

2015 Special Report: Network Virtualization in the Data Center



contents

Table of Contents

Introduction	5
The Drivers for Network Virtualization	6
Benefits of Network Virtualization	6
A Look at Who's Adopting Network Virtualization	8
Where Network Virtualization is Being Deployed.	9
Network Virtualization Use Cases.	10
What Organizations are Looking for in NV Solutions.	11
Approaches to Network Virtualization	15
Network Virtualization in the Data Center	15
Network Virtualization as a Service.	16
Network Virtualization for the WAN	17
Market Shifts: Some Key Production Deployments by Market Leaders	17
VMware - NSX	18
Cisco - ACI/Nexus/AVS/Intercloud	19
Juniper Networks - Contrail	21
Nuage Networks - Virtualized Service Platform	22
Vendor Profiles	23

Commercial [featured]

Dell	24
----------------	----

Commercial

Avaya	25
Big Switch Networks	25
Cisco Systems	26
CPLANE NETWORKS	26
Extreme Networks	27
Hewlett Packard Enterprise	27
Juniper Networks, Inc.	28
Midokura	28
NEC	29
Nuage Networks	29
PLUMgrid.	30
Pluribus Networks.	30
VMware, Inc.	31

Open Source

Akanda	32
Metaswitch Networks.	32
OpenDaylight	33
Open vSwitch	33

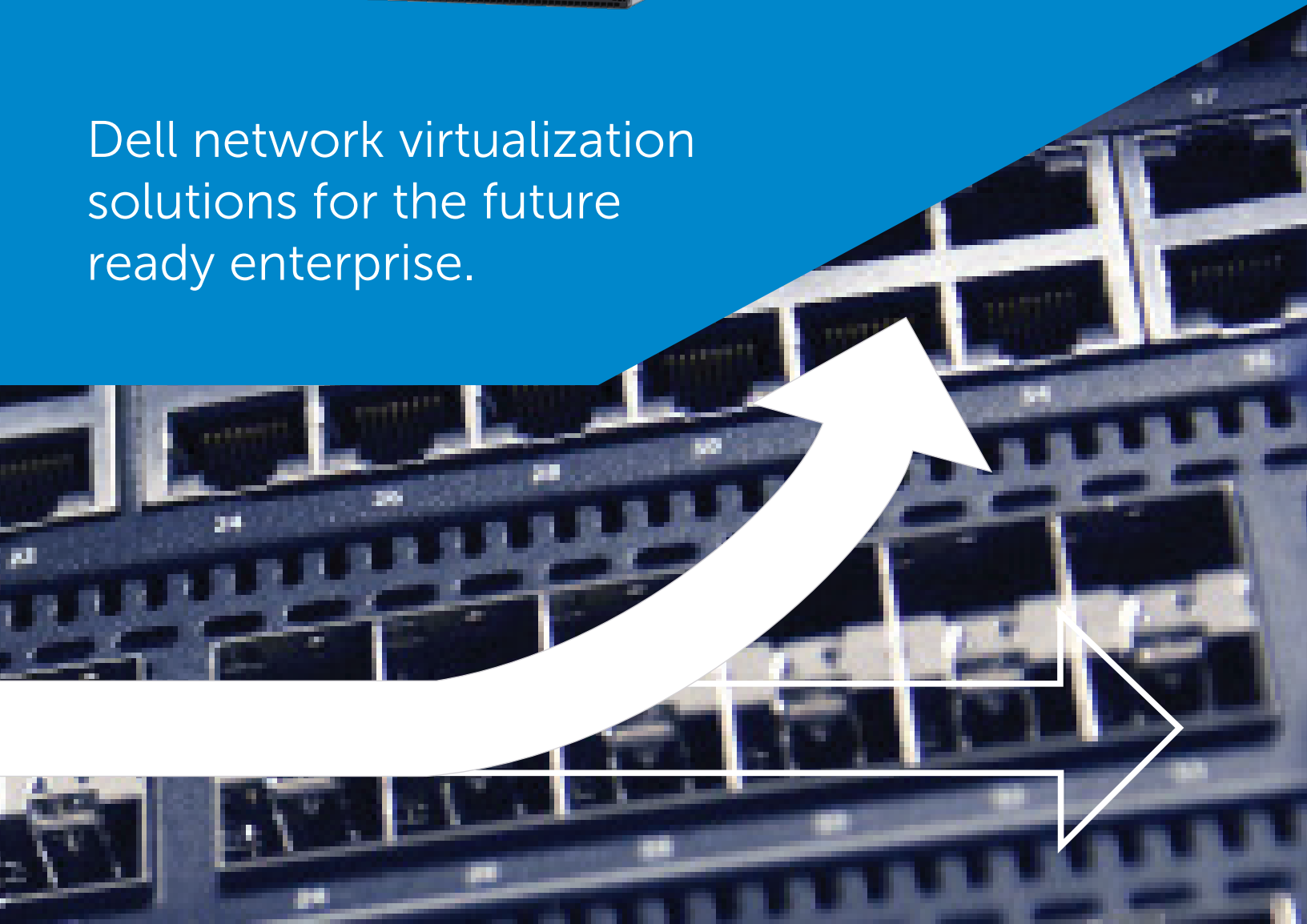
Open networking across the enterprise. Now that's a switch.



Drive innovation with the new
Dell open standard
1-100GbE SDN-ready switches.



Dell network virtualization
solutions for the future
ready enterprise.



Discover VMware NSX

Improve your performance with VMware NSX network and security virtualization

VMware NSX® is the network virtualization and security platform for the software-defined data center. NSX brings virtualization to your existing network and transforms network operations and economics without replacing your hardware!

What NSX Does



Agility

NSX reduces the time it takes to provision custom, multi-tier network topologies and enterprise class security services from weeks to seconds.



Cost

NSX reduces both OPEX and CAPEX. Automation eliminates manual configuration from the network provisioning process and simplifies network hardware requirements.



Choice

The NSX network virtualization platform operates on any hypervisor, any network hardware and integrates with any cloud management platform.



Virtualized Network

Similar to a virtual machine for compute, a virtualized network is a fully functional network in a software container, provisioned independent of underlying hardware or topology.



Distributed Security

NSX delivers a new model for network security. Security profiles are distributed to and enforced by virtual ports and move with VMs.



Scale & Performance

NSX is deployed in production today by several of the largest service providers, global financials and enterprise data centers in the world.

For more information, visit:
www.vmware.com/products/nsx

market summary

Introduction

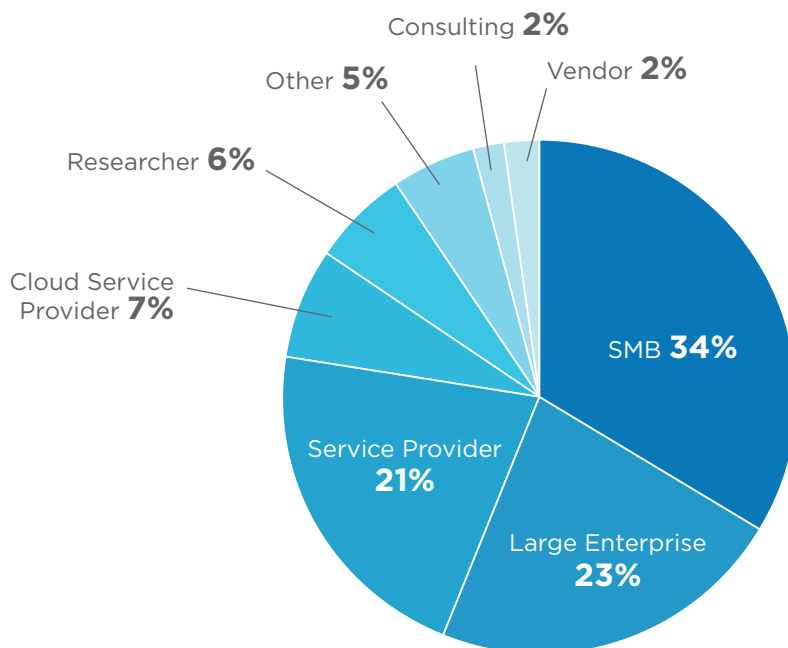
There is no doubt about it, the network is going virtual. Network virtualization (NV) creates a logical virtual network that runs on top of a physical one, making it easy for organizations to roll out, scale and adjust workloads and resources to meet changing needs. Adoption of NV solutions is ramping with organizations large and small, as they strive to improve the flexibility, scalability and overall efficiency of their data center and cloud environments.

While NV may be inevitable, there are still questions around the details – who, what, where, when and why. These are the questions the 2015 Network Virtualization Report aims to answer, or at least provide insights to, based on current market trends. The Report covers:

- What is driving the adoption of NV
- The primary benefits of NV
- Where NV is being deployed
- How NV is being used
- Different approaches vendors are taking to the market
- Key attributes to consider when evaluating NV solutions
- Market trends – announcements and moves by NV leaders
- Vendor profiles

This report will include perspectives from members of the SDxCentral community, with original research¹ from the SDxCentral Research Team on current perceptions and experiences with network virtualization. Results from the SDxCentral Survey on NV are used throughout to provide a snapshot of what is actually happening with NV within organizations.

RESPONDENTS TO SDXCENTRAL NV SURVEY BY TYPE



If you have questions or feedback on the survey, please feel free to contact the research team at research@sdxcentral.com.

¹ SDxCentral conducted a survey on the SDxCentral site, www.sdxcentral.com, in which 107 respondents provided answers to multiple choice and open-ended questions on their experiences with network virtualization. Survey respondents represented a sampling of enterprise and service provider end-users from large and small organizations.

market summary

The Drivers for Network Virtualization

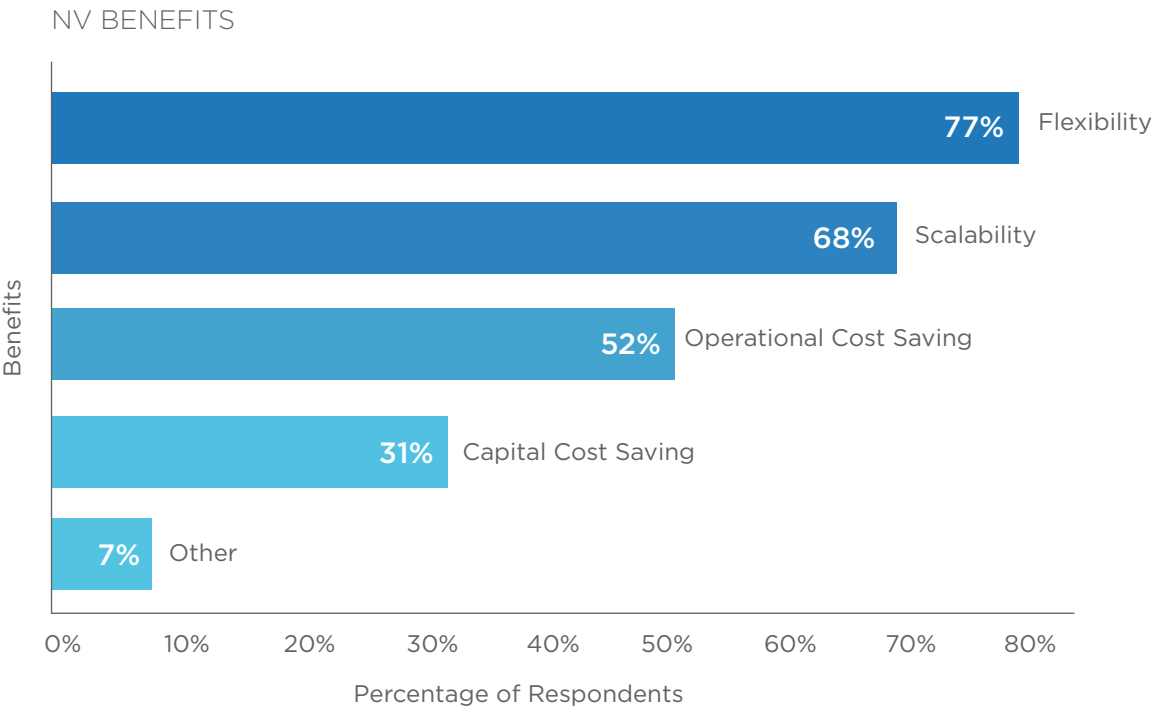
While organizations may have initially considered deploying network virtualization to garner cost savings (associated with the adoption of off-the-shelf hardware), the adoption has been ramping due to the need of the network to support the fast pace and scale of today’s environments. When asked to rank how important it was to find a NV solution in the next 2-5 years, 88% of respondents to our NV Survey said it was “Important” or “Mission Critical.”

The demands on the network are growing exponentially, with the explosion of users, devices and apps requiring resources. Network virtualization gives organizations a way to keep up. The ability to quickly deploy, change and move network resources allows organizations to scale their networks to meet changing demands. It also provides the flexibility required by the underlying infrastructure to support applications as they move from legacy client-server models to being delivered in the cloud as a software as a service (SaaS) offering.

Overall, network virtualization helps the network better integrate and align with the highly virtualized storage and compute resources it is connecting, delivering quick provisioning, improved resource utilization and operational efficiencies.

Benefits of Network Virtualization

For the past two years, organizations have cited the flexibility NV delivers as the biggest benefit. When asked to choose all the benefits that apply to NV, an overwhelming 77% picked flexibility. This year, scalability (68%) overtook operational cost savings (52%), which was the distant runner up last year. Interestingly cost savings came in fourth at 31%.



Network virtualization solves a lot of the networking challenges in today’s data centers, helping organizations centrally program and provision the network, on-demand, without having to physically touch the underlying infrastructure.

market summary

Flexibility

With NV, organizations can quickly provision (in a matter of minutes versus hours/days), move and scale the network to meet the ever-changing needs of the highly virtualized compute and storage infrastructures. In a world where agility is critical to being competitive, the ability to quickly make adjustments to support the business and optimize the overall experience improves the network's time-to-value.

NV makes easy to support micro-segmentation and multi-tenancy that gives organizations ultimate flexibility, in terms of how they organize and manage their environment. Organizations can have multiple silos and virtual networks, even using the same IP space, running over the same physical links. The benefits span from operations (allowing networks to be managed independently from a centralized location) to security (keeping resources separate, applying controls (e.g. firewalls) for each and every application in a data center, and helping contain attacks).

Modifications to the network's topology or how traffic is handled can be tried in different ways, without having to modify the existing physical networks. For example, the endpoints can all run a modified networking stack, with new protocols tunneled through existing physical legacy networks, without impacting existing networks.

Scalability

Current network topologies are rigid and prone to all kinds of problems. Overlay networks can help organizations avoid the limitations that come with VLANs, which can only support 4096 isolated networks, providing a 24-bit virtual network interface (VNI) that supports 16 million virtual networks.

Network virtualization ensures organizations can deploy the network resources whenever and wherever they need them. In addition, they can add capacity to make sure the network delivers the performance and reliability demanded of their environment. There is the ability to save and restore network topologies and configurations, via snapshotting, check pointing, and rollbacks, to support faster recovery from both bad configuration decisions and equipment failures in disaster recovery situations.

Operational Efficiencies/Costs Savings

Being able to centrally manage the distributed network has a lot of inherent benefits. In the future, as we see even more convergence between virtualization and cloud management, we can expect the benefits to compound.

One of the main reasons NV is so efficient is that any changes made to the physical underlay network do not impact the virtual overlay, removing a lot of the time and complexity required to deploy, manage and maintain traditional networks. Virtual machines (VMs) can be moved around without impacting the flow of traffic; there is no need to manually reconfigure physical links or endpoint settings.

In addition, organizations can take advantage of "template-ized" deployments of standard application stacks, with built-in networking topologies, enabling error-free, fast roll outs, as well as pre-checks to ensure the deployment supports compliance efforts uses networking best practices. Organizations can also save significant time by automating the set-up of service chains, within both Layer 3 and Layer 4-7 services, and accelerating the roll out of services, such as firewalls, IPS, etc. (particularly as the network is increasingly micro-segmented).

Cost Savings

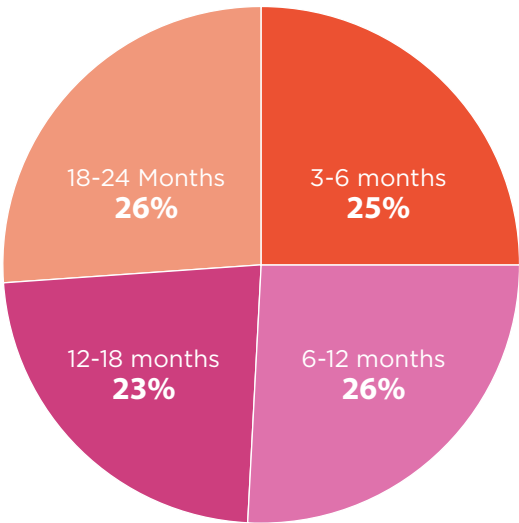
In addition to the capital savings associated with replacing costly, proprietary solutions with off-the-shelf, general-purpose hardware, organizations can benefit from overall improved resource utilization. The higher density of multiple virtual networks improves utilization, without running into IP subnet or VLAN conflicts. It also delivers subsequent operational cost efficiencies, associated with less real estate, power, cooling, etc.

market summary

A Look at Who's Adopting Network Virtualization

Overall, half of the respondents to our survey have already adopted NV solutions and half have not. Of those that haven't, 78% have plans to deploy NV solutions. 40% have plans to deploy in the next 3-12 months; while 60% believe they will have deployments in the next 12-24 months. Of those who have already deployed NV solutions, half did so about a year ago and half almost two years ago.

LENGTH OF TIME NV SOLUTIONS HAVE BEEN DEPLOYED

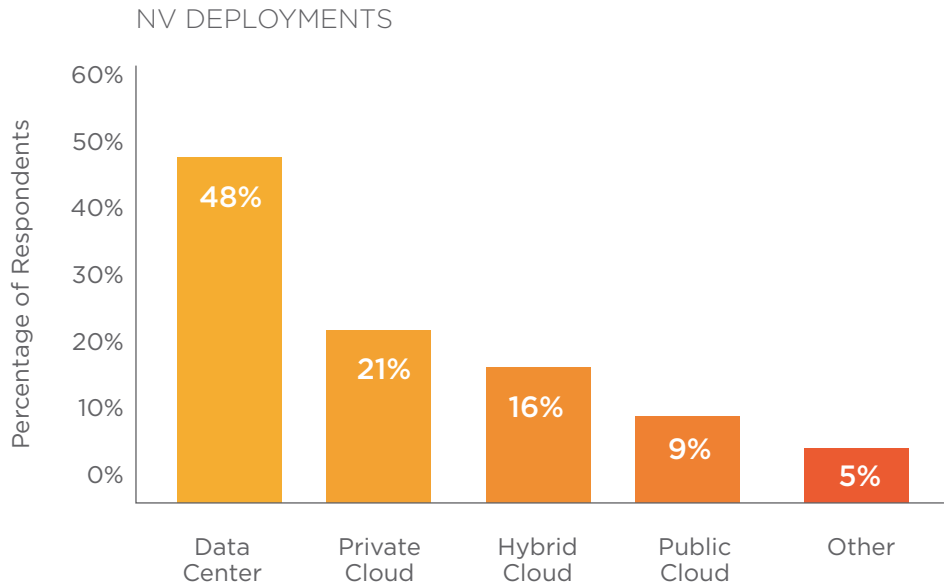


In terms of market segments, cloud service providers continue to lead the way, with 75% already using NV solutions and the other 25% planning on adding NV capabilities in the next 18-24 months. We saw a jump in adoption among service providers from last year, with 68% reporting they use NV solutions in their networks today. This was opposed to 41% last year; the adoption, however, is on par with what we expected, given that 85% of those who hadn't deployed NV last year were planning on doing so - 43% thought they would deploy within 3-12 months. Only 5% of service providers said they had no plans to use NV solutions in the foreseeable future.

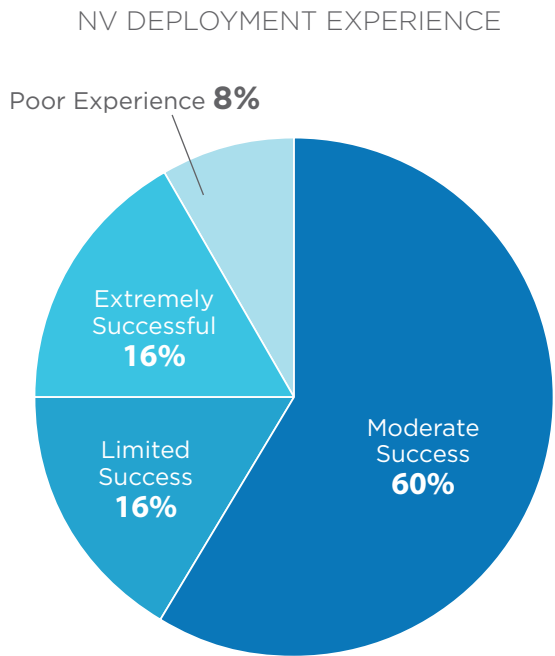
Large enterprises remain split in terms of their actual adoption; half have deployed, while the other half are in the planning stages, according to our survey. Only 8% have no plans to deploy in the next two years. Small to medium businesses continue to lag in terms of adoption with only 34% using NV solutions in their environment. The respondents this year, however, were more receptive to NV solutions, with 74% of those who don't have NV solutions indicating they have plans to deploy in the 12-24 months. That means only 26% have no immediate plans, which is an improvement from the 38% we saw in last year's results.

Where Network Virtualization is Being Deployed

Overall, the data center continues to be where organizations (48%) deploy network virtualization solutions, followed by private clouds (21%), hybrid clouds (16%) and public clouds (9%).



While many organizations have adopted NV solutions, most are still in the Proof of Concept (PoC)/testing phase – 54% of respondents to the SDxCentral Survey have not yet deployed their NV solutions in a production environment. Of those who have, 60% had moderate success (some issues) with their deployment, 16% indicated their deployment went off without a hitch, while 8% had implementations that failed.



market summary

Network Virtualization Use Cases

Some of the most common deployment scenarios and **use cases** for network virtualization can be found in the data center and campus/branch virtual networks:

Data Center Virtual Networks: Organizations are looking to create and manage multiple, isolated virtualized networks to support the needs of their different customers/clients, lines of business and/or departments. These virtualized networks can simultaneously handle multiple tenants, while keeping traffic and management controls separate between tenants.

Micro-Segmentation of the Data Center: With NV, organizations can deploy controls (firewall functionality) that segment the network and manage access to resources across different tenants within the data center network. Organizations can even segment the network to control access to individual apps.

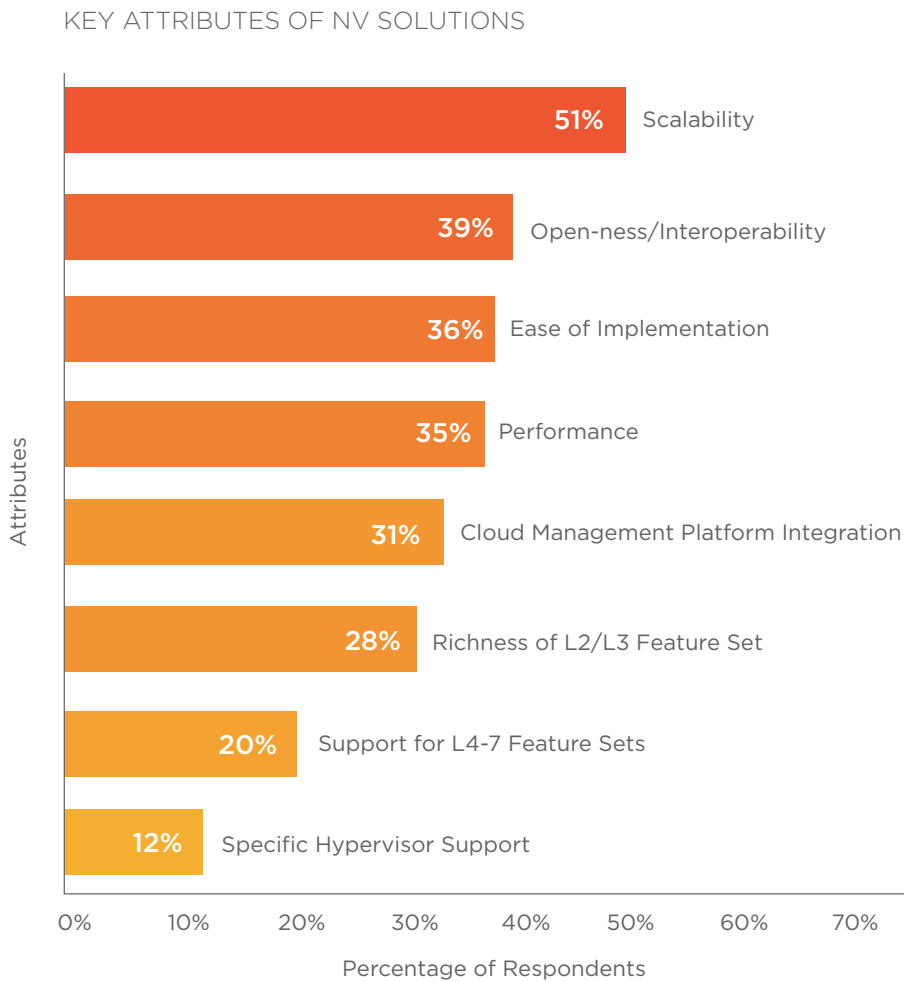
Data Center Refreshes: As organizations look to upgrade their infrastructure to support new, more agile business models, they are looking to deploy NV solutions that can help them spin up and scale virtual workloads.

Centralized Management of the Distributed Network: Organizations are looking to create an overlay that spans all their branch locations to give them centralized visibility and control over network traffic. The overlay streamlines the organizations ability to apply unified policies, automate campus and branch network operations, and maximize the utility of network resources.

Infrastructure as a Service: Cloud and service providers are offering on-demand network function services (e.g. virtual routers or virtual L4-7 functions) that customers can scale up or down as needed to move workloads to the cloud.

What Organizations are Looking for in NV Solutions

When asked to identify the top two attributes organizations are looking for from NV solutions, responses in our survey were divided. Only scalability got a majority vote – at 51%. Openness and interoperability came in second at 39%, which speaks to the varied architectures of most organizations and their need to ensure the solutions they choose can ‘play nicely’ in their environment. Ease of implementation and performance came in at 36% and 35%, respectively.



market summary

The SDNCentral Research Team has developed the following key capabilities to consider when evaluating NV solutions, based on real-world deployment experiences:

Capability	Consideration
Hypervisor Compatibility	<p>The virtual switch on the hypervisor plays a key role within any NV deployment. Choosing a hypervisor is often a strategic decision and, once deployed, can be difficult to change, so it is critical to ensure that the network virtualization solution natively supports the hypervisor of choice.</p> <p>Be aware that solutions marked as “compatible” with the hypervisor may be using a virtual switch instance that is running in a VM, with port-group mapping or another similar mechanism, to insert itself into the hypervisor environment. This is true particularly with VMware ESXi, which today restricts choices of virtual switches to its built-in version or limited partners. Performance for these “compatible” solutions has been less of an issue in the last year, as hypervisors improve the VM I/O performance, and non-VMware vendors are starting to displace VMware NSX on ESXi hypervisors with a VM-based workaround.</p>
Network Model	<p>More mature NV solutions will provide a network model that helps visualize and define the topology, including Layer 2, Layer 3, routing, gateways, Layer 4-7 chaining, etc. The more complex the environment, the more critical the model is to ensuring it is working properly.</p>
Physical Switch Infrastructure Compatibility	<p>While NV solutions try to operate primarily within the virtual domain, most require integration with the physical infrastructure, which means the availability and performance of physical to virtual gateways is critical. For NV solutions using VXLAN, there is an increasing number of switches that can act as hardware VTEPs (VXLAN termination endpoint) to facilitate these boundary transitions at wire-speed.</p>
QoS Support	<p>In networks that are jitter- or latency-sensitive, such as those supporting streaming media, voice, or critical apps (e.g. financial and medial apps), the presence of QoS support (Layer 2/Layer 3) can be helpful. In such environments, NV solutions based on direct-fabric programming may be able to provide better QoS control than pure overlay solutions.</p>
High Availability	<p>Most NV solutions depend on the physical underlay network to provide Layer 3 connectivity, rather than relying on conventional protocols, those solutions that program the fabric directly may be able to better detect and work around faults to improve overall availability of the network.</p>
Scalability	<p>Some NV solution designs may encounter performance challenges when the control planes reach their limits or when the data plane replicates broadcast, unknown unicast, or multicast traffic across the physical fabric unnecessarily. Vendors are working to overcome these limitations, but whether the solutions can scale to support large cloud environments with 10,000s of physical servers is still to be seen.</p>

market summary

Cross-Data Center Capabilities	Cross-Data Center capabilities are needed when multiple Data Centers are considered part of a single domain, as well as for disaster recovery (DR) or load rebalancing use cases. The ability to move VMs seamlessly across Data Centers, without reconfiguring the network can significantly reduce operational complexity.
Network Services	In virtualized networks, DHCP and IPAM/DNS services enable virtual machines to be brought up seamlessly. Some NV solutions have built-in DHCP and IPAM capabilities (usually basic and static), while others depend on third-party external DNS and IPAM appliances or services.
Layer 3 Routing Capabilities	Most NV solutions provide some routing capabilities, from limited, static routing to supporting a full suite of routing protocols (BGP, OSPF, and ISIS). Those without built-in protocol handling must integrate a virtual router or third-party virtual router. More mature solutions have distributed routing capabilities that can perform routing functions at the edge to reduce unnecessary packet traversal over physical and virtual links.
Layer 4-7 Capabilities/ NAT/ Service Chaining	<p>Many NV solutions have built-in Layer 4-7 capabilities, including Layer 3/Layer 4 Stateful Firewalls, DDoS prevention, caching, Web application FWs, IPS/IDS, IPsec VPN, and SLB. These capabilities mitigate the need for chaining with external Layer 4-7 services (physical or virtual) and make deployment of NV services more cost effective, however, they may not have all the features organizations need. If the solution needs to be integrated with more mature, feature-rich, third-party solutions, the ease of building service chains will be an important factor to consider.</p> <p>Without network address translation (NAT), virtual networks that live within a private address space (often overlapping with other tenants) cannot communicate with external entities. Advanced NV solutions provide more fine-grained controls over NAT, usually in conjunction with a Layer 4 FW capability.</p> <p>IPsec VPNs are typically required to integrate with private clouds and are useful in cloud bursting scenarios for hybrid cloud deployments.</p>
Visibility and Analytics	<p>Visibility is critical for network troubleshooting and management. For example, the ability to look into overlay tunnels and understand how they are traversing a particular physical path is key to optimizing the network's performance.</p> <p>On the analytics front, NV vendors tout monitoring and analysis within their solutions, with the ability to analyze traffic trends (throughput, latency) within the solution itself. However, most of these implementations are relatively basic, focusing on data capture, look for capabilities to mature in the coming months to improve analysis.</p>
Usability and Manageability	Due to the scale of NV solutions, usability and manageability are key considerations. The control and management panels for these solutions have to accommodate tens of thousands or hundreds of thousands of networks (perhaps millions in the near future). This unprecedented scaling presents a new challenge for user interfaces. Some of the complexity may be hidden through integration with an upper layer orchestration system, such as OpenStack, but monitoring and troubleshooting of large numbers of virtual networks is still a challenge many years into the NV journey.

market summary

Orchestration Stack Integration/ VM Mobility Support	<p>Most cloud environments deployed today have (by necessity) an orchestration system, such as OpenStack, CloudStack, vRealize (vSphere), and Microsoft SCVMM.</p> <p>Compatibility with the orchestration stack already in place in a cloud environment is critical; many NV solutions claim compatibility with multiple stacks, but the reality is the level of integration varies widely. Many orchestration stacks are still undergoing rapid development and refactoring, so the stability of the networking APIs tends to be low, forcing NV vendors to find alternate means to manage these integrations.</p> <p>For end users it means evaluating the nature of the stack integration at a deeper level and ensuring that what is needed is doable via a combination of external UI and orchestration stack integration. Organizations should also look for the support of VM mobility, which allows VMs to be moved across servers, racks, and Data Centers, while preserving network properties, such as IP address, ACLs, QoS, and other attributes.</p>
Automation and Programmability	<p>Most NV solutions claim support for RESTful APIs to enable automation and programmability, however, the granularity of such controls vary widely. In most cases, these APIs still are relatively immature, with only limited role-awareness and a lack of proper security controls, which means they probably can't be used in any type of compliance-heavy environment.</p>
Company Stability and Longevity	<p>Look at the pedigree of the vendor offering the solution to better understand their capabilities, longevity, roadmaps, and capacity for innovation - are they a networking incumbent, infrastructure company new to networking, recently funded startup?</p>
Openness of Solution, Compatibility with Other Elements	<p>Look for NV solutions that support standard protocols to improve compatibility with other network elements. VXLAN is the most popular encapsulation protocol today.</p> <p>On the direct-fabric programming side of the equation, the OpenFlow protocol is the most prevalent southbound protocol supported by switches, enabling the NV solution to have a wider reach, though Cisco's proprietary ACI has also experienced strong market adoption.</p>
Solution Availability	<p>Many NV solutions are shipping, but many are running in beta or have only limited availability. Customer timelines may dictate which solution is most appropriate, based on solution availability, quality and maturity.</p>
Container Support Strategy	<p>With the move towards Linux Containers, a new attribute to evaluate is the vendor's strategy for dealing with applications as they move from VMs into Containers. The rapid rise of Docker and their recent acquisition of container networking vendor Socketplane means it is important to understand how NV solutions integrate with Containers. Some NV vendors have already demonstrated early Container support.</p>

market summary

Approaches to Network Virtualization

The market is still early, marking a critical evolutionary step for the communications infrastructure that is relied on by almost everyone and everything. There are a number of vendors, new and old, who are each working to deliver what they see as the optimal network virtualization (NV) offerings. There are some that believe changes should be driven by the network, itself, while others feel the applications should be the main influencing factor. It is too early to tell which approach will win, which will lose or which will morph into something yet to be defined.

The approaches that vendors are taking are heavily dependent on where the NV solutions are going to be deployed. As noted earlier, many organizations are deploying NV solutions within their Data Center environments, followed by private, hybrid and public cloud environments. In addition, there are vendors specializing in offering solutions for infrastructure as a service (IaaS) or WAN deployments.

Network Virtualization in the Data Center

There are really two main approaches to data center deployments:

- 1. Directly programming the fabric.** This approach takes explicit control over the switches, creating and coordinating the virtual networks by directly programming the virtual switch and physical switches. Typically this approach requires customers to upgrade all their physical switches to support the appropriate protocols; a flow-control protocol, such as OpenFlow, or a vendor's proprietary protocol, will be used to manage the network.
- 2. Developing a network overlay.** There are a variety of ways in which an overlay network is accomplished; the most common is to modify or replace the virtual switch. In some cases, kernel modules are inserted into the hypervisor (most commonly with KVM as the hypervisor). In situations where the virtual switch cannot be replaced and the hypervisor is proprietary (VMware ESXi), vendors may choose to use a VM running a virtual switch instance as the terminating point for virtual networks.

In the overlay approach, multiple encapsulation protocols are available, ranging from straight GRE and IPsec, to NVGRE, STT and VXLAN, among others. Currently, VXLAN is dominant in the market, with support within many physical switches and hardware-based Layer 4-7 devices. The Generic Network Virtualization Encapsulation (GENEVE), which was proposed in Feb, 2014 as the uber-encapsulation protocol, had some uptake initially and interest waned after. It is the key encapsulation protocol in the new OVN (network virtualization on Open vSwitch) project and that may drive renewed interest.

market summary

The following table summarizes the benefits and challenges of the different approaches:

Approach	Example Vendors	Pros	Cons	Best Fit Use Case
Direct Programming - with explicit control over switches (using OpenFlow, SPB or other proprietary methods)	Cisco (ACI), Avaya, NEC PFC, Big Switch	No tunneling or encap/de-encap, fragmentation; possible strong QoS/SLA controls, simplified troubleshooting	Requires OpenFlow (or other similar protocol) or vendor equipment throughout the entire infrastructure	Where a user has complete control over entire infrastructure and needs fine grained control over QoS, SLA, etc.
Overlay - virtual switch centric, including kernel modules in the hypervisor	VMware NSX, Cisco Nexus 1000V, VTS, Midokura, PLUMgrid	No need for drivers on guest VMs, which supports more VM OSes	Access to the hypervisor is required for kernel modules (not always easy); if running a vSwitch in a VM (due to limitations by VMware), there can be significant performance degradation	Either KVM/ OpenStack deployments with access to hypervisor, or VMware environments, if the vSwitch is certified by VMware
Overlay - guest VM driver, or a driver on a desktop	SD-WAN implementations - please see our “Virtual Edge” report for more information.	Simple to deploy, ability to connect VMs everywhere, regardless of location	Requires client driver on each host; might have scalability limits; little control over QoS; only supports virtual Layer 3, Layer 4-7 services	IaaS environments or other location where the user has little control over the infrastructure

Network Virtualization as a Service

Buying network virtualization capabilities as a service is increasingly popular. With the rise of public cloud platforms, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, IBM SoftLayer and Rackspace, as well as other private/hybrid platforms offered by service providers, including AT&T, NTT, Verizon and other carriers, many enterprises are migrating their traditionally internal applications to run in public or private clouds operated by service providers.

Increasingly, these migrated applications require more sophisticated networking than just a single public IP address, so cloud providers are delivering network virtualization capabilities, in the form of infrastructure as a service (IaaS) offering, to allow customers to provision the network to meet their needs. 39% of respondents to the SDxCentral Survey indicated they would use a Network Virtualization as a Service (NVaaS) as part of the public or hybrid IaaS solutions.

NVaaS could provide self-service, dynamic network capabilities, such as virtual routing, L2 over the WAN, Layer 4-7 service chaining for firewalls, load-balancing and other functions. Typically, to deliver these services, providers will utilize overlay technologies, with a mix of proprietary, custom solutions (e.g. Amazon, Azure, Google) and packaged, managed versions of commercial products (e.g. NTT, Verizon). Sometimes they may use a blend of commercial, custom and open-source solutions (Dreamhost, Rackspace).

market summary

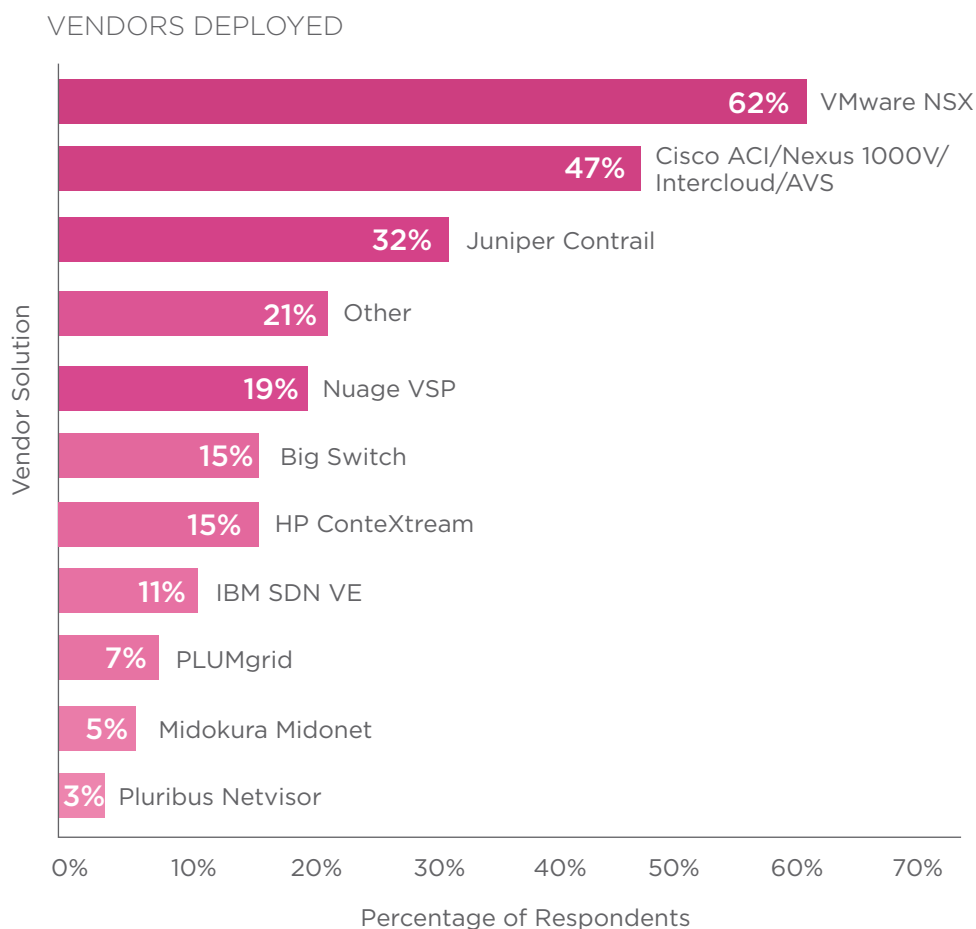
Network Virtualization for the WAN

The WAN, which is covered comprehensively in the recent 2015 Virtual Edge Report, has long been running network virtualization, as evidenced by the fact that very few dedicated links exist today. The majority of approaches used by providers to achieve virtualization consists of using L2 or L3 VPN technology, such as MPLS VPNs (L2 and L3), VPLS, L2TP and OTV, to name a few.

Direct fabric programming enables providers to more easily attain tight controls over quality of service (QoS), while overlays require more advanced handling to achieve those controls. Overlays, however, can provide a little more flexibility, employing WAN virtualization techniques, such as MPLS VPN over GRE (or multipoint GRE) to allow the traffic to traverse networks that are not MPLS-ready via tunneling. In terms of categorization, IPsec VPNs could be considered an overlay WAN virtualization technology, since it provides the means of running multiple private networks over a shared WAN infrastructure.

Market Shifts: Some Key Production Deployments by Market Leaders

For the second year in a row, in the SDxCentral NV Survey, VMware NSX was the vendor most often cited as being used or under evaluation by customers, followed by Cisco's ACI/ Nexus switches/Intercloud/AVS. This is slightly different from industry analysis, which has indicated Cisco ACI is outpacing VMware NSX by about 2:1.²



² Gartner Analyst Andrew Lerner, Oct. 2015.

market summary

SDxCentral's Research Team took a look at the technology and solution announcements the leaders in this space made and the customer deployments they referenced this past year to try to understand some of the movements in the market. Our assessment is that the market is being driven by the "big four" -- VMware, Cisco Systems, Juniper Networks and Nuage. In most major installations, these are the big NV players being considered. These companies also have announced the most customers.

While our own survey indicates that VMware is the leader with Cisco in the number two spot, we'll note there is other research and data out there ranking the vendors in different orders, though the top four are almost always the same. For example, a recent IHS data-center study released this year ranked the top three as VMware, Nuage, and Cisco, in that respective order.³

To get more detail on what's going on, the section below compiles recent activity by the big four.

VMware - NSX

NSX is VMware's network virtualization platform for the software-defined data center (SDDC). It allows organizations to treat the "physical network as a pool of transport capacity, with network and security services attached to virtual machines (VMs), with a policy-driven approach."⁴ In July, VMware announced they had more than 700 customers, which is up from 150 just a year ago.⁵

"NSX is not a step, it's an evolutionary leap in capability around operations, around security," said David Giambruna, CIO, **Tribune Media**, who used NSX to migrate 141 applications onto their new infrastructure in five months, with virtually no disruption. If a Tribune property comes under attack, he can quickly move it. If he decides to shift an application to or from the cloud, he can do that too, and best of all, the security moves right along with it.⁶

In August of 2015, VMware released NSX 6.2, touting its Cross vCenter Networking and Security features, which allow it to extend the virtual network to another data center. Earlier in the year, VMware announced integrations with Docker (adding to its partner portfolio, which includes Palo Alto Networks) to provide security controls for the virtual network. (VMware is leveraging libnetwork to bring micro-segmentation, using strong, policy-driven stateful firewalling to Docker container environments, via VMware NSX.⁷) In addition, they described how customers who adopted the newly released Horizon 6 solution, could benefit from the micro-segmentation of NSX to secure east-west traffic between virtual machines (VMs).

In general, VMware played up the micro-segmentation and distributed firewall capabilities of NSX this year, noting at VMworld a number of customers have deployed micro-segmentation in their production networks/data centers. They noted the drivers for micro-segmentation are the ability to improve the coverage of their security controls – "75% of data center network traffic is east-west... nearly all security controls look exclusively at north-south traffic as it moves in and out of the data center, which means 90% of east-west traffic never sees a security control."⁸

One of the customers VMware highlighted was **Synergent Corporation**, who wanted to onboard customers more quickly and deliver services faster. They created a cloud-based multi-tenant environment built on VMware's vCloud Suite Advanced and deployed VMware NSX to virtualize its network. With NSX, Synergent implements micro-segmentation, based on fine-grained policies, to enable security inside and outside of Synergent's datacenter. The NSX platform's policy-based distributed firewalling and L3 routing enable multi-tenancy for the financial services applications Synergent hosts for its credit union customers. "We've reduced provisioning times for new virtual machines and scale quickly," said Trever Jackson, Enterprise Infrastructure Architect at Synergent. "We achieved our goal for average cost-per-virtual machine and more manageable costs."⁹

³IHS data center SDN survey, Nov. 2015 (<http://www.infonetics.com/pr/2015/Data-Center-SDN-Strategies-Survey.asp>)

⁴<https://www.vmware.com/products/nsx>

⁵<https://blogs.vmware.com/networkvirtualization/2015/07/3-months-on-the-road-with-nsx.html>

⁶<http://www.vmware.com/radius/tribune-media-reinvents-its-network/>

⁷<https://blogs.vmware.com/networkvirtualization/2015/06/vmware-docker-networking.html#more-1945>

⁸"Organizations Can be Twice as Secure at Half the Cost," VMware blog, Sept. 9, 2015, <http://blogs.vmware.com/networkvirtualization/>.

⁹<http://virtualizeyournetwork.com/synergent-taps-vmware-nsx-for-micro-segmentation-and-it-automation-in-the-software-defined-data-center/>

market summary

Another customer for the micro-segmentation use case was **Exostar**, who deployed it to isolate and segment different tenants within the same cloud infrastructure and prevent attacks from spreading. “With VMware NSX, Exostar has significantly reduced the time it takes to onboard customers and bring up new services, saving hours for IT. Exostar IT can spin up environments for new customers with all of the requisite security and networking with the click of a mouse. If IT adds, moves or decommissions a service, all of the buildup and tear down of the infrastructure is automatically handled by VMware NSX. The solution has allowed Exostar to simplify its network architecture without sacrificing performance or security, improving network management and troubleshooting.”¹⁰

The NSX firewall is a license that can be added to a customer’s vSphere deployment to controls ports and protocols close to the source/destination, at the vNIC level; this delivers a high degree of control and enables organizations to clamp down on the lateral spread of an attack within the virtual environment.

GCN reported the **City of Avondale**, Arizona used NSX 6.1 as its firewall and load balancing solution. NSX enabled the city to “boost its security posture by segmenting the network, essentially putting firewalls between servers to secure traffic moving between virtual machines or apps... ‘It’s really nice to have one single pane of glass that is going to give us the ability to see where this data is going or who has access to what,’ said Wesley Harris, an Avondale IT system administrator. ‘Before, if a system engineers asked whether something was ‘set up inside of VMware or is it set up on a physical switch,’ I’d have to go to the network guys and have them look at the firewall there. Now we can all work together as a team.’”¹¹

Avondale’s deployment is different from another VMware NSX customer, **Columbia Sportswear**, which used an integrated firewall service from Palo Alto Networks when it adopted a SDDC model. The value of the joint solution, according to John Spiegel, Columbia Sportswear global IS communications manager, is its reduced time and costs to implement.

“If Columbia Sportswear were to conduct this project in the traditional way, using physical hardware and physical solution and physical approach,” said Spiegel, “our costs would have been an additional \$2 million. Additionally it would have taken 12 months to implement. Right now we are adding security to our data centre at one third the cost and one third of the time. Securing our systems in the right way, moving faster, transforming while keeping an eye on the bottom line. This will be a big win for us.”¹²

Cisco – ACI/Nexus/AVS/Intercloud

Cisco’s offerings center around its **Application Centric Infrastructure (ACI)**, which is an SDN architecture that uses a common policy-based operating model across an ACI-ready network. The goal is to create an environment that is more responsive to business and application needs, with the applications driving network behavior.

ACI uses pre-defined application requirements and policy profiles to automate the provisioning of the network, application services, security policies, tenant subnets and workload placement.¹³ Cisco uses its **OpFlex** policy protocol to communicate with the **Application Policy Infrastructure Controller (APIC)**, which controls the underlying network (made up of Nexus Switches – **Nexus 1000/9000** – and **Cisco Application-centric Virtual Switches (AVS)**, which are hypervisor-residents of the Nexus virtual switch).

Cisco’s Intercloud Fabric (ICF) is made up of the Intercloud Director and Fabric Secure Extender; it’s designed to provide interconnectivity to a large ecosystem of cloud providers to support hybrid cloud deployments, that leverage ACI, for enterprises.

¹⁰ <http://www.vmware.com/company/news/releases/vmw-newsfeed/Exostar-Deploys-VMware-NSX-to-Deliver-Strong-Security-and-IT-Automation-for-Customers-in-Highly-Regulated-Industries/1989167>

¹¹ <https://gcn.com/articles/2015/05/27/avondale-virtualized-network-platform.aspx>

¹² <http://www.computerworlduk.com/news/infrastructure/how-columbia-sportswear-will-enhances-security-with-software-defined-data-centre-approach-3606103/>

¹³ <http://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/aci-fabric-controller/at-a-glance-c45-729864.pdf>

market summary

One thing that makes Cisco's strategy so powerful is the ecosystem that is behind it. There is, of course, the recently announced Ericsson partnership, which will likely bring some interesting capabilities to the market (only time will tell), but they have also announced other partnerships, including:

- **CLiQr** - for end-to-end provisioning of the cloud infrastructure
- **VCE and NetApp** - to build Intercloud-ready solutions
- **Johnson Controls** - to add compute capacity to the data center
- **Accenture** - for cloud management and orchestration capabilities
- **Telstra, Dimension Data and Sungard Availability Services** (Sungard AS) - as Intercloud partners who will align their public cloud infrastructure with ACI

Cisco also has continued to add integrations with partners, such as **A10** (for protecting a compromised web site within ACI with A10's Thunder ADC), as well as other Cisco solutions, such as the Cisco **FirePOWER** family of security appliances (physical and virtual) to provide threat intelligence to combat emerging data center threats. They also announced ACI was validated by independent auditors for deployment in PCI compliance networks.

Cisco is taking advantage of data center refresh cycles to drive adoption of ACI. In September, Cisco announced it had 1000 SDN customers, adding 100 in just two months. The list includes named accounts, such as **Danske Bank, Qbranch, Experian, Symantec, NetApp** and **Zitcom** customers. Some snapshots of customers highlighted this year include:

- **Symantec** is using Cisco ACI to change the way their data centers operate. Over the next five years, they expect Cisco ACI will deliver real business benefits - \$25.27 million in risk mitigation and business productivity, \$10.08 million in IT infrastructure cost reduction, \$8.50 million in IT staff productivity.¹⁴
- **Alestra** plans to deliver hybrid cloud solutions based on ICF and ACI. Alestra CEO, Rolando Zubiran, believes "Alestra has become the first service provider to offer to the customers [in Mexico] the capability to connect their private infrastructure with our best-of-breed Cisco Cloud Service in a hybrid mode."¹⁵
- **Bowling Green State University** announced it was using ACI to support a "more efficient, highly secure data center."¹⁶ As the university looks to improve the use of technology in the classroom for active learning and expand beyond its traditional on-campus activities, with eLearning offerings, it believes its new data center, based on Cisco's SDN technology, will enable them to better deliver on these new opportunities.
- **UAE Telecommunications Regulatory Authority** chose Cisco to power the Telecommunications Regulatory Authority's (TRA) Electronic Federal Network (FedNet) which will connect all federal government entities in the United Arab Emirates (UAE) via the government's Smart Cloud. ACI is one of the architectures that will be employed in the deployment.

While many organizations are using the APIC, which is the brains of ACI, the underlying hardware for ACI - the Nexus 9000 - has not seen quite as rapid an uptick to support ACI. While there are 4100 customers for the Nexus 9000 switch, which is the next-generation of the Nexus 1000 switch that has been shipping for over a year and a half, the number of those customers who are ACI customers is significantly smaller (20% according to their quarterly report in February 2015¹⁷).

With all the good news Cisco issued, they also had a serious security advisory on a vulnerability in the cluster management configuration of the APIC and the Nexus 9000, which "could allow an authenticated, remote attacker to access the APIC as the root user."¹⁸ While security advisories aren't unique in any way to Cisco, they illustrate the overall importance of building the appropriate security capabilities and controls into these architectures and offerings.

¹⁴ <http://www.cisco.com/c/dam/en/us/solutions/data-center-virtualization/application-centric-infrastructure/benefits-aci.pdf>

¹⁵ <http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1726332>

¹⁶ <http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1725211>

¹⁷ <http://investor.cisco.com/investor-relations/financial-information/sec-filings/sec-filings-details/default.aspx?FilingId=10497412>

¹⁸ <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-apic>

market summary

Juniper Networks - Contrail

This year, Juniper highlighted the advancements they have been making in software – pointing out that 80% of their Juniper Development and Innovation engineers are actually software developers¹⁹. Their most notable offering is **OpenContrail**, which is an open source project that integrates with OpenStack, and **Contrail Networking**, which is an open SDN solution designed to provide network virtualization and automation for clouds.

There are a number of customers who have described their use of Contrail within their production environment. **Symantec** uses OpenContrail within their cloud platform for its network virtualization and SDN capabilities²⁰. **Cloudwatt** integrated OpenContrail into their OpenStack cloud management platform, giving them full control over the infrastructure to support the customization and optimization of their public cloud environment; Cloudwatt uses Contrail's analytics, real-time monitoring, diagnostics and troubleshooting to improve the cloud's operational efficiency and provide transparency to support their security and regulatory compliance initiatives²¹. **SunGard, Jaguar Network** and **Orange Business Services** were early adopters of Contrail, using it to virtualize and automate their network infrastructure.

Early in 2015, Canonical and Juniper teamed up to deliver the **Contrail Cloud Platform**, an Ubuntu-based distribution for data center ecosystems that combines Contrail Networking with Juniper's OpenStack distribution. The Platform gives service providers a highly flexible service delivery platform that helps them create and scale SDN and NFV capabilities across their data centers and seamlessly join multi-tenant hybrid OpenStack clouds.

"**Wingu** is a key African public cloud service provider that is launching commercial Infrastructure-as-a-Service services later this year to address the challenges that businesses face when deploying applications and workloads in the cloud... The Wingu platform will be used to develop advanced SDN and NFV solutions," said Thomas Lee, general manager, Cloud Services at XON Systems, which is an investor in Wingu. "This latest technology integration between Canonical and Juniper provides a stable, scalable and agile platform for Wingu to deliver cloud services, allowing them to leverage the best open source and commercial platforms and expertise."²²

In November of 2015, Juniper introduced **Contrail Service Orchestration** (expected to be available in Dec. 2015)²³, which is software that enables service providers to manage the entire service lifecycle and simplifies the integration of third-party virtual network functions. The software will also support a software portal that will allow customers to self-select the services they want, such as virtual security. Additionally, they announced a **NFX250 Network Services Platform** (expected to be delivered in first half of 2016)²⁴, which is a secure, software-driven, on-premises device that offers server-like functionality, and a Cloud customer premises equipment (**CPE**) solution, which combines the Contrail Cloud Platform, Contrail Service Orchestration and NFX250 Network Services Platform, as a use case for service providers to "deliver managed services to enterprise customers."²⁵

AT&T cited collaborating with Juniper to develop the CPE solution they are using to "give customers more control, allowing them to quickly update network functions without having to buy new hardware... 'We're working with Juniper to build and deploy the next generation of networking services. With the support of their technology, we can build and deploy new business services faster. Businesses can be more agile and cost efficient,' said John Donovan, senior executive vice president, AT&T Technology and Network Operations."²⁶

¹⁹ <http://forums.juniper.net/t5/The-New-Network/Agility-And-Choice-Demand-An-Open-Software-Business/ba-p/283641>

²⁰ <http://www.juniper.net/us/en/company/case-studies/service-provider/symantec/>

²¹ <http://www.juniper.net/assets/us/en/local/pdf/case-studies/3520522-en.pdf>

²² <http://www.businesswire.com/news/home/20150226005299/en/Juniper-Networks-Canonical-Partner-Deliver-OpenStack-Based-Cloud>

²³ <http://newsroom.juniper.net/press-release/juniper-networks-transforms-network-economics-with-scalable-nfv-solution>

²⁴ <http://newsroom.juniper.net/press-release/juniper-networks-transforms-network-economics-with-scalable-nfv-solution>

²⁵ <http://www.juniper.net/us/en/solutions/nfv/cloudcpe/>

²⁶ http://about.att.com/story/network_on_demand_juniper.html

market summary

Nuage Networks – Virtualized Service Platform

Nuage Networks is Alcatel-Lucent's SDN venture. Their architecture is based on OpenStack and the Nuage Virtualized Services Platform, which is available as a pre-designed, public-facing environment. The platform includes a services controller (brains/management) and directory (logic) and routing and switching modules.

This year Nuage introduced a POC for service chaining for large enterprises; working with **Telefonica Business Solutions**, Nuage announced they had successfully tested the service chaining of virtualized network functions (NFV) in a multi-vendor SDN environment. VSP provided the automated overlay network for Telefonica's VMware environment, which enabled the automatic insertion of physical and virtual network services with the appropriate configurations and policies as part of their cloud based offerings.²⁷

Other customers of the platform highlighted this year included **CTCC** and **CenturyLink**. CTCC, China Telecom's cloud services-focused subsidiary. They chose Nuage VSP for their SDN deployment to improve the elasticity and scalability of their cloud services platform.²⁸ They plan to use the micro-segmentation capabilities of the platform to isolate networks within its data center to mitigate the impact that distributed denial of service (DDoS) attacks could have on their environment.

"We are pleased that Nuage Networks has helped us to achieve scalability in our cloud infrastructure and improve the availability of the services," said Guang Xiaoming, the chief technology officer of CTCC. "We can now offer our customers self-serve public cloud services in a more secure and dynamic way, giving them services that are tailored to meet their unique business requirements," Xiaoming said.

CenturyLink, Inc. is going to use Nuage to provide networking functionality for their Programmable Services Backbone (PSB) network. "CenturyLink is transforming its network to offer businesses quick delivery of reliable and automated services, and is pushing those services where they are most needed – at the edge of our network," said Aamir Hussain, CenturyLink executive vice president and chief technology officer. "This fundamental architectural shift will enable dynamic delivery of scalable services for customers and provide even more differentiated services in the future."²⁹

Nuage also joined forces with **HP** (and **F5**) to provide a multi-vendor, production ready, enterprise-grade cloud solution. "HP Helion OpenStack 2.0 enables customers to create and manage software defined networks (SDN) in a distributed, multi-datacenter environment through integration with HP Distributed Cloud Networking (DCN) and Nuage Networks Virtualized Services Platform. This removes the boundaries of traditional networking, unlocking the full automation and agility needed for hybrid cloud."³⁰

This announcement actually points to a larger trend of interoperability, which, as we've already noted, is a key feature that customers are looking for in their NV solutions. The fact that network functions can be spun up, down or moved on-demand, makes it that much more important all the pieces work well together; compatibility issues can eliminate the flexibility, scalability and efficiency gains that network virtualization can deliver.

In addition to HP, Nuage collaborated with **Arista Networks**, announcing a common framework for network automation that will integrate virtualized and bare metal assets in the data center.³¹ They also took efforts to ease customer's minds around interoperability by launching a self-service certification initiative, focused on vendor interoperability for Layer 4-7 application delivery and security. Newly certified vendors include **Citrix, CounterTack, Fortinet, vArmour, Palo Alto Networks** and **GuardiCore**.

²⁷ <http://www.nuagenetworks.net/news/nuage-networks-and-telefonica-business-solutions-complete-service-chaining-proof-of-concept-for-large-enterprise-customers/>

²⁸ <http://www.nuagenetworks.net/china-telecom-stacks-cloud-infrastructure-nuage-sdn/>; <http://www.nuagenetworks.net/news/china-telecoms-cloud-arm-chooses-nuage-networks-sdn-technology-enable-public-cloud-services-china/>

²⁹ <http://www.nuagenetworks.net/news/nuage-networks-sdn-technology-selected-for-centurylinks-network-architecture/>

³⁰ <http://www8.hp.com/us/en/hp-news/press-release.html?wireId=1996634&pageTitle=HP+Helion+OpenStack+2.0+Delivers+a+Production+Ready%2C+Enterprise+Grade+Cloud+Platform+#.VkoInberSM9>

³¹ <http://www.nuagenetworks.net/news/nuage-networks-collaborates-with-arista-networks-for-open-networking/>

market summary

Vendor Profiles

The following sections profile many of the vendors in the NV 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.

In addition to commercial vendor solutions, open-source continues to be a big part of the whole SDN and NFV ecosystem. We have included a list of prominent open-source network virtualization initiatives and solutions, including Akanda, Project Calico, OVN and the VTN module within OpenDaylight. Extended commercial and open-source 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.

category: **commercial**

DELL

Dell Active Fabric Manager (Click for online version)<http://www.dell.com/us/business/p/dell-fabric-manager/pd>

One Dell Way
Round Rock, TX 78682
<http://www.dell.com>
info@dell.com

Description: Dell has multiple NV products of their own as well as from partners. Primarily Dell's network OS support OpenFlow and VXLAN for NV. Partner solutions on operating systems are available from Cumulus, BigSwitch networks, Pluribus and IPInfusion. On network overlays Dell's infrastructure works with VMware NSX, Midokura and Nuage from commercial and OpenDayLight on opensource. Commercial OpenFlow Controller comes from integration with NEC Controller. Dell Active Fabric Manager automates the design, implementation and monitoring of fabrics. Additionally there is support for scripting and automation tools like Puppet on the switch OS.

COMPANY TYPE	COMPANY SIZE	SUPPORTED HYPERVISORS
Private	10,000+	KVM, Xen, Hyper-V
CUSTOMER SEGMENTS		ORCHESTRATION STACK INTEGRATION
Cloud Service Providers, Healthcare, Financials, Government & Education, Retail		OpenStack, VMware vCloud Suite, CloudStack, Support for Dell CloudManager and other vendor CMP solutions.
DEPLOYMENT LOCATION		LAYER 2+ NETWORK SERVICES
Intra-Datacenter, Inter-Datacenter, Campus, WAN		DHCP, DNS, NTP, BOOTP, Dell Open Automation & Bare Metal Provisioning
NV CLASSIFICATION		LAYER 3 NETWORK SERVICES
Overlay, Direct fabric programming, Hybrid		L3 static routing, L3 distributed routing
SOUTHBOUND PROTOCOLS		BUILT-IN LAYER 4-7
OpenFlow (1.0, 1.1, 1.3), OVSD, OF-Config, Vendor-specific RESTful API		L3 Firewall, L4 Stateful Firewall, L7 application-aware Firewall (ALG), L3 Load balancing, L4-L7 Stateful Load balancer, IPS, DDoS prevention, Generic DPI rules. This is from partners NV solution. Not all these come on the same product.
ENCAPSULATION FORMATS		LAYER 4-7 SERVICE INSERTION
VXLAN, GRE, NVGRE, STT		Basic service chaining, Chaining of virtual services, Chaining of physical services, Rewrite capabilities (IP, VLAN), Load balancing across service insertion chains, L4-L7 rule-based service chaining. The service chaining features are available on Dell's partner solutions
QoS SUPPORT		DIFFERENTIATION IN APPROACH
L2 QoS, L3 QoS		Dell enables the Open Networking Ecosystem with a complete suite of solutions in addition to Dell Active Fabric Manager that include Dell OpenFlow Offerings, Dell OpenDayLight Controller, Dell Active Systems Manager (ASM) and Dell Software Foglight for Virtualization (FVE). In addition Dell provides reference architectures, best practices and services including pre-integrated solution bundles for Microsoft, VMware and OpenStack private cloud solutions.
BUILT-IN ROUTING PROTOCOLS		CUSTOMERS
BGP, OSPF, RIP, ISIS		https://www.sdxcentral.com/wp-content/uploads/2015/03/Key-customers-Dell.png
CROSS-DATA CENTER (STRETCHING) SUPPORT		
With Dell Fabric Manager and other solutions there are numerous ways to accomplish cross-Data Center support depending on the solution chosen; the most common methods include using Dell's VXLAN feature, Dell/VMware NSX and Dell/Silver Peak solutions.		
VALUE PROPOSITION		
Dell's Active Fabric Manager uniquely manages multiple fabrics from a single GUI/console and automates the design & deployment of multi-tier fabric topologies. Complete with over 100 customizable templates, industry-leading northbound API integrations, a variety of platform element managers including VMware vSphere and OpenStack Neutron and support for discovering & integrating existing switching/virtual fabrics clients reduce the costs and time required to manage data center's network fabric.		

Avaya Fabric Connect (Click for online version)<http://www.avaya.com/ca-en/solution/fabric-connect/>**AVAYA**<http://www.avaya.com/usa/>

Description: Avaya's Fabric Connect is the foundation to our SDN Fx architecture, supporting full L2/3 virtualization with integrated routing and multicast. It is unique in that it extends from Data Center to desktop, incorporating wired and wireless domains, and across geographical distances seamlessly (via stretched L2 domains or overlaid across IP WANs) enabling horizontal segmentation.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 10,000+	Fujitsu, Montreal Canadians Bell Center, Sochi 2014 Olympic Winter Games, Long Island Railroad, City of Troy
PRODUCT DETAILS	
Customer Segments: Healthcare, Financials, Government & Education, Hospitality (stadiums, gaming, convention centers and hotels) Deployment Location: Intra-Datacenter, Inter-Datacenter, Campus, WAN, IP Video Distribution and IP Video Surveillance deployments NV Classification: Hybrid Southbound Protocols: OpenFlow 1.4, NetConf and SNMP	Hypervisors: KVM, ESXi, Xen, Hyper-V Orchestration Integration: OpenStack Encapsulation Formats: VXLAN, IEEE 802.1aq QoS Support: L2 QoS, L3 QoS, Layer 4 QoS Built-in Layer 4-7: Not Applicable Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services, Load balancing across service insertion chains, L4-L7 rule-based service chaining

Big Cloud Fabric (Click for online version)<http://www.bigswitch.com/sdn-products/big-cloud-fabric>**BIG SWITCH NETWORKS**<http://www.bigswitch.com>

Description: Big Switch's Big Cloud Fabric (BCF) is built using Open Ethernet switches (whitebox or brightbox) and SDN controller technology. Customers benefit from application agility due to automation, operational simplification due to SDN and, dramatic cost reduction due to hardware and software disaggregation.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 51-200	Clean Safe Cloud, Clemson University, Fidelity, Intuit, U2 Cloud
PRODUCT DETAILS	
Customer Segments: Financials, Government & Education, Telecom Deployment Location: Intra-Datacenter NV Classification: Direct fabric programming, Unified Physical + Virtual SDN Fabric Southbound Protocols: OpenFlow 1.3, Vendor-specific RESTful API Encapsulation Formats: VLAN QoS Support: L2 QoS	Hypervisors: KVM, ESXi, Xen, Hyper-V Orchestration Integration: OpenStack, VMware vCloud Suite, CloudStack Built-in Layer 4-7: L3 Firewall Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services, Load balancing across service insertion chains

Cisco ACI, Virtual Topology System (VTS) Cisco Nexus 1000V, AVS, VACS (Click for online version)

CISCO SYSTEMS
<http://www.cisco.com>

www.cisco.com/go/aci, <http://www.cisco.com/go/vts>

Description: Cisco ACI delivers policy based automation across any endpoint for operational efficiency. Cisco Nexus 1000V and AVS leverage Cisco NX-OS software used by Nexus switches. Virtual Application Cloud Segmentation (VACS) Services comes with preconfigured and integrated virtual services, switching, and workflow automation tools. Virtual Topology System (VTS), a standards-based, open, overlay management and provisioning system, provides scale and simplicity to VXLAN Overlays.

COMPANY DATA	CUSTOMERS
Company Type: Public Company Size: 10,000+	ACI: Symantec, NetApp, Experian, Du Telecom, Pulsant VTS: http://www.networkworld.com/article/2994289/cisco-subnet/cisco-supplying-sdn-and-nfv-to-softbank.html
PRODUCT DETAILS: ACI	PRODUCT DETAILS: VTS
Customer Segments: Enterprise, Commercial, Healthcare, Defense, Financials, Service Providers Deployment Location: Intra-Datacenter, Inter-Datacenter Hypervisors: KVM, ESXi, Xen, Hyper-V Southbound Protocols: Vendor-specific RESTful API, OpFlex	Customer Segments: Cloud Service Providers, Service provider and Enterprise operations teams Deployment Location: Intra-Datacenter, Inter-Datacenter Hypervisors: KVM, ESXi Southbound Protocols: Vendor-specific RESTful API, NETCONF, RESTCONF, MP-BGP EVPN

Dynamic Virtual Networks (DVN) (Click for online version)

CPLANE NETWORKS
<http://www.cplanenetworks.com>

<http://www.cplanenetworks.com/openstack>

Description: CPLANE's Dynamic Virtual Networks (DVN) family of products automates the creation of virtual data center and wide area networks (with QoS) for OpenStack. Distributed OpenStack clouds can be seamlessly connected through our Overlay Gateway Router (OGR). OGR also enables OpenStack cloud bursting to public clouds such as Amazon Web Services via Internet/IPSEC or AWS Direct Connect. Products include: DVNd for data center networking, DVNi for WAN automation, DVNe for edge services (OGR).

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 1-50	Not Disclosed
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Government & Education, Telecom, Retail NV Classification: Overlay, Direct fabric programming, Direct programming of MPLS, physical and virtual network functions (i.e. gateways), service chaining Southbound Protocols: OpenFlow 1.3, OVSD, Vendor-specific RESTful API, REST, CLI, NETCONF, SNMP, XML, proprietary extensible	Hypervisors: KVM Orchestration Integration: OpenStack Deployment Location: Intra-Datacenter, Inter-Datacenter, WAN Encapsulation Formats: VXLAN, MPLS QoS Support: L2 QoS, L3 QoS Built-in Layer 4-7: BGP, OSPF, RIP, ISIS Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services

OneController (Click for online version)<http://www.extremenetworks.com/product/onecontroller>**EXTREME NETWORKS**<http://www.extremenetworks.com>

Description: Extreme Networks' OneController leverages the OpenDaylight framework to provide an open and standards-based SDN Controller for automation and orchestration of the network. It forms the basis of Extreme Networks' evolutionary SDN Platform which allows you use products based on based REST (web-based) APIs which provide users the ability to create application using the language of their choice to program and control their network.

COMPANY DATA	CUSTOMERS
Company Type: Public Company Size: 1,001-5,000	http://www.extremenetworks.com/customers
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Healthcare, Government & Education, Manufacturing, Data-center Deployment Location: Intra-Datacenter, Inter-Datacenter, Campus, WAN, Wired and Wireless Campus NV Classification: Overlay, Direct fabric programming, Hybrid, Underlay Southbound Protocols: OpenFlow (1.0, 1.3), OVSD	Hypervisors: ESXi, Xen, Hyper-V Orchestration Integration: OpenStack, VMware vCloud Suite Encapsulation Formats: VXLAN, GRE, MPLS, SPB QoS Support: L2 QoS, L3 QoS, L4-7 QoS via DPI Built-in Layer 4-7: L4-L7 Stateful Load balancer, Generic DPI rules Layer 4-7 Service Insertion: Rewrite capabilities (MAC, IP, VLAN), L4-L7 rule-based service chaining

Virtual Application Networks (Click for online version)<https://www.hpe.com/us/en/networking/nfv.html>**HEWLETT PACKARD ENTERPRISE**<http://www.hpe.com>

Description: HP Enterprise delivers SDN and Network Virtualization through its "Virtual Application Networks" (VAN) framework. VAN offers an end-to-end virtualization solution that, when delivered through HP's Intelligent Management Center (IMC), enables policy-based automation and orchestration for traditional networks.

COMPANY DATA	CUSTOMERS
Company Type: Public Company Size: 10,000+	Telefonica. Kettering Health Network
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail Deployment Location: Intra-Datacenter NV Classification: Hybrid Southbound Protocols: OpenFlow (1.0, 1.3), OVSD, Vendor-specific RESTful API Encapsulation Formats: VXLAN, MPLS	Hypervisors: KVM, ESXi, Xen, Hyper-V Orchestration Integration: OpenStack, VMware vCloud Suite QoS Support: L2 QoS, L3 QoS Built-in Layer 4-7: L3 Firewall, L4 Stateful Firewall, L3 Load balancing, L4-L7 Stateful Load balancer, IPS Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services

Juniper Contrail, MetaFabric Intelligent Services Edge, vSRX and vMX (Click for online version)

<http://www.juniper.net/us/en/solutions/nfv/>

JUNIPER NETWORKS, INC.

<http://www.juniper.net>

Description: Juniper's solution combines Juniper Contrail, a turnkey software cloud management system, MetaFabric, a foundation for cloud-based data centers, Intelligent Services Edge, for visibility and control of SDNs, and vSRX and vMX virtual platforms for virtualized network functions (VNFs) to securely extend to the customer premises with the NFX250 Network Services Platform.

COMPANY DATA	CUSTOMERS
Company Type: Public Company Size: 5,001-10,000	https://www.juniper.net/us/en/company/case-studies/
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom Deployment Location: Intra-Datacenter, Inter-Datacenter, WAN NV Classification: Overlay, Direct fabric programming, Hybrid Southbound Protocols: OVSDDB, XMPP-based API, Netconf	Hypervisors: KVM, ESXi, Xen, Hyper-V Orchestration Integration: OpenStack Encapsulation Formats: VXLAN, MPLS, MPLS over GRE and MPLS over UDP Built-in Layer 4-7: L3 Firewall, L3 Load balancing, DDoS prevention Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services, Load balancing across service insertion chains, L4-L7 rule-based service chaining

Midokura Enterprise MidoNet (Click for online version)

<http://www.midokura.com/midonet-enterprise>

MIDOKURA

<http://www.midokura.com/>

Description: Midokura Enterprise MidoNet is a scalable network virtualization solution designed for Infrastructure as a Service (IaaS) clouds. Operators can build isolated networks as an overlay on top of the existing hardware-based network infrastructure. MidoNet Community Edition provides distributed L2-4 networking services including L2/L3 switching, routing, NAT, firewall, load balancing, DHCP. MidoNet provides port mirroring and service chaining of network services like security and IDS.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 1-200	Auro, Blue Jeans, Colt Technology Services, Dell IT, Overstock.com
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Government & Education, Web Services, Enterprises Deployment Location: Intra-Datacenter, Inter-Datacenter, WAN NV Classification: Overlay Southbound Protocols: OpenFlow, OVSDDB Encapsulation Formats: VXLAN, GRE QoS Support: L2 QoS, L3 QoS	Hypervisors: KVM, ESXi Orchestration Integration: OpenStack, Docker, Mesos Built-in Layer 4-7: L3 Firewall, L4 Stateful Firewall, L3 Load balancing, L4-L7 Statefull Load balancer Layer 4-7 Service Insertion: Basic service chaining, chaining of virtual services, chaining of physical services, L4-L7 rule-based service chaining

NEC ProgrammableFlow Networking Suite (Click for online version)<http://www.necam.com/SDN/>**NEC**<http://www.nec.com>

Description: The NEC ProgrammableFlow Networking Suite is a comprehensive solution for datacenter and enterprise networks consisting of the ProgrammableFlow Controller, physical and virtual switches and network orchestration. NEC has more than 250 deployments of the ProgrammableFlow Network Suite worldwide, in a wide range of service provider and enterprise environments.

COMPANY DATA	CUSTOMERS
Company Type: Public Company Size: 10,000+	http://www.nec.com/en/case/sub/prdslt_p43.html
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Healthcare, Financials, Government & Education, Telecom, Retail Deployment Location: Intra-Datacenter, Inter-Datacenter, Campus, WAN NV Classification: Direct fabric programming, Hybrid Southbound Protocols: OpenFlow (1.0, 1.3) Encapsulation Formats: MLPS QoS Support: L2 QoS, L3 QoS, L4-7 QoS via DPI	Hypervisors: KVM, ESXi, Hyper-V Orchestration Integration: OpenStack Built-in Layer 4-7: L3 Firewall, L3 Load balancing Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services, Rewrite capabilities (MAC, IP, VLAN), Load balancing across service insertion chains, L4-L7 rule-based service chaining

Nuage Networks Virtualized Services Platform (VSP) (Click for online version)<http://www.nuagenetworks.net/products/virtualized-services-platform/>**NUAGE NETWORKS**<http://www.nuagenetworks.net>

Description: Nuage Networks VSP virtualizes and automates data-center network infrastructure, enabling the delivery of cloud applications across thousands of tenants, in a policy-driven manner. Nuage SDN is deployed worldwide by banks, cloud providers, and telcos today for multi-DC network virtualization as well as for enabling new models for delivering network services beyond the datacenter (SD-WAN).

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 201-500	Santander, CenturyLink, Telefonica, China Mobile, China Telecom (CTCC)
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Financials, Telecom Deployment Location: Intra-Datacenter, Inter-Datacenter, WAN NV Classification: Overlay Southbound Protocols: OpenFlow, OVSDB Encapsulation Formats: VXLAN, GRE, MPLS QoS Support: L2 QoS, L3 QoS, Customer Payload Marking, Tunnel Marking	Hypervisors: KVM, ESXi, Xen, Linux containers Orchestration Integration: OpenStack, VMware vCloud Suite, CloudStack Built-in Layer 4-7: L3 Firewall, L4 Stateful Firewall Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services, Rewrite capabilities (MAC, VLAN), L4-L7 rule-based service chaining, Redundant appliance support

PLUMgrid Open Networking Suite for OpenStack (Click for online version)

<http://www.plumgrid.com/product/overview/>

PLUMGRID

<http://www.plumgrid.com>

Description: PLUMgrid Open Networking Suite for OpenStack is a comprehensive software defined networking suite that enables secure and scalable cloud infrastructure. Built on PLUMgrid Platform and IO Visor technology, the software suite lets users create private Virtual Domains to provide isolation, security, and policy enforcement across tenants.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 51-200	Key customers are listed on our main page: http://www.plumgrid.com
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Financials, Government & Education, Telecom, Retail Deployment Location: Intra-Datacenter, Inter-Datacenter NV Classification: Overlay Southbound Protocols: IO Visor based Encapsulation Formats: VXLAN QoS Support: None	Hypervisors: KVM, ESXi Orchestration Integration: OpenStack, VMware vCloud Suite Built-in Layer 4-7: L3 Firewall, L3 Load balancing Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services, L4-L7 rule-based service chaining

Netvisor OS (Click for online version)

<http://www.pluribusnetworks.com/products/netvisor-os/>

PLURIBUS NETWORKS

<http://www.pluribusnetworks.com/>

Description: The Netvisor family of operating systems for open switches brings the ability to virtualize any number of switches to create a single networking fabric, which is provisioned and managed as if it were a single logical switch. Netvisor is a bare metal (type 1) hypervisor for open switches. It is based on a highly available, scalable, controller-less architecture to provide visibility, automation and dramatic operational simplification and cost reduction.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 51-200	Tibco, Lucera http://www.pluribusnetworks.com/about/customers/
PRODUCT DETAILS	
Customer Segments: Healthcare, Financials, Telecom, Retail Deployment Location: Intra-Datacenter NV Classification: Direct fabric programming, Hybrid Southbound Protocols: OpenFlow (1.1), OVSDB, Vendor-specific RESTful API Encapsulation Formats: VXLAN QoS Support: L2 QoS, L3 QoS	Hypervisors: KVM, ESXi Orchestration Integration: OpenStack Built-in Layer 4-7: L3 Firewall, L3 Load balancing Layer 4-7 Service Insertion: Basic service chaining, Chaining of virtual services, Chaining of physical services, L4-L7 rule-based service chaining

VMware NSX (Click for online version)<http://www.vmware.com/products/nsx/>**VMWARE, INC.**
<http://www.vmware.com>

Description: VMware NSX delivers the operational model of a virtual machine for the network. Similar to virtual machines for compute, virtual networks are programmatically provisioned and managed independent of underlying hardware enabling any network topology. NSX reproduces the entire network model in software, enabling any network topology—from simple to complex multi-tier networks—to be created and provisioned in seconds.

COMPANY DATA		CUSTOMERS	
Company Type: Public Company Size: 10,000+		DirecTV, Tribune Media, Columbia Sportswear, Novamedia, Exostar	
PRODUCT DETAILS			
Customer Segments: Healthcare, Financials, Government & Education, Retail Deployment Location: Intra-Datacenter, Inter-Datacenter NV Classification: Overlay Southbound Protocols: OpenFlow (1.0, 1.1, 1.3, 1.4), OVSDb, Vendor-specific RESTful API, XMPP-based API Encapsulation Formats: VXLAN, GRE, STT QoS Support: L2 QoS, L3 QoS		Hypervisors: KVM, ESXi, Xen Orchestration Integration: OpenStack, VMware vCloud Suite, CloudStack Built-in Layer 4-7: L3 Firewall, L4 Stateful Firewall, L3 Load balancing, L4-L7 Stateful Load balancer, IPS, Generic DPI rules Layer 4-7 Service Insertion: Chaining of virtual services, Load balancing across service insertion chains, L4-L7 rule-based service chaining	

category: ■ **open source****Astara** (Click for online version)<http://akanda.io/blog/blog-what-is-akanda/>**AKANDA**<http://www.akanda.io>

Description: Astara is the only open source network orchestration solution built by OpenStack operators for OpenStack clouds. Astara eliminates the need for complex SDN controllers, overlays and multiple plugins for cloud networking by providing a simple integrated networking stack (routing, firewall, load balancing) for connecting and securing multi-tenant OpenStack environments.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 1-50	Not Disclosed
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers Deployment Location: Intra-Datacenter, Inter-Datacenter, Campus, WAN NV Classification: Overlay, Astara/Akanda orchestrates network services on top of OpenStack Southbound Protocols: Neutron APIs Encapsulation Formats: VXLAN, GRE QoS Support: Provided by the OpenStack Neutron environment	Hypervisors: KVM, ESXi, Xen, Hyper-V Orchestration Integration: OpenStack Built-in Layer 4-7: L3 Firewall, L4 Stateful Firewall, L7 application-aware Firewall (ALG), L3 Load balancing, L4-L7 Stateful Load balancer, Pluggable driver architecture allows for maintenance of several higher level network services Layer 4-7 Service Insertion: L4-L7 rule-based service chaining

Project Calico (Click for online version)<http://www.projectcalico.org/>**METASWITCH NETWORKS**<http://www.metaswitch.com>

Description: Calico's pure L3 approach to data center networking integrates seamlessly with cloud orchestration systems (such as OpenStack) to enable secure IP communication between virtual machines, containers, or bare metal workloads.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 501-1,000	Not Disclosed
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Financials, Government & Education, Telecom, Retail Deployment Location: Intra-Datacenter NV Classification: Non-overlay virtual networking Southbound Protocols: Vendor-specific RESTful API, BGP Encapsulation Formats: None in normal operation. Optional IP-in-IP	Hypervisors: Not Disclosed Orchestration Integration: OpenStack, Docker, Mesos, Brooklyn, Kubernetes, Clocker, Rkt QoS Support: L3 QoS Built-in Layer 4-7: L3 Firewall, L4 Stateful Firewall Layer 4-7 Service Insertion: Any IP addressed service can be inserted into a Calico fabric.

category: ■ **open source****Virtual Tenant Network (VTN)** (Click for online version)<https://wiki.opendaylight.org/view/>

OpenDaylight_Virtual_Tenant_Network_(VTN):Overview

OPENDAYLIGHT<https://www.opendaylight.org>

Description: OpenDaylight delivers a common SDN platform, which many regard as the industry's de facto standard. OpenDaylight Virtual Tenant Network (VTN) is an application that provides multi-tenant virtual networks on an SDN controller.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 201-500	https://www.opendaylight.org/user-stories/
PRODUCT DETAILS	
Customer Segments: Primarily focused as open source code that can be leveraged by companies who offer their own solutions, applications, services, casting and support. Deployment Location: Intra-Datacenter, Inter-Datacenter, WAN NV Classification: Overlay Southbound Protocols: OpenFlow, Vendor-specific RESTful API	Hypervisors: VTN is built on top of Open Daylight, support of hypervisors not relevant. Orchestration Integration: OpenStack Encapsulation Formats: VXLAN QoS Support: L2 QoS, L3 QoS Built-in Layer 4-7: Not Applicable Layer 4-7 Service Insertion: Basic service chaining

Open Virtual Network (Click for online version)<http://openvswitch.org/support/slides/OVN-Vancouver.pdf>**OPEN VSWITCH**<http://openvswitch.org>

Description: OVN is an expansion to Open vSwitch and will integrate with existing Open vSwitch components. It is a new network virtualization project that brings virtual networking to the Open vSwitch user community. It is being developed by the core OVS team. OVN will support the same container and virtual machine environments as OVS, including KVM, Xen, and Hyper-V. OVN will include logical switches and routers, security groups, and L2/L3/L4 ACLs, implemented on top of a tunnel-based overlay network.

COMPANY DATA	CUSTOMERS
Company Type: Private Company Size: 1-50	Not Disclosed
PRODUCT DETAILS	
Customer Segments: Cloud Service Providers, Part of the OpenStack and Open vSwitch platforms. Deployment Location: Intra-Datacenter NV Classification: Overlay Southbound Protocols: OpenFlow, OVSDBI Encapsulation Formats: VXLAN, GRE, NVGRE, STT QoS Support: L2 QoS, L3 QoS	Hypervisors: KVM, Xen, Hyper-V Orchestration Integration: OpenStack, CloudStack Built-in Layer 4-7: L3 Firewall, L3 Load balancing, Generic DPI rules. While OVS can do some L4-7 services, OVN is L2/L3 only. Layer 4-7 Service Insertion: While OVS can do some L4-7 services, OVN is L2/L3 only

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