

www.a-bb.net/index.php/products/active-programmable-gateway

ACTIVE BROADBAND NETWORKS

www.a-bb.net

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Packet Core / Gateways

Description: The APG/80 Active Programmable Gateway is the software-based switching element in Active Broadband's Software-Defined Broadband Network Gateway (SD-BNG) platform. A new class of "soft white-box" switch, the APG/80 is Network Function Virtualization (NFV) infrastructure that allows broadband providers to exploit the economies of scale of general-purpose hardware to significantly reduce capital costs.

Uniqueness: The Active Programmable Gateway supports Future Time Hybrid Queuing (FTHQ). FTHQ is a hierarchical based QoS solution that provides policing, shaping, WFQ & WRED down to the application level. FTHQ was developed to specifically address the limitations that are experienced when re-using porting mechanisms that have previously been deployed in ASICs.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux	Not provided

Affirmed Mobile Content Cloud

(Click for online version)

www.affirmednetworks.com/products-solutions

AFFIRMED NETWORKS

www.affirmednetworks.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Packet Core / Gateways

Description: The Affirmed Mobile Content Cloud is a flexible, scalable, carrier-class virtualized software architecture that provides multiple industry leading innovations, including the Affirmed Open Workflow. The Affirmed Mobile Content Cloud operates on the company's AN3000 off-the-shelf platform and on numerous industry-leading computing platforms, such as its partners' blade servers.

Uniqueness: Dynamic capacity scaling: Scale in or out traffic capacity based on traffic demands; geo-independence: Pool network resources centrally and provision dynamically across geographies to reduce under/over capacity in certain regions; clustered architecture: Consolidating the EPC functions into a cluster – virtualized moble cores can shift capaicty by function ie. SAE GW, Gi Lan Services.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD, CloudStack
Supported OS	**Customers**
Linux (Red Hat Enterprise Linux OpenStack)	ATT Domain 2.0 Partner, Telus, Vodafone

category: ■ VNF

Allot Service Gateway Tera

(Click for online version)

www.allot.com/resource-library/allot-service-gateway-tera

ALLOT COMMUNICATIONS LTD

www.allot.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: Security

Description: Allot Service Gateway Tera is a high-performance DPI-based platform built to power the deployment and delivery of digital lifestyle services in fixed, mobile and cloud networks. Providing a unified framework for traffic detection, policy enforcement and service integration across any access network, Allot Service Gateway Tera helps you manage the heaviest traffic loads and ensure that your network keeps pace with the growing demand for services and the complex needs of application delivery.

Uniqueness: Allot's pre-integrated approach to virtualized services is designed to overcome challenges and provide a complete VNF for rapid service delivery. Allot VNFs for virtualized Parental Control, Anti-Malware, URL Filtering, DDoS Mitigation, Traffic Management, and more are engineered with a wealth of capabilities built-in and pre-integrated, so all carriers have to do is deploy an instance of the pre-integrated VNF and that service is ready.

Supported Hypervisors	Supported CMP
KVM	Not specified
Supported OS	**Customers**
Linux	Not provided

ASOCS Virtual Base Station (vBS)

(Click for online version)

www.asocsnetworks.com/Solutions.html

ASOCS NETWORKS

www.asocsnetworks.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: Virtual Base Station

Description: ASOCS's virtual Base Station enables the realization of end-to-end, fully virtualized networks, from core to edge. The virtual Base Station (vBS) solution is designed in accordance with the ETSI NFV framework decouple, and virtualize all software and hardware resources including: The Base Station L1/PHY software, x86 compute and Hardware acceleration (HWA) platform to process real-time, Signal processing type of workloads.

Uniqueness: The ASOCS Virtual Base Station offers a complete RAN virtualization built on an open platform. It allows customers to achieve spectrum efficiency. It transforms traditional base stations to compute-compatible software on COTS platforms. It allows other NFV and VAS applications to be co-located at the same datacenter, which enables next-generation Communication as a Service (Caas) business models. The ASOCS vBS offers unmatched spectrum and energy efficiency solution: all resources are sharable, scalable and economical.

Supported Hypervisors	Supported CMP
KVM	OpenStack
Supported OS	**Customers**
Linux (WInd River Linux)	Not provided

Virtual Service Edge (Click for online version)

www.sdxcentral.com/products/virtual-service-edge

BENU NETWORKS

http://benu.net

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: vRouters, Packet Core / Gateways, Network Services, vCPE

Description: Benu's VSE is a virtual platform for service providers that combines Mobility, Wi-Fi, vCPE and SD-WAN technologies to deliver innovative cloud managed services to residential and enterprise markets. The Benu VSE is available in both high performance silicon and a virtualized COTS infrastructure.

Uniqueness: Benu's VSE is a single platform for operators to create different service slices to enable Carrier Wi-Fi, and virtual CPE managed Home and Business services. The Benu VNFs provide multi-tenant framework to flexibly scale the number of subscribers and services. These virtualized network functions are assembled into a set of Operator service domains that are highly programmable via REST API and support Service Function Chaining (SFC) to integrate value-added service functions on per subscriber bases.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux (RHEL 7, CentOS 7, Fedora 20)	Not provided

Brocade Virtual Traffic Manager

(Click for online version)

www.brocade.com/en/products-services/software-networking/application-delivery-controllers/virtual-traffic-manager.html

BROCADE

www.brocade.com/en.html

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Acceleration

Description: The Brocade Virtual Traffic Manager is a software-based Layer 7 application delivery controller designed to deliver faster, high performance user experience, with more reliable access to public websites and enterprise applications in any virtual or cloud environment, while maximizing the efficiency and capacity of web and application servers. While traditional application delivery controllers have only focused on delivering scalability and reliability for enterprise and Web applications within the data center, Brocade builds on this functionality to deliver accelerated applications from any data center or cloud platform.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V, XenServer 6.1, 6.2, OracleVM for x86 2.1. 2.2, 3.2, 3.3	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (CentOS 6.x, 7.x, Red Hat Enterprise Linus 6.x, 7.x, Ubuntu 12.04, 14.04. Linux x86_64: Kernel 2.6.8 – 3.13 (2.6.22+ for IPv6)), Solaris 10 (x86_64)	

CA Virtual Network Assurance

(Click for online version)

www.ca.com/content/dam/ca/us/files/data-sheet/ca-virtual-network-assurance.pdf

CA TECHNOLOGIES

www.ca.com/us.html

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Service Assurance & Monitoring

Description: CA Virtual Network Assurance is a flexible and scalable solution gateway providing extended visibility into the multi-layered SDN/NFV stack and its physical network relationships for improved orchestration and agility.

Uniqueness: Overlay/underlay correlation; dynamic multi-layer relationship tracking; service chain building block views of network health

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V	OpenStack
Supported OS	**Customers**
Linux (RHEL, CentOS, Ubuntu)	Not provided

Ciena 3938vi Service Virtualization Switch

(Click for online version)

http://media.ciena.com/documents/3938vi_DS.pdf

CIENA

www.ciena.com

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: vSwitches

Description: The 3938vi is a carrier-grade VNF host based on the Service-Aware Operating System (SAOS) used in all of Ciena's packet switches, providing operational efficiency and consistent system attributes. SAOS delivers benefits across all Ethernet access and aggregation applications.

Uniqueness: The 3938vi is a component of Ciena's overall SDN/NFV solution offerings that enables customers, carriers, to more easily deploy and enjoy VNFs. Ciena's 3938vi is a part of the Agility Matrix cloud-based VNF Market and Blue Planet ecosystems which enables customers and carries to deploy on-demand services. Ciena refers to this as VNF-as-a-Service (VaaS). Ciena tests and certifies those vendors that participate in the NFV market place.

Supported Hypervisors	Supported CMP
Proprietary Service-Aware Operating System (SAOS) solutions. However, the 3938vi can incorporate x86 supported apps via its Director functionality (based on OpenStack).	OpenStack. Ciena's Agility Director, which generates on-the-fly licenses for the VNFs and manages their end-to-end lifecycle.
Supported OS	
3938vi is based on the Service-Aware Operating System (SAOS) used in all of Ciena's packet switches.	

Cisco Next-Generation Virtual Intrusion Prevention System (NGIPSv)

(Click for online version)

www.cisco.com/c/en/us/products/collateral/security/firepower-7000-series-appliances/datasheet-c78-733165.html

CISCO SYSTEMS, INC.

www.cisco.com

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Security

Description: Cisco NGIPSv uses industry-leading threat protection of the Cisco FirePOWER next-generation IPS (NGIPS) solution to address the risks posed by virtualization because it is able to inspect traffic between virtual machines. NGIPSv simplifies deployment at remote locations with limited resources.

Uniqueness: The dynamic nature of virtual networks regularly involves changes to the virtual network's topology as well as configuration changes to individual virtualized hosts that can introduce security exposures if implemented incorrectly (on purpose or accidentally). Cisco NGIPSv for VMware will alert you to misconfigurations and violations of policy so they can be addressed; provide threat protection by identifying and blocking any malicious traffic between your virtualized networks and individual VMs; provide visibility to better control and secure your virtualized environment with real-time network, user, and VM discovery.

Supported Hypervisors	Supported CMP
ESXi	VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux (multiple)	Not provided

Cisco Web Security Virtual Appliance (WSAv) and Cisco Email Security Virtual Appliance (ESAv) (Click for online version)

www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/data_sheet_c78-729630.html?cachemode=refresh

www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/data-sheet-c78-729751.html?cachemode=refresh

CISCO SYSTEMS, INC.

www.cisco.com

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Security

Description: The Cisco WSAv and ESAv significantly lower the cost of deploying web and email security, especially in highly distributed networks, by letting administrators create security instances where and when they are needed. They enable simpler, faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs.

Uniqueness: Talos Security Intelligence: 24/7 view of global traffic to analyze anomalies, uncover new threats, and monitor traffic trends. Prevents zero-hour attacks, continually creating new rule updates for the WSAv and ESAv every 3 to 5 minutes, hours or even days before competitors.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (Red Hat Enterprise Linux; Ubuntu LTS (KVM/OpenStack only for Web Security))	

PowerMedia XMS (Click for online version)

www.dialogic.com/~/media/products/docs/media-server-software/12888-powermedia-xms-ds.pdf

DIALOGIC

www.dialogic.com

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Video / Media / Messaging

Description: PowerMedia XMS is a virtualized, NFV-ready media server, Media Resource Function, and Multipoint Control Unit that supports real-time media applications like video conferencing, RCS and WebRTC. Highlights include: COTS and virtual machine support, Public/Private cloud deployable, Production-ready App Server interfaces with optional developer APIs, Standards compliant, fully functional IMS MRF.

Uniqueness: PowerMedia XMS is 100% software and can be deployed on bare metal, virtualized, or in the Cloud to supports massive scalability. It provides industry standard application interfaces for the creation of several types of applications.

Supported Hypervisors	Supported CMP
ESXi, KVM, Oracle VM, XEN	OpenStack
Supported OS	**Customers**
Linux (RedHat Enterprise Linux, CentOS, Oracle Enterprise Linux)	www.dialogic.com/en/products/media-server-software/xms.aspx

Ericsson Virtual Evolved Packet Core

(Click for online version)

www.ericsson.com/ourportfolio/telecom-operators/virtual-evolved-packet-core

ERICSSON

www.ericsson.com/us

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Packet Core / Gateways

Description: 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.

Uniqueness: Ericsson's virtual EPC includes all the benefits of NFV and it also offers a complete solution, meaning virtualization of all EPC components. Ericsson provides full feature compatibility with native EPC and are compatible with surrounding systems from devices and RAN to charging systems and services. With a common O&M solution and smooth evolution paths Ericsson provides unique features across native and virtualized network nodes.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux (WindRiver-5 (for vSGSN-MME))	Public deployments include SoftBank, Digicel, Swisscom, Telstra, and KT.

Ericsson Virtual Router

(Click for online version)

http://archive.ericsson.net/service/internet/picov/get?DocNo=3/28701-FGB1010557&Lang=EN&HighestFree=Y

ERICSSON

www.ericsson.com/us

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: vRouters

Description: Ericsson Virtual Router (EVR) is the industry's first carrier-grade virtual router that delivers agility in service and infrastructure deployment based on a truly modular, high performance and resilient architecture.

Uniqueness: Because of its modular architecture, the Ericsson Virtual Router is capable of seamlessly scaling out beyond the limitations of a single x86 socket or server. It has been designed to deliver industry leading scale and resiliency for critical carrier applications. EVR offers redundancy and scaling that is 20 times higher than its nearest competitor to lead the industry in elasticity. The EVR architecture is based on fully independent control and data planes interconnected with a virtual backplane (cloud fabric). The control plane is made up of one or two virtual Router Processors (vRP), while the data plane is composed of one to twenty virtual Forwarders (vForwarders).

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux	Not provided

F5 Virtual Network Functions (VNFs)

(Click for online version)

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

F5 NETWORKS

https://f5.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Acceleration, Security, Video / Media / Messaging, Network Services

Description: F5 offers a broad portfolio of products and solutions that allow maximum flexibility as you deploy and virtualize your network. F5 VNFs are interoperable with leading management and orchestration systems – providing a complete NFV ecosystem.

Uniqueness: F5 solutions can be deployed on purpose built platforms or as VNFs to enable superior throughput, and accommodates unmatched levels of connection rates and concurrent sessions in the industry. F5 BIG-IP virtual editions (VEs) includes virtual firewall (vFW), virtual Application Delivery Controller (vADC), virtual policy charging enforcement function (vPCEF), and virtual DNS (vDNS). F5 also offers virtual Diameter Routing Agent and virtual Diameter Edge Agent via the F5 Traffix™ Signaling Delivery Controller™ (SDC) for Diameter-based network.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux (Linux is CentOS 6.6)	Telestra

QUANTiX SBC (Session Border Controller) (Click for online version)

www.genband.com/products/session-border-controllers

GENBAND

www.genband.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: Security

Description: GENBAND provides a range of cost effective enterprise SBC solutions designed to meet the technical and business needs of the enterprises of all sizes.

Uniqueness: The Genband e-SBC line of SBC software allows for simplified multi-vendor PBX and SIP interoperability, unique "network Wide Licensing" that results in 50% savings, multi-tenancy, QoS SLA assurance tools, and more.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux	www.genband.com/company/case-studies

HPE VSR1000 Virtual Services Router

(Click for online version)

http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA4-8850ENW&doctype=data%20sheet&doclang=EN_US&searchquery=&cc=us&lc=en

HEWLETT PACKARD ENTERPRISE

www.hpe.com

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: vRouters, Network Services, Firewall, crypto VPN, QoS and MPLS are provided without purchasing additional feature licenses.

Description: The HPE VSR1000 Virtual Services Router Series is a software application, running on a server, which provides functionality similar to that of a physical router: robust routing between networked devices using a number of popular routing protocols.

Uniqueness: The HPE VSR1000 Virtual Services Router Series is focused on the data center. It supports rich data center and SDN features like VXLAN and OpenFlow. It also supports 2:1 Hewlett Packard Enterprise IRF (Intelligent Resilient Fabric) virtualization to provide an advanced HA solution.

Supported Hypervisors	Supported CMP
ESXi, KVM, VMware ESXi hypervisor, including versions 4.1, 5.0, 5.1, and 5.5, and Linux KVM hypervisor (Linux kernel version 2.6.25 or later).	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (CentOS 7, Ubuntu 14.04, Red Hat Enterprise Linux (RHEL) 6.3, and SUSE Linux Enterprise Server 11 SP2).	

Huawei FusionSphere

(Click for online version)

http://e.huawei.com/en/products/cloud-computing-dc/cloud-computing/fusionsphere/fusionsphere

HUAWEI

www.huawei.com/en

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: vSwitches, Service Assurance & Monitoring, Network Services

Description: Huawei's FusionSphere OS integrates the FusionCompute virtualization platform and FusionManager cloud management software. As a result, a wide range of enterprises can horizontally consolidate physical and virtual resources in data centers and vertically optimize the service platform.

Uniqueness: Huawei's FusionSphere is a complete Cloud OS stack and consists of FusionCompute, FusionStorage, and FusionNetwork in addition to FusionManager. The features supported across these VNFs are vast and include VxLAN networking, storage QoS control, SLA QOS control, multi-tenant isolation and stratification, & more.

Supported CMP	
OpenStack	
Supported Hypervisors	**Supported OS**
Huawei UVP Virtualization Hypervisor. Huawei also claims to support 'third party' hypervisors with FusionManager.	Linux (FusionSphere is Huawei's own Cloud OS), Windows (Huawei supports multiple version of Windows as a guest operating system (OS))

SDN Adaptive

(Click for online version)

http://kemptechnologies.com/sdn-adaptive-load-balancing

KEMP TECHNOLOGIES

http://kemptechnologies.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Network Services

Description: SDN Adaptive is a feature that enables the LoadMaster product to monitor the condition of all ports in the SDN switch infrastructure and based on congestion conditions, steer flows down alternative paths to servers that are not under the same conditions.

Uniqueness: In traditional IP networks, applications don't always get the best performance possible because end-to-end visibility of traffic flows and patterns usually don't exist and routes (flows) are not always optimized. In SDN networks the SDN controller has this end-to-end view. KEMP SDN Adaptive takes advantage of this by accessing the information from the SDN Controller allowing flows from applications to be routed dynamically in the most optimized manner.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V, Virtual Box, XEN	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux (Custom)	Not Provided

Evolved Packet Core (EPC)

(Click for online version)

www.mitel.com/evolved-packet-core

MITEL

www.mitel.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: Packet Core / Gateways

Description: Mitel's Virtualized Evolved Packet Core (EPC) is a software-based, carrier grade solution that can be deployed on cloud-based infrastructures using Network Functions Virtualization (NFV) to rapidly scale capacity and adapt to new deployment models.

Uniqueness: Mitel's EPC has been deployed widely as globally operators transform towards 4G LTE networks. Current EPC deployments are primarily targeted towards initial 4G LTE devices geared for mobile internet traffic. With its proven leadership in VoLTE and RCS, Mitel brings in a unique perspective of utilizing EPC for telecom communication driven services such as user-to-user voice, video, messaging, content sharing etc.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD, HPE Helion and HPE NFV Director
Supported OS	**Customers**
Linux (Mitel Standard Linux)	www.mitel.com/insights?body_value=&field_article_type_tid[]=55

OS-V Series - 10GbE CPE/Demarcation

(Click for online version)

www.mrv.com/products/os-v

MRV COMMUNICATIONS

www.mrv.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: vSwitches

Description: The OS-V Series, a portfolio of MEF CE 2.0-Compliant modular and programmable 1RU 10GbE CPEs, is a new enhancement to the field-proven OptiSwitch product line. The OS-V Series addresses the ongoing market demand for scalable 10GE (and fractional 10GbE) services as well as the requirement for openness, increasing intelligence, programmability, and virtualization in the access network.

Uniqueness: The OS-V Series is available in two form factor variants (OS-V8 and OS-V20) to address the performance, intelligence and flexibility requirements for various applications at the network edge. OS-V is fully integrated into MRV's advanced Pro-Vision service orchestration and management system.

Supported Hypervisors	Supported CMP
Master-OS a proprietary MRV software.	MRV offers Pro-Vision at service orchestration layer that unifies management of both the packet and optical domains.
Supported OS	**Customers**
Linux, Master-OS a proprietary MRV software.	CyC S.A Argentina, PEG Bandwidth, FiberLight

Virtualized Customer Premises Equipment (Click for online version)

www.sdxcentral.com/products/virtualized-customer-premises-equipment-vcpe

NEC/NETCRACKER

www.nec.com
www.netcracker.com
OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Network Services

Description: The NEC/Netcracker vCPE solution is built on the concept of moving IP functions and hardware-centric value-added service features out of the enterprise or residential customer premises equipment into the service provider's point of presence (PoP) or data center. With this shift in architecture, IP functions and services are run as VMs on top of commercial-off-the-shelf (COTS) hardware.

Uniqueness: SDN-enabled vCPE through integration with NEC's ProgrammableFlow suite of SDN controllers, a proven, first-to-market solution with more than 200 commercial deployments. By leveraging ProgrammableFlow, service providers can support dynamic service chaining and virtualize CPE environments with optimized network control and performance.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (Red Hat Enterprise Linux 7.x)	

Virtualized Evolved Packet Core

(Click for online version)

www.sdxcentral.com/products/virtualized-evolved-packet-core-vepc

NEC/NETCRACKER

www.nec.com
www.netcracker.com
OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Packet Core / Gateways

Description: NEC/Netcracker provide one of the first publicly deployed virtualized Evolved Packet Core (vEPC) solutions, which supports the 3GPP release 11 standards and provides the following virtual network functions: Service GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Mobility Management Entity (MME), Serving GW (S-GW), PDN GW (P-GW), Home Subscriber Server (HSS) and Policy and Charging Rules Function (PCRF).

Uniqueness: The unique design principle underlying the vEPC system is an intelligent function decomposition that enables agile and elastic system scaling. At the management and provisioning level, vEPC defines logical system units that can be independently managed, deployed and scaled. At the functionality level, the decomposition separates the control plane functionalities from the data plane functionalities.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (Red Hat Enterprise Linux 6.x/7.x)	

Lithium SMS Platform (Click for online version)

www.newnet.com/wp-content/uploads/2014/04/Lithium-SMS-Product-Brief.pdf

NEWNET COMMUNICATIONS TECHNOLOGIES

http://newnet.com
OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Video / Media / Messaging, SMS software platform including router, gateway, and firewall services.

Description: Lithium is a modular SMS software platform for mobile operators, carriers and enterprises. Lithium is designed to efficiently replace end-of-life SMSCs or application gateways.

Uniqueness: Existing Short Message Service Centers (SMSCs) have not kept up with the technology curve in terms of the cost of the equipment, performance and operating efficiency. They lack message-handling flexibility and do not support advanced features such as First Delivery Attempt (FDA), real-time pre-paid charging, SPAM control and real-time service monitoring; which would help operators significantly improve the efficiency and performance of their networks.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD, CloudStack
Supported OS	**Customers**
Linux (RHEL 6.0), Solaris	Not provided

Mercury MMS Solution

(Click for online version)

http://newnetmobility.com/resources/data-sheet

NEWNET COMMUNICATIONS TECHNOLOGIES

http://newnet.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Video / Media / Messaging, MMSC

Description: NewNet's Mercury MMS Solution enables content and service providers (CSPs) to deliver rich multimedia content to all subscribers, quickly and easily.

Uniqueness: The Mercury MMS platform features the broadest range of features that include a robust MMSC with features such as routing delivery queues, message storage, MM1 notifications, retrieval request responses, billing and reporting for A2P and P2P MMS solutions. The WAP Gateway converts messages to HTTP, compresses ML text, compiles plain text WMLS to byte code format, and provides WAP push capabilities. The composer & campaign manager is a web-based interface for advertisers and the operator to create, schedule and monitor MMS campaigns. The Mercury transcoder can resize, re-encode, reformat, shift aspect ratio and convert from video to animation over a variety of content formats to optimize the MMS subscriber experience.

Supported Hypervisors	Supported CMP
ESXi	OpenStack
Supported OS	**Customers**
Linux (RHEL 6.0)	Not Provided

NFWare Virtual Carrier Grade NAT

(Click for online version)

www.nfware.com/products/carrier-grade-nat

NFWARE

www.nfware.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: vRouters, Packet Core / Gateways, Security

Description: NFWare Carrier Grade NAT (or Large Scale NAT) is an NFV-based virtual appliance designed to provide high-performance transparent address and protocol translation. Virtual CG-NAT allows service providers to extend IPv4 network connectivity and offers a variety of options for a smooth transition to IPv6.

Uniqueness: NFWare vCG-NAT is a high performance multi-vendor solution which provides one of the highest throughputs and can be run on any HW, infrastructure and managed by 3rd party orchestration and management systems using standard interfaces.

Supported Hypervisors	Supported CMP
KVM	OpenStack
Supported OS	**Customers**
Linux (RHEL, Ubuntu, CentOS)	Not provided

Virtualized Service Router (VSR)

(Click for online version)

http://resources.alcatel-lucent.com/?cid=182483

NOKIA

https://networks.nokia.com

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Not provided

Description: The Nokia Virtualized Service Router (VSR) [formerly by Alcatel-Lucent] is a virtualized IP/MPLS router offering extensive suite of applications for telco cloud environments to allow flexible growth of networks to support the growth of mobile, residential, enterprise and wholesale services.

Uniqueness: High-performance; independent scaling of the control plane and data plane; advanced architecture and packet processing and acceleration techniques; symmetric multi-processing (SMP) to maximize the power and performance of multi-core processing; 64-bit OS to address larger CPU core memory space; high control plane resiliency through stateful active/standby VM protection; high availability, non-stop routing and services, and in-service software upgrades; flexible management options – from working with open frameworks to delivering OpenStack-integrated VNF management and element management capabilities with Nokia 5620 Service Aware Manager (SAM).

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, CloudBand
Supported OS	**Customers**
Linux (CentOS, RHEL, Ubuntu (future))	Telefonica

N2 Platform (Click for online version)

http://nominum.com/wp-content/uploads/2015/09/Nominum-Product-Brief-N2-Engage.pdf

NOMINUM INC.

http://nominum.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Security. N2 Platform also provides solutions for DNS to enable services, policy and data gathering.

Description: N2 Engage is an innovative application purpose-built for service providers to deliver cloud-based services to subscribers. With N2 Engage, service providers enable subscribers to manage Internet access and content for their household, protect subscribers from malware-related Internet threats and comply with government mandates & regulations regarding Internet content.

Uniqueness: N2 Engage is a comprehensive 1-to-1 service delivery platform that allows subscribers to set policies restricting and/or allowing Internet access and content and assists providers in identifying and communicating with subscribers regarding Internet-based security threats. N2 Engage is also deployed to support service provider's efforts to comply with government mandates regarding Internet content. N2 enables subscriber facing services leveraging in place DNS assets. The unique control plane based approach minimizes impact on the network.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux	Not Provided

Vantio CacheServe 7 (Click for online version)

http://nominum.com/wp-content/uploads/2015/06/Vantio-CacheServe7-DataSheet.pdf

NOMINUM INC.

http://nominum.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Network Services, DNS Resolver with advanced policy framework

Description: Future ready DNS. Highest performing, fastest caching DNS servers with the most threat adaptivity and lowest TCO. Six times faster than open source, i.e. BIND, with 40% lower TCO.

Uniqueness: Industry-best algorithms developed by the leading DNS engineering team set the standard for recursive performance. DNS cache poisoning defenses remain the most effective in the industry. Lowest latency and 100% availability promote subscriber satisfaction and retention. CacheServe "client subnet" feature provides query details to authoritative servers resulting in better geo-targeting of subscribers and more cost effective content delivery. Resilience to extreme traffic spikes means CacheServe answers queries when other caching software, load balancers and switches fail. This prevents outages or slowdowns that stress operations teams and provoke costly subscriber support calls. CacheServe Precision Policies adapt as DNS DDoS attacks evolve, safeguarding vital DNS resources, and eliminating damage from malicious traffic. Fine-grained filtering (IP, domain, Query Type and more) or rate limiting of queries coupled with truncated responses protect legitimate DNS queries.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux (RHEL 6.5, CentOS 6.5)	Not provided

ONEv600

(Click for online version)

www.sdxcentral.com/products/onev600_52129773

ONEACCESS NETWORKS

www.oneaccess-net.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: vRouters

Description: Application-Aware, Secure Routing & Switching VNF. The ONEv600 VNF enables the creation of value-added hybrid WAN services between enterprise branches and data centers. The ONEv600 technology provides SMB and enterprise customers with an extensive range of carrier-grade switching and routing functions and enables service providers and large network providers to deploy within an NFV environment today. The core OneOS management plane delivers state-of-the-art APIs for efficient programming and operations of service provider's managed services.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux (Yocto, Debian, CentOS)	Not provided

ONEvSBC (Click for online version)

www.sdxcentral.com/products/onevsbc

ONEACCESS NETWORKS

www.oneaccess-net.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Security

Description: ONEvSBC has two main modes of operation, providing service assurance, network optimization, and security for a variety of SIP based services: The transparent mode forwards and authenticates SIP phone signaling to the service provider's network, thus preserving value-added communication services.

Uniqueness: ONEvSBC (OneAccess virtual eSBC) differentiation points are: Its architecture is such that no or minimal adaptations are required to interoperate with 3rd party PBX, thus reducing the time and effort associated with interoperability; turnkey, customizable management solutions enable service providers to personalize the (zero-touch) deployment models and offer self-service operations for end-users or installers; the small virtual machine footprint reduces the virtualization capex and opex.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux (Yocto, Debian, CentOS)	Not Provided

Openwave Mobility Integra

(Click for online version)

http://owmobility.com/uploads/white_papers_datasheets/Integra_Feb18_%283%29.pdf

OPENWAVE MOBILITY INC

http://owmobility.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: Security

Description: Integra provides single-point service orchestration / service chaining and a dynamic policy enforcement point which can be expanded into the ALL-IP traffic flows.

Uniqueness: At the heart of Integra lies a plug-in Layer 4-7 orchestration layer, providing dynamic triggering of Layer 7 services with attributes from the flow, profile, authentication and web service combined into a single intelligent switching capability. This capability is provided with low latency and best in class capacity numbers in throughput for signaling and data plane traffic per blade. Integra also delivers on network function virtualization both from the perspective of virtual network function components (VNFC) and service orchestration, dynamic function chaining and elastic deployment.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD, CloudStack
Supported OS	**Customers**
Linux (RedHat version 6.4 and version 7)	Not provided

Oracle Enterprise Session Border Controller (E-SBC) (Click for online version)

www.oracle.com/us/industries/communications/enterprise-session-director-ds-1985037.pdf

ORACLE

www.oracle.com/index.html

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Security

Description: Oracle Enterprise Session Border Controller securely connects Enterprise VoIP and UC systems to SIP Trunking and Wide Area Network Services while mitigating security threats, curing interoperability problems and ensuring reliability.

Uniqueness: Industry leading SBC with deployments in the majority of Communications Service Providers and Enterprises

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	
Linux (Solaris, Linux x86 -o Oracle Linux on x86 (64-bit), Linux 5 update 8 or higher (such as Linux 5.8, 5.9, or 5.10), Linux 6 update 2 or higher (such as Linux 6.2, 6.3, or 6.4), Red Hat Enterprise Linux on x86 (64-bit), Linux 5 update 8 or higher (such as Linux 5.8, 5.9, or 5.10), Linux 6 update 2 or higher (such as Linux 6.2, 6.3, or 6.4))	

PLUMgrid OpenStack Networking Suite

(Click for online version)

www.plumgrid.com/wp-content/uploads/documents/PLUMgrid_ONS_For_OpenStack.pdf

PLUMGRID

www.plumgrid.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: vRouters, vSwitches, Security, Network Services. Additionally developers can extend or create new VNFs using the SDK.

Description: The PLUMgrid OpenStack Networking Suite (ONS) is a secure, comprehensive and open software-only solution that delivers terabits of performance and scales across tens of thousands of workloads. Built on PLUMgrid Platform and IO Visor technology, it provides highly automated workflows that significantly reduce the deployment time of OpenStack clouds and enables users to create private Virtual Domains for applications and projects.

Uniqueness: PLUMgrid ONS is a comprehensive suite of virtual network services that is designed with a programmable, distributed architecture providing secure multi- tenancy, scale-out performance, production-grade resiliency, and automation for a wide range of use cases for financial, retail, healthcare, public sector, and telecom. PLUMgrid ONS provides a rich portfolio of virtual network functions.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux (Canonical, Mirantis, Oracle, Rackspace, Red Hat, and SUSE)	www.plumgrid.com/resources/testimonials

Procera PacketLogic/V (Click for online version)

www.proceranetworks.com/products/platforms/plv

PROCERA

www.proceranetworks.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: Security, Service Assurance & Monitoring

Description: The PacketLogic platforms are the vehicle for delivering an enhanced subscriber experience to broadband subscribers. These systems are empowered by the PacketLogic software suite and are designed to enable network operators to gain insights and take action on broadband traffic to enhance the subscriber experience. PacketLogic/V platforms enable flexible deployments of PacketLogic software using industry-standard, off-the-shelf hardware and software virtual machine environments.

Uniqueness: Flexible network deployment supporting full migration capabilities to add services wherever needed without pre-installation of PacketLogic-specific hardware platforms. Analytics and enforcement capabilities sized for your needs with easy upgrades from 1Mbps to over 155Gbps of network traffic throughput in a single instance. Multiple solutions can be deployed, delivering the features required for specific services. Designed for tight integration with partner NFV products based on the ETSI NFV architectural framework and ONF SDN standard.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD, CloudStack
Supported OS	**Customers**
PacketLogic OS	Boingo Wireless is the current publicly named customer.

DPI as a Virtual Network Function Component (VNFC) (Click for online version)

http://www.qosmos.com/wp-content/uploads/2015/11/Qosmos_DPI_VNFC_Datasheet_Nov2015.pdf

QOSMOS

www.qosmos.com

OPNFV: **ETSI NFV ISG:**

Description: Qosmos DPI as a Virtual Network Function Component (VNFC) complies with an official use case standardized by ETSI in July 2013. This new Qosmos product runs in a virtual machine and uses optimized interface to feed application information and metadata to other integrated components, together forming virtual networking equipment (VNFs) such as Service Routers, GGSN, PCEF, BRAS, ADC/Load Balancers, Network Analytics, NG Firewalls, WAN optimization, etc.

Supported Hypervisors	Supported CMP
Not provided	Not provided
Supported OS	**Customers**
Not provided	Not provided

Saisei FlowCommand (Click for online version)

http://saisei.com/wp-content/uploads/Saisei-Datasheet-Product-Overview.pdf

SAISEI

http://saisei.com

OPNFV: N **ETSI NFV ISG:** Y

Sub-Category: Security, Service Assurance & Monitoring, Network Performance Enforcement (NPE)

Description: FlowCommand has added security and control features designed specifically for service providers and for the largest of distributed enterprise customers.

Uniqueness: 1) Completely monitors and controls every flow and microflow on up to 10G links applying policy to individual flows or groups of flows based on 40+ L2-L7 metrics, including user, application, geo-location and more, 2) Expands bandwidth utilization on IP links to over 95% while guaranteeing that no user session will ever time out even at 95% rate. 3) Eliminates any need for queuing, allowing QoS mechanisms in routers and network equipment to be turned off. 4) Enforces fair usage/net neutrality on all users regardless of application at the click of a button.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux (Ubuntu 14.04)	Not Provided

Diameter Signaling Controller (DSC SWe) (Click for online version)

www.sonus.net/sites/default/files/DS_SonusDSC.pdf

SONUS NETWORKS

www.sonus.net

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Integrated Diameter Signaling Controller and SS7 Signaling Transfer Point

Description: The DSC SWe is a virtual, integrated solution for Diameter Signaling Control (DSC) as well as an SS7 Signaling Transfer Point. The IP-centric design of the DSC SWe facilitates its integration into service provider networks without the use of external IP switching equipment. The incorporation of internal Ethernet switching provides a high capacity IP backplane and is also the basis for the most efficient, network-friendly SIGTRAN implementation available.

Uniqueness: The Sonus DSC SWe is the only solution on the market to offer a combined STP and Diameter router in a single VM. The DSC SWe provides an internal virtual routing node separate forwarding tables and accounting counters which enables scalability and makes it perfectly suited for mobile operators and IPX providers who interconnect to multiple other networks. Multiple DSC instances for both STP and Diameter routing functionality can be managed from a single operations point.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux (Red Hat v7)	Not provided

PSX SWe (Click for online version)

www.sonus.net/sites/default/files/data_sheet_psx_swe_30_september_2014.pdf

SONUS NETWORKS

www.sonus.net

OPNFV: Y **ETSI NFV ISG:** Y

Sub-Category: Security

Description: Sonus' PSX is the a feature-rich policy and routing control platform, delivering reliability in the world's most demanding environments. The PSX SWe provides least cost and QoS routing, centralized policy control, integrated number portability, and centralized dial plan management for both SIP and legacy network elements, including session border controllers, media gateways, and softswitches. The PSX SWe is also deployable as part of a virtual, multi-vendor IMS infrastructure performing the Breakout Gateway Control Function (BGCF).

Uniqueness: The Sonus PSX SWe has the following unique differentiators: Centralized routing and policy Engine; vendor agnostic; highly scalable and high performance master-replica architecture; carrier-grade five 9s reliability; built-in Least Cost Routing functionality; integrated number portability; migrates seamlessly to an IMS Breakout Gateway Control Functions (BGCF)

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack
Supported OS	**Customers**
Linux (Red Hat Enterprise Linux v6.4)	Not provided

NFV CyberGuard (Click for online version)

www.telco.com/index.php?page=download&file=A149&-ref=219&src=NFV+CyberGuard+Solution&filename=NFV-CyberGuard-Solution_A4.pdf&filetype=Solutions+Overview

TELCO SYSTEMS

www.telco.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Security

Description: Virtualized cybersecurity solution to protect against inherent SDN and NFV vulnerabilities. Four steps to cybersecurity – the NFV CyberGuard solution leverages sophisticated algorithms, probes and big-data analytics to protect NFV and SDN networks from threats, in a continuous four-stage process.

Uniqueness: 1) NFV CyberGuard is the one of the only cyber-security solution designed specifically to protect SDN and NFV networks. 2) NFV CyberGuard is deployed as a NFV at network edge at the closest point to all endpoints providing real-time monitoring and analysis of network threats, complete visibility of the entire network and the ability to apply cyber-security policies and efforts to the entire infrastructure. 3) NFV CyberGuard includes an open API for integration of external systems and third-partly applications and algorithms.

Supported Hypervisors	Supported CMP
KVM	OpenStack
Supported OS	**Customers**
Linux (Ubuntu and Fedora)	Not Provided

Vantrix Bandwidth Optimizer

(Click for online version)

http://info.vantrix.com/hs-fs/hub/452806/file-2558006220-pdf/Vantrix-Bandwidth-Optimization-Overview-0215.pdf

VANTRIX

http://vantrix.com/home

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Video / Media / Messaging

Description: Control your mobile bandwidth with smart, precise media optimization from Vantrix. The massive growth in mobile video presents challenges and opportunities for mobile service providers. Vantrix provides the optimization solutions you need to meet QoE goals, drive revenue and reduce infrastructure costs.

Uniqueness: Vantrix provides surgical optimization for policy-driven control of your network resources with Vantrix Bandwidth Optimizer. Vantrix ensures that multimedia messages are delivered efficiently in the right format for any device with Vantrix Message Optimizer. Both solutions are built on a virtualized media processing platform, and can be delivered on turnkey appliances deployed in private or public cloud scenarios.

Supported Hypervisors	Supported CMP
KVM	OpenStack
Supported OS	**Customers**
Linux (CentOS, Redhat)	Not provided

Cloud-Delivered SD-WAN Service

(Click for online version)

www.velocloud.com/documents/VeloCloud_Service_Provider_Overview.pdf

VELOCLOUD NETWORKS

www.velocloud.com

OPNFV: Y **ETSI NFV ISG:** N

Sub-Category: vRouters

Description: VeloCloud Cloud-Delivered SD-WAN incorporates a distributed network of service gateways deployed at top tier cloud datacenters around the world, providing scalability, redundancy and on-demand flexibility.

Uniqueness: VeloCloud Edges perform deep application recognition, application and packet steering, performance metrics and end to end quality of service in addition to hosting virtual network function (VNF) services. VeloCloud Dynamic Multipath Optimization (TM) comprises of automatic link monitoring, auto-detection of provider and auto-configuration of link characteristics, routing and QoS settings.Also, On-demand, Per-packet application steering is performed automatically based on the measured performance metric, intelligent application learning, business priority of the application, and link cost.

Supported Hypervisors	Supported CMP
ESXi, KVM, Hyper-V	OpenStack
Supported OS	**Customers**
Linux (Redhat Enterprise 7.2, Ubuntu 14.0.4)	Deutsche Telekom, Vonage, MetTel, Devcon Construction

TrueSpeed VNF

(Click for online version)

www.viavisolutions.com/sites/default/files/technical-library-items/truespeedvnf-pb-tfs-nse-ae.pdf

VIAVI SOLUTIONS

www.viavisolutions.com/en-us

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: Service Assurance & Monitoring

Description: TrueSpeed VNF provides network operators and enterprise users with a repeatable, standards-based test methodology to resolve complaints about poor network performance faster than ever before.

Uniqueness: TrueSpeed VNF is the first and only RFC 6349 network testing application that offers an unbiased and predictable measurement of performance based on standards of a software only implementation. This allows for greater implementation flexibility and speed.

Supported Hypervisors	Supported CMP
ESXi, KVM	OpenStack, VMware vRealize/vCAC/vCD
Supported OS	**Customers**
Linux (Red Hat Enterprise Linux, CentOS)	Not Provided

category: ■ VNF Service Offerings

Cloud Voice Platform (Click for online version)

www.alianza.com/hubfs/Collateral/Hosted_NFV_VoIP_Solution_Brief_-_Alianza.pdf?t=1457033842534

ALIANZA INC.

www.alianza.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: VNFaaS, Entire VoIP solution - all VNFs integrated into a single solution

Description: Alianza's Cloud Voice Platform is a single-source solution for service providers seeking to quickly and profitably deploy next generation voice services.

Uniqueness: Cloud Voice Platform provides all the elements (servers, VM, SBC, app server, VoIP core, etc.) required to define, deliver and monetize VoIP services. It is turnkey and integrated–meaning service providers are not cobbling together the NFVI, VNF and MANO layers. With our cloud, service providers benefit from a "voice-network-as-a-service" delivered with a SaaS business model. 1) Lower overall cost – eliminates CAPEX and reduces OPEX (up to 50% TCO savings). 2) Simplified operations – integrated VoIP platform means a single interface to manage and troubleshoot voice; this reduces operational costs and accelerates problem resolution. 3) More rapid innovation – features and bug fixes are regularly (1-2 times/month) released. 4) Faster time to revenue – flow-through provisioning, including integration with back-office and 3rd party services, automate business processes and eliminate swivel chair.

Supported Hypervisors	Supported CMP
KVM	OpenStack
Supported OS	**Customers**
Linux (CentOS 7), N/A – as a service-based offering	Blue Ridge Communications, WEHCO Media, SELCO

WAN Optimization as-a-Service

(Click for online version)

http://info.aryaka.com/Cloud-Acceleration.html

ARYAKA NETWORKS

www.aryaka.com

OPNFV: N **ETSI NFV ISG:** N

Sub-Category: VNFaaS

Description: Aryaka's WAN Optimization as-a-Service is a global connectivity and application acceleration service that combines a global private network, WAN Optimization, SD-WAN functionality and 24x7 support to deliver up to 40x faster application performance around the world, and up to 56% cost savings compared to traditional network alternatives like MPLS.

Uniqueness: Global network, multi-cloud access; end-to-end security, application acceleration, visibility and control; availability

Supported Hypervisors	Supported CMP
Container based	Proprietary Stack
Supported OS	**Customers**
Linux (Ubuntu)	www.aryaka.com/proven-success

SDNCentral, LLC
955 Benecia Avenue
Sunnyvale, CA 94085 USA
www.sdxcentral.com

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

Rev B