The 2015 Guide to SDN and NFV

Executive Summary

By Dr. Jim Metzler, Ashton Metzler & Associates
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Platinum Sponsors:

Gold Sponsors:

Produced by:

Executive Summary

Software Defined Networking (SDN)

Introduction

This e-book is based in part of two surveys that were administered in September and October of 2014. One of the surveys focused on SDN and the other on NFV. Throughout this executive summary, the respondents to those surveys will be referred to respectively as The SDN Survey Respondents and The NFV Survey Respondents.

The responses to the SDN survey indicated that the general familiarity with SDN has increased significantly over the last year and that while the percentage of IT organizations that have implemented SDN in production is still small, it has increased somewhat significantly over the last year. The SDN Survey Respondents also indicated that the percentage of IT organizations who have SDN in production will likely increase somewhat over the next year, but the percentage will remain small.

The e-book identified a number of changes that have occurred with SDN over the last year. One thing that has changed is that most of the discussion around whether or not an overlay network virtualization solution is indeed SDN has gone away. Today, most IT professionals regard an overlay solution as being a form of SDN. The e-book discusses the pros and cons of the overlay and the underlay SDN models and presents market research that indicates that by a small margin that The SDN Survey Respondents believe that the underlay model will provide more value over the next two years.

Another change that has occurred in the SDN landscape within the last year is that the Open Networking Foundation (ONF) established the Northbound Interface (NBI) working group with the goal of eventually standardizing SDN's northbound interface. Sarwar Raza, the chairman of the working group, is quoted as saying that standardization was not a short term goal of the group and that "Our goal in the next year is to formalize the framework along with the information and data models and then iterate some with code before we even start a standards discussion." The NBI working group intends to work with one or more open source initiatives to develop working code for the NBIs and the group aims to work on standardization at an appropriate time in the future.

Another change in the SDN landscape that is discussed in the e-book is that in February 2014 the OpenDaylight community issued its first software release, called Hydrogen and in September 2014 issued its second software release called Helium. A number of vendors have announced their intention to use the OpenDaylight solution as the basis of their SDN controller. This creates the potential for SDN solutions based on OpenDaylight solutions to reach critical mass in the near term and hence accelerate the adoption of SDN.

The majority of The SDN Survey Respondents indicated that they thought that SDN and NFV are complimentary activities and a quarter of the respondents indicated that they thought that in at least some instances that NFV requires SDN. That second school of thought is in line with the ONF who in March of 2014 published a white paper that included uses cases that the ONF believes demonstrate how OpenFlow-enabled SDN can meet the need for automated, open, and programmable network connectivity to support NFV.

SDN Use Cases

The SDN Survey Respondents indicated that a wide range of factors were driving their interest in SDN including the desire to better utilize network resources and to perform traffic engineering with an end-to-end view of the network. However, very few of the respondents indicated that they thought that SDN would help them reduce CAPEX or reduce complexity. The SDN Survey Respondents also indicated that a wide range of factors were inhibiting their interest in SDN. Some of the inhibitors to SDN adoption, such as the immaturity of current products and the immaturity of enabling technologies, will naturally dissipate over time. However some of the key inhibitors, such as the lack of a compelling business case, need to be addressed or they will continue to impede SDN adoption.

The SDN Survey Respondents indicated that over the next two years that the primary focus of their SDN deployment will likely to be in the data center. However, they expressed considerable interest in deploying SDN in the WAN as well as in branch and campus networks. In addition, when asked to look forward three years, The SDN Survey Respondents indicated that three years from now that they will have deployed SDN pervasively in their data centers and that they will also have made significant SDN deployment both in their WAN and in their campus networks.

The e-book discussed a number of SDN use cases. The WAN use case that was discussed was how Google has deployed SDN to connect its data centers and as a result of that deployment, has driven its network utilization to 95%. The campus use cases that were discussed were:

- Dynamic QoS and traffic engineering;
- Unified wired and wireless networks;
- QoS management for Microsoft Lync across wired and wireless networks;
- Personal Bonjour;
- Roll based access.

The data center use cases that were discussed were:

- Virtual machine migration;
- Service chaining;
- Security services;
- Load balancer services;
- Software defined clouds;
- Cloud hosting.

The Operational Implications

Thirty five percent of The SDN Survey Respondents indicated that SDN will enable them to implement more effective security functionality and 12% of The SDN Survey Respondents indicated that concerns about possible security vulnerabilities is a significant inhibitor to SDN deployment. As the e-book discusses, one of the ways that SDN can enhance security is by implementing security services on OpenFlow-based access switches that can filter packets as they enter the network. Another such example is role based access that is implemented by deploying a role-based resource allocation application that leverages the control information and capability of the SDN controller.

The e-book discuses some of the security challenges including:

- The centralized controller emerges as a potential single point of attack and failure that must be protected from threats.
- The southbound interface between the controller and underlying networking devices is vulnerable to threats that could degrade the availability, performance, and integrity of the network.

The e-book describes OpenStack and points out that orchestration engines such as OpenStack are important to both SDN and NFV. As explained in the e-book, in conjunction with the orchestration engine, the role of the SDN controller is to translate the abstract model created on the orchestration engine into the appropriate configuration of the virtual and physical resources that will deliver the desired service. For example, the orchestration engine can instruct the controller to perform a variety of workflows including

- Create a VM;
- Assign a VM to a Virtual Network (VN);
- Connect a VM to an external network;
- Apply a security policy to a group of VMs or a VN;
- Attach Network Services to a VM or chain Network Services between VMs.

In spite of the importance of orchestration, only a small minority of The SDN Survey Respondents indicated that their organization had a well thought out strategy for how they would do orchestration.

Similar to the situation with security, the e-book shows how management is a double edged sword. Fifty three percent of network organizations believe that SDN will ease the administrative burden of management tasks such as configuration and provisioning while 13% of network organizations believe that concerns about how to manage SDN is a significant inhibitor to SDN deployment.

The e-book highlights the fact that in SDN environments the challenges associated with end-to-end service performance management are more demanding than they are in traditional network environments. Some of the reasons for that are that in an SDN environment:

- The combination of physical and virtual infrastructure and dynamically changing resources requires a more holistic approach to instrumentation, consolidation of individual datasets, and analysis of the consolidated dataset in a service contextual fashion.
- The SDN controller needs to be instrumented and monitored just as any other application server and the southbound protocol needs to be monitored the same way as any other protocol.
- Network management organizations need tools that enable them to be able to dynamically discover, procure, allocate and reconfigure resources.
- Network management organizations need to be able to perform a two-way mapping between an application or service and all of the virtual services that support it and they must be able to perform a two-way mapping between the virtual services that support a given service or application and the physical infrastructure that supports them.

The e-book positions SDN as being a part of a broader movement to implement all IT functionality in software, referred to as Software Defined Everything (SDE) and points out that the adoption of an SDE approach is causing the role of network and IT infrastructure professionals to change. Some of the key characteristics of the emerging roles are:

- An increased knowledge of other IT disciplines;
- More focus on setting policy;
- More knowledge of the business;
- More understanding of applications;
- More emphasis on programming.

The Survey Respondents were asked how they thought that the SDE movement would likely impact their organization. Their answers included:

- A likely re-org around application development and network operations;
- An increase in cross functional teams and projects;
- Moving from a tower based organization to a DevOps model;
- An increased focus on software engineering;
- Team work will involve an enhanced mix of skills including programming, networking, virtualization and DevOps.

The Survey Respondents were also asked how they thought told that the SDE movement would likely impact their jobs. Their answers included:

- The way to design, implement and troubleshoot networks will change a lot;
- The job will require new skill sets in general and more programming knowledge in particular;
- There will be new security requirements;
- New architectures will need to be developed;
- There will be a lot of re-training and re-trenching.

Network Functions Virtualization (NFV)

Introduction

NFV is being driven by a number of different types of players who are described in the e-book. This includes industry organizations such as the TM Forum and ETSI, open source communities such as OPNFV and traditional standards development organizations such as IETF.

As described in the e-book, early in 2014 the TM Forum announced its Zero-touch Orchestration, Operations and Management (ZOOM) project. According to the Forum, the goal of Zoom is to define a vision of the new virtualized operations environment and a management architecture based on the seamless interaction between physical and virtual components that can easily and dynamically assemble personalized services. As of November 2014, the ZOOM team has delivered an assessment of how virtualization impacts SLAs and is currently working on information and policy models, NFV preparedness, and a set of operational support system (OSS) design principles needed for NFV adoption to become widespread.

The ETSI NFV ISG has identified nine NFV use cases and is currently driving 25 POCs. The ETSI NFV ISG was established with a two year life span that expires in January 2015. In late July and early August 2014 the NFV ISG met in Santa Clara, CA. At that meeting the primary objectives of NFV Phase 2 were identified. Whereas ETSI characterizes Phase 1 as being the Requirements Phase, ETSI characterizes Phase 2 as being the Implementation Phase. The objectives of Phase 2 include building on the achievements that were made in the first two years of the ISG and consist of an enhanced focus on interoperability, formal testing, as well as working closer with projects developing open source NFV implementations. In addition, the NFV ISG also released nine draft NFV documents for industry comments and published a publically available document that summarizes the key concepts that are contained in those documents.

In September 2014 the Linux Foundation announced the founding of the Open Platform for NFV Project (OPNFV). As part of the announcement the Linux Foundation declared that OPNFV will establish a carrier-grade, integrated, open source reference platform that industry peers will build together to advance the evolution of NFV and ensure consistency, performance and interoperability among multiple open source components. The Foundation also stated that because multiple open source NFV building blocks already exist, OPNFV will work with upstream projects to coordinate continuous integration and testing while filling development gaps.

Although their efforts are just getting started, the IETF can be expected to play a significant role in the evolution of standards for SDN and NFV. For example, the IETF Service Function Chaining (SFC) Work Group (WG) currently has over forty active Internet drafts on the topic of delivering traffic along predefined logical paths incorporating a number of service functions. As described in one of those Internet drafts, the basic concept of SFC is similar to ETSI NFV ISG's Virtualized Network Function (VNF)-Forwarding Graphs.

In spite of the fact that the vast majority of The NFV Survey Respondents believe that NFV is applicable in both an enterprise and a service provider environment, only a modest number of IT organizations have implemented NFV in a production network. However, driven primarily by the belief that NFV will enable them to reduce the amount of time it takes to deploy new services, a large percentage of IT organizations are currently in varying stages of analyzing NFV.

The NFV Survey Respondents indicated that the primary impediments that would keep their organization from broadly implementing NFV are:

- Concerns about end-to-end provisioning;
- The lack of a compelling business case;
- The immaturity of the current products.

Use Cases and Proof of Concept (POC)

The e-book discusses some of the use cases and POCs being sponsored by ETSI and by the TM Forum. The ETSI use cases are:

- NFV Infrastructure as a Service (NFVIaaS)
  NFVIaaS is analogous to a cloud IaaS that is capable of orchestrating virtual infrastructures that span a range of virtual and physical network, compute, and storage functions.

- Virtual Network Functions as a Service (VNFaaS)
  Many enterprises are deploying numerous network service appliances at their branch offices; e.g., access routers, WAN optimization controllers, stateful firewalls and intrusion detection systems. Virtual Network Functions delivered as a Service (VNFaaS) is an alternative solution for enterprise branch office networks whereby VNFs are hosted on servers in the network service provider's access network PoP.

- Virtualization of the Home Environment (VoHE)
  Virtualization of the Home Environment is analogous to VNFaaS. In this case the residential gateway (RGW) and the set top box (STB) are virtualized as VNFs residing on servers in the network service provider's PoP.

- VNF Forwarding Graph (FG)
  IT organizations need to be able to orchestrate and manage traffic flows between virtualized service platforms (e.g., VNFs) and physical devices in order to deliver a complete service to the end user.

  The VNF Forwarding Graph (VNF FG) is a service that provides flow mapping (a.k.a., service stacking or chaining) from a management and orchestration system that may or may not be part of an SDN infrastructure.

- Virtual Network Platform as a Service (VNPaaS)
  VNPaaS is similar to an NFVIaaS that includes VNFs as components of the virtual network infrastructure. The primary differences are the programmability and development tools of the VNPaaS that allow the subscriber to create and configure custom ETSI NFV-compliant VNFs to augment the catalog of VNFs offered by the service provider.

- Virtualization of Mobile Core Network and IP Multimedia Subsystem
  The 3GPP is the standards organization that defines the network architecture and specifications for Network Functions (NFs) in mobile and converged networks. Each NF typically is run on a dedicated appliance in the mobile network PoP. Running the NFs as VNFs on virtualized industry standard servers is expected to bring a number of benefits in terms of CAPEX, OPEX, as well as flexibility and dynamic scaling of the network to meet spikes in demand.

- Virtualization of the Mobile Base Station
  3GPP LTE provides the Radio Access Network (RAN) for the Evolved Packet System (EPS). There is the possibility that a number of RAN functions can be virtualized as VNFs running on industry standard infrastructure.

- Virtualization of Content Delivery Networks (CDNs)
  Some ISPs are deploying proprietary CDN cache nodes in their networks to improve delivery of video and other high bandwidth services to their customers. Cache nodes typically run on dedicated appliances running on custom or industry standard server platforms. Both CDN cache nodes and CDN control nodes can potentially be virtualized.

- Virtualization of Fixed Access Network Functions
  NFV offers the potential to virtualize remote functions in the hybrid fiber/copper access network as well as PON fiber to the home and hybrid fiber/wireless access networks. In a DSL access network some of the functions that can potentially be virtualized include the DSLAM and Message Display Unit (MDU) forwarding functions, while control functions remain centralized at the central office.

The POCs that are being driven by the TM Forum that are discussed in this e-book are:

- Closing the Loop: Data-driven network performance optimization for NFV & SON
  In this context closing the loop means collecting and analyzing data to identify how the network can be optimized and then implement those changes. This POC showed how network operators can use Self-Organizing Networks (SON) and Network Functions Virtualization (NFV) in tandem to automate closing the loop and improve performance for customers.

- CloudNFV: Dynamic, data-driven management and operations Catalyst
  This POC builds on TM Forum's Information Framework to create a meta-data model using *active virtualization*, a term coined by the CloudNFV™ consortium. The specific challenge this POC is addressing is that without these connections, services like dynamic quality of service likely won't work at scale.

- Orchestrating Software-Defined Networking (SDN) and NFV while Enforcing Service Level Agreements (SLAs) over Wide Area Networks (WANs)
  One set of challenges that this POC addressed are the challenges that service providers face when offering private clouds to enterprises and managing SLAs in a virtualized environment. Another set of challenges are the challenges that geographically diversified enterprises encounter when integrating data centers.

- Service bundling in a B2B2X marketplace
  This POC showed how a buyer can bundle a collection of services sourced from different suppliers and deliver them seamlessly to a customer in a business-to-business or business-to-business-to-consumer arrangement. These components could include traditional network access products, as well as NFV and infrastructure-as-a-service products.

The Operational Implications

The majority of The NFV Survey Respondents indicated that they believe that even if a NFV-related POC is successful, it will take between a significant and a tremendous amount of effort to broadly implement that solution in production. One of the operational challenges that can make it difficult to move from POC to production is performance. As discussed in the e-book, in order to move VNFs into production, it must be possible to achieve the same or greater performance in a software-based environment as is possible in a traditional hardware-based environment. However, that isn't possible without an enabling software architecture because of the bottlenecks that are associated with the hypervisors, virtual switches and virtual machines that are the foundation of the emerging software-based approach to IT.

The adoption of NFV poses a number of other significant challenges that must be overcome in order to ensure the ability to continue to implement effective end-to-end management. These challenges include:

- **Dynamic relationships between software and hardware components.** With NFV, software running on virtual machines (VMs) can readily be moved among physical servers or replicated to run on newly created VMs in order to dynamically maintain availability, expand/shrink capacity, or balance the load across physical resources.

- **Dynamic changes to physical/virtual device configurations.** To accommodate the dynamic nature of virtualized networks, end-to-end management systems will need to be able to adjust the configuration of devices to react to changing conditions in the network.

- **Many-to-Many relationships between network services and the underlying infrastructure**. In a virtualized infrastructure a network service can be supported by a number of VNFs which may be running on one or several VMs. A single VNF may also support a number of distinct network services. In addition, the group of VNFs supporting a single network service could possibly be running on a number of distinct physical servers.

- **Hybrid physical/virtual infrastructures.** As virtualization is gradually adopted, service providers will need to be able to integrate virtual environments into their existing end-to-end traditional/legacy monitoring infrastructures.

- **Network services spanning multiple service providers.** Some of the VNFs comprising a virtualized network service may be hosted in the clouds of multiple collaborating providers.

- **IT and Network Operations collaboration.** These organizations will need to cooperate effectively to establish new operational processes that meet the demands of end-to-end management of hybrid physical/virtual infrastructures.

Roughly a third of IT The NFV Survey Respondents believe that over the next two years that the adoption of NFV is likely to have a significant or very significant impact on the structure of their organization. When asked what type of changes they expected, a number of The NFV Survey Respondents commented that it would require them to change how they implemented SLAs, how they developed a business case and it would cause them to rethink their business models. Other comments included:

- We will need to adopt a new approach to service provisioning and management;

- It will cause us to consolidate our physical platforms;
- It will change how we do network planning;
- We will need to determine how we are going to orchestrate end-to-end systems.

Almost half of The NFV Survey Respondents indicated that over the next two years that the adoption of NFV will likely have a significant or very significant impact on the skill base of IT professionals. When asked to indicate the type of impact, the answers included:

- We will need to know multiple technologies;
- We will need to think in software and end-to-end terms rather than in component terms;
- It will require the skills to drive the integration between legacy equipment and management systems and NFV management systems;
- We will need to modify our change management, incident and problem management processes.

An additional hurdle that has to be overcome before the full benefits of NFV can be realized is that IT organizations must take a DevOps-like approach to network operations. The e-book describes the key principles that characterize DevOps and also describes how a DevOps approach has to be modified in order to be applied to network operations.

The SDN and NFV Ecosystem

The e-book identifies the primary classes of vendors that either currently do, or can be expected to provide either parts or all of a SDN solution. Included in the discussion is the value proposition of this class of vendor as well as a set of representative vendors. The classes of SDN vendors included in the e-book are:

- Merchant Silicon/Chip Vendors;
- HyperScale Data Centers;
- Telecom Service Providers;
- Switch Vendors;
- Network and Service Monitoring, Management and Automation;
- Providers of Network Services;
- Testing Vendors and Services;
- Standards Bodies and Related Communities;
- Providers of SDN Controllers;
- Providers of Telcom Service Provider's Infrastructure/ Optical Networking;
- Server Virtualization Vendors.

The e-book also identifies the primary classes of vendors that either currently do, or can be expected to provide either parts or all of a NFV solution. Included in the discussion is the value proposition of this class of vendor as well as a set of representative vendors. The classes of NFV vendors included in the e-book are:

- Telecom Service Providers;
- Merchant Silicon/Chip Vendors;
- Network Systems and Electronic Equipment Vendors;
- Virtualized Network Service and Cloud Service Vendors;
- SDN Controller Software Vendors;
- NFVI Providers;
- Orchestration Software Vendors;
- Network Monitoring, Management and OSS/BSS Vendors;
- Hypervisor Vendors;
- Test Equipment Vendors and Test Services;
- Standards Bodies and Related Communities.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

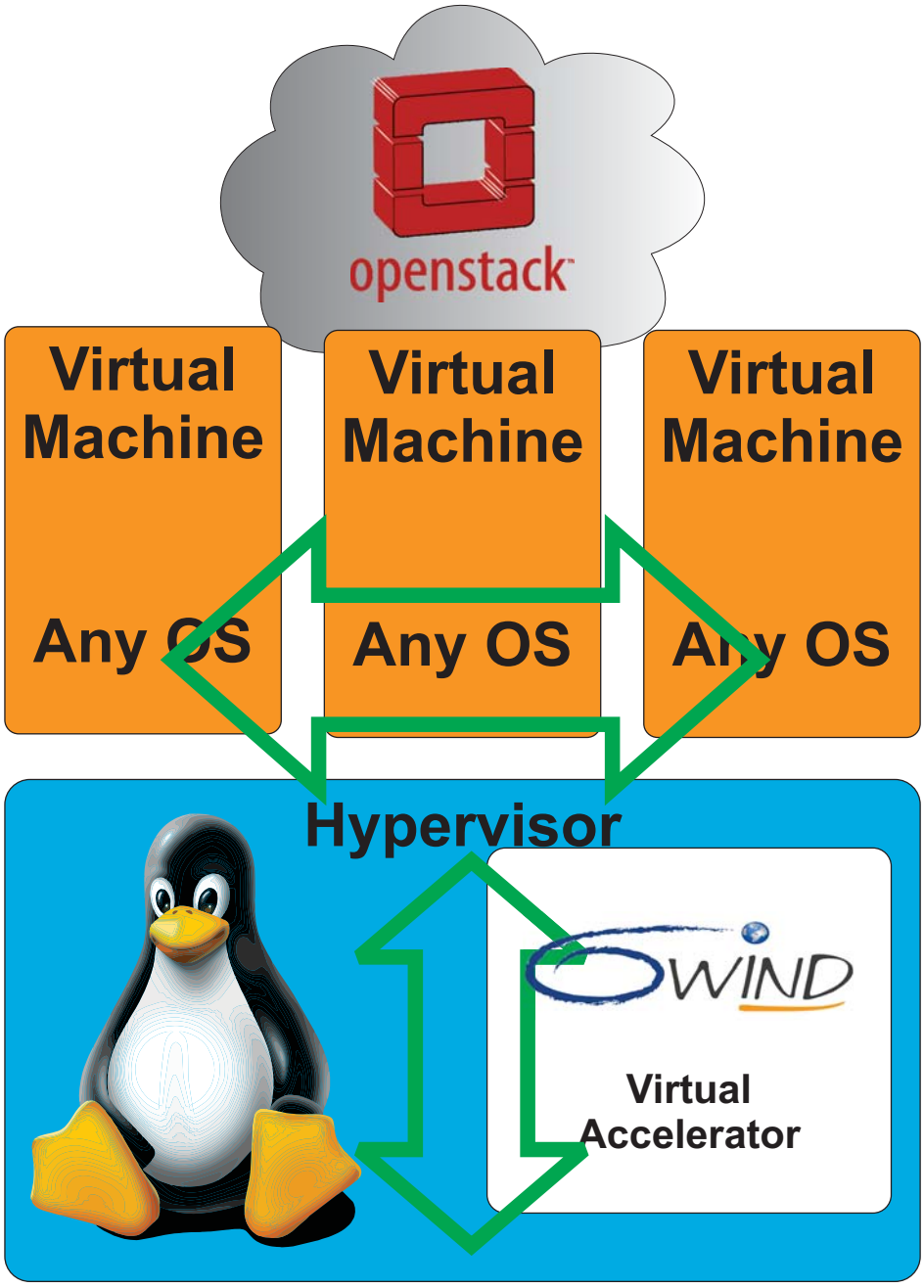
For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
Steven Taylor

6WIND Virtual Accelerator

Enable NFV And Virtual Networking



Transparent OpenStack orchestration support

High bandwidth for VM performance, density and communications

Complete virtual networking infrastructure

Support for Open vSwitch and Linux Bridge with no modifications

Network hardware independence for seamless hardware upgrades

6WIND

Wire Speed Virtual Switching
From Common Hardware

www.6WIND.com

AUTOMATE YOUR CLOUD WITH aCLOUD SERVICES ARCHITECTURE

Integrate dynamic services into your Cloud Data Center

www.a10networks.com

Dynamic Cloud, Dynamic Services

Service providers are on a journey to the cloud. Network function virtualization (NFV) and software-defined networking (SDN), when fully implemented, will create highly dynamic networks with an unprecedented level of scale, resiliency and programmability.

The result will be new dynamic services, where the network adapts to users' demands, rather than limits what the user can do. These new services promise to be more flexible and offer a better user experience. However, for service providers to remain viable businesses, it is critical that the migration to this new architecture does not disrupt existing services, and the new services do not cost more to deliver than users are willing to pay.

Alcatel-Lucent and Bell Labs have been with you on this journey from the beginning. From the first telephone, to the invention of the transistor, from the earliest digital telephone systems and cellular networks to today's advanced IP/optical and LTE networks, we have been the industry's leading pioneers. We are also an early leader in adapting cloud technologies to the telecom world, and we have the key solutions to get you started on the next stage of your journey.

The NFV Journey

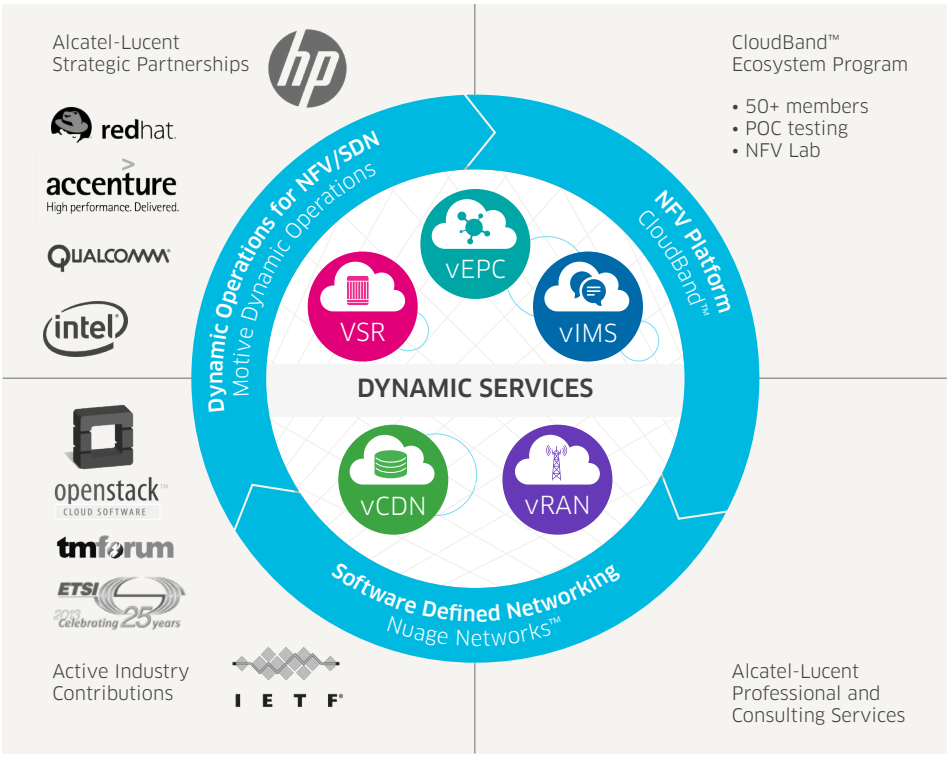
NFV is the start of a multi-year journey; a journey that is being made possible as a result of many technical advances coming together simultaneously. The journey to a fully operational NFV network requires the coordination of three interlinked but separate development paths: virtualization, orchestration and automation. Balancing the investments a service provider allocates to each path has much to do with where they start and their strategy. No path should be considered in isolation.

1. Virtualization

The abstraction of the Telecom functions software from dedicated hardware to run on open commercial-off-the-shelf (COTS) hardware, as well as the need to balance performance and cost reductions, will force service providers to make critical roadmap decisions. Some functions will achieve significant advantages of scale and flexibility from COTS hardware, while other functions, or even the same function, may benefit from the performance advantages of dedicated hardware. This duality is likely to exist for a while, as we pass through a transition phase, but this should not complicate the operational model, provided the same management entities exist. While exact feature parity may not be critical, function performance and robustness cannot be compromised. Service providers should consider the many years of feature development put into the existing functions, and consider carefully how this work will be carried forward into the new mode.

While virtualization of the function is one activity on the path to full NFV, consideration must also be given to how the function will scale. Initially scaling may happen manually, but ultimately, it should be fully automated. Scale and distribution will drive a need for tight inter-virtual machine (VM) communication, and this must be achieved without performance impact.

Alcatel-Lucent's uniquely open approach and ecosystem



The path to full NFV may follow a number of steps as systems evolve:

1. Virtualized software running in a static mode on a defined COTS hardware and software build
2. Virtualized software functions on any COTS or other specialized virtual servers with manually triggered scaling
3. Full cloud implementation with auto scaling, resiliency and open APIs that enable dynamic service activation by third parties, including control of core network functions

When making a decision on which step to take first, the end game should be in sight or it may delay other decisions later on.

2. Orchestration

The orchestration and management of virtual machines needs to be done differently in a telecom network than a typical IT data center. Whether the service provider is offering a mobile app or real-time voice within a Web app (WebRTC) there will be many software routines all interconnected and sharing data across internal and external APIs. Each software module is uploaded onto a virtual machine image within a server. As a result, the telecom domain requires many thousands of virtual machines, which for reasons of resiliency and SLA integrity may be widely distributed. Managing the distribution to assure service performance requires a higher degree of orchestration.

The orchestrator automates the process of preparing and tracking virtual machines within the service provider's network. Each telecom function requires a different virtual machine setup and configuration. Through templates and recipes the orchestrator knows the configuration required to support each application. When a new function and/or more capability is required, an available virtual machine will be located and made available with the correct configuration.

The orchestrator is responsible for the lifecycle management of the virtual machine and its hosted function, including the creation of VM profiles and a wide variety of other functions. A horizontally scalable VNF management function enables the NFV platform to be set up as a Carrier Platform as a Service (CPaaS). The industry still needs to converge on a common scripting tool to create the VNF profiles. The Topology and Orchestration Specification for Cloud Applications (TOSCA) is considered a front-runner.

Quality of service metrics must also be standardized to ensure that when application performance is measured and monitored the performance is considered against a consistent metric and appropriate actions are taken to improve the metric.

3. Automation

As NFV scales, the operator must simultaneously manage the underlying network infrastructure. To do this cost effectively, it is necessary to automate the network to ensure it is in step with application demand. This is the role of SDN.

SDN is currently deployed in data centers where an overlay control layer is proving critical to meet the networking demands of the rapidly rising number of virtual machines. In these deployments, SDN ensures that network connections can be made as fast as the virtual machines within a server are created. The adoption of cloud computing within telecom networks additionally brings much shorter service lifecycles combined with increased application mobility. For typical telecom services, the location of the host for a service can move very rapidly. Thus the wide area network (WAN) environment is more dynamic than in data-center applications.

Adoption of SDN within the WAN will improve the resource and capacity utilization of the network by automating adjustments based on real-time usage. A fully dynamic network will be achieved by implementing NFV and SDN on top of a converged and programmable IP/optical network fabric to scale and automate application and service performance when and where it's needed.

Alcatel-Lucent has already developed the pieces, partners and ecosystem that operators will need to start down these three interconnected paths. We offer best of breed solutions for the different layers of NFV, using industry-supported open platforms and standards that avoid vendor lock-in. Our professional services organization operates a fully featured test bed environment where our partners, ecosystems of developers and service provider customers can ensure the continuity and resilience that real world deployments will demand.

Find out how we can help you on your journey to virtualization: **www.alcatel-lucent.com/solutions/cloud**

CloudBand

The industry reference NFV platform, CloudBand is a management and orchestration platform for open and massive distribution of virtualized telecom functions. With more than 30 customer trials, including most Tier 1 operators, CloudBand also has over 50 ecosystem members who share experiences, as well as implement and test services.

Virtualized Service Routing

The Alcatel-Lucent Virtualized Service Router (VSR) is a highly flexible, virtualized IP edge router optimized for x86 server environments. The VSR delivers a broad and rich set of virtualized IP edge applications and services. It is built to deliver high performance and elastic scalability, and enables rapid service innovation, extends service reach, opens new markets, and accelerates time to market while lowering operating costs with a homogenized physical infrastructure.

Virtualized IMS

The full portfolio of Alcatel-Lucent IMS solutions is now virtualized and commercially available. It has complete feature parity with native solutions, including the same committed SLAs, OpenStack with HEAT support today, migrating to TOSCA. New service innovations beyond VoLTE are enabled by our IMS APIs and WebRTC in partnership with leading application developers.

Virtualized IP Mobile Core

Alcatel-Lucent has virtualized the IP Mobile Core, including gateways, management, policy and charging, subscriber management and element and network management. It is a proven solution, widely deployed and fully supportive of 2G, 3G and LTE Mobile Core features. Deployed and tested in many NFV trials in conjunction with IMS, it has demonstrated tangible benefits for VoLTE.

Nuage Networks SDN

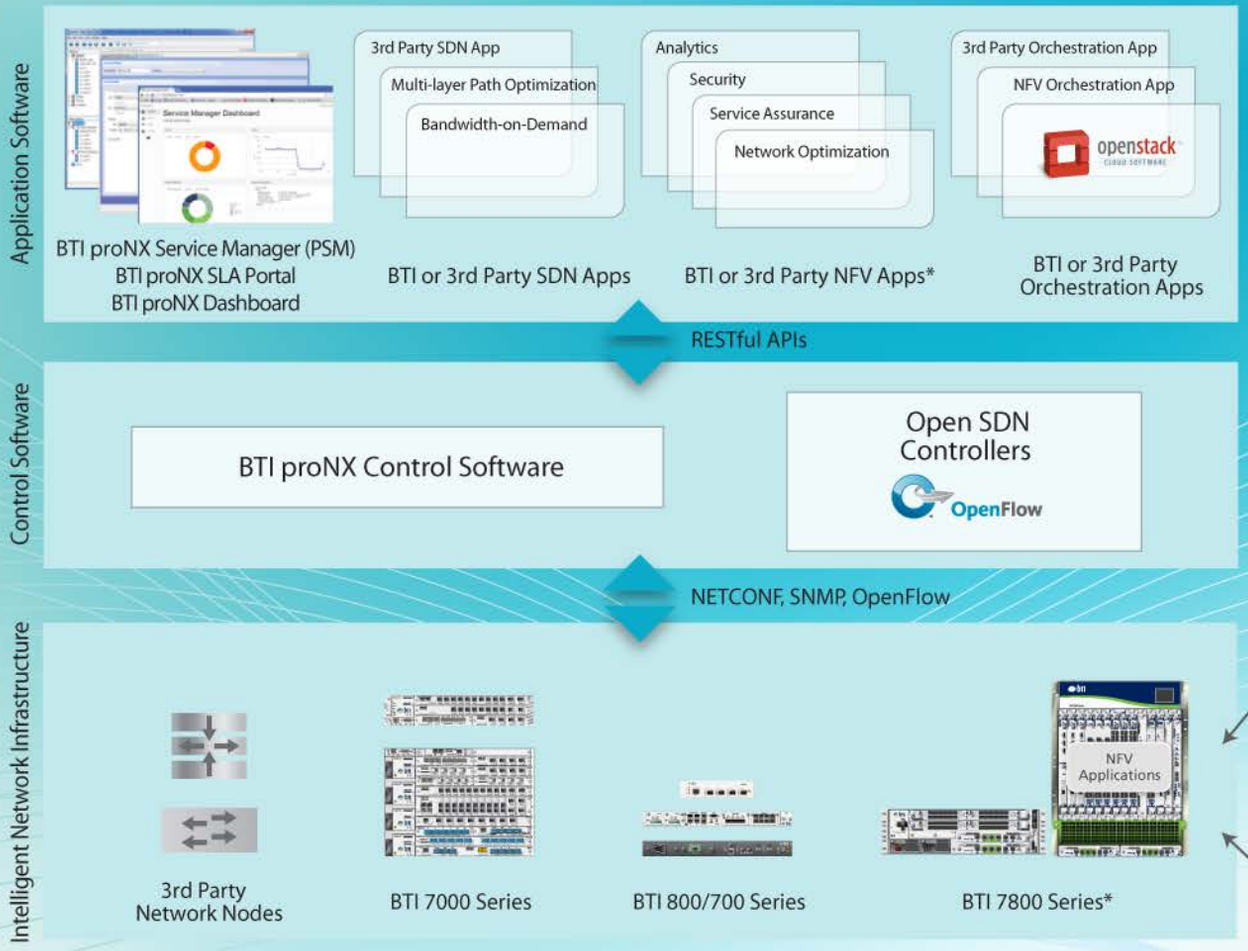
Nuage Networks is a leader in SDN. It focuses on modern datacenter requirements for multi-tenancy, full-featured routing and security at scale. The Nuage Networks platform transforms the physical network into a simple to manage, rack-once and wire-once, vendor-independent IP backplane. As a result, network resources within and across datacenters can be treated as an elastic resource pool of capacity that can be consumed and re-purposed on demand.

Motive Dynamic Operations

The new OSS for SDN and NFV, the Motive Dynamic Operations suite brings Motive's rich history with customer experience solutions to the management of SDN automation and NFV abstraction, as well as analytics and professional services – all designed to address different, critical touch points in the relationship between communications service providers and their customers.

Alcatel·Lucent

BTI's SDN & NFV Solutions

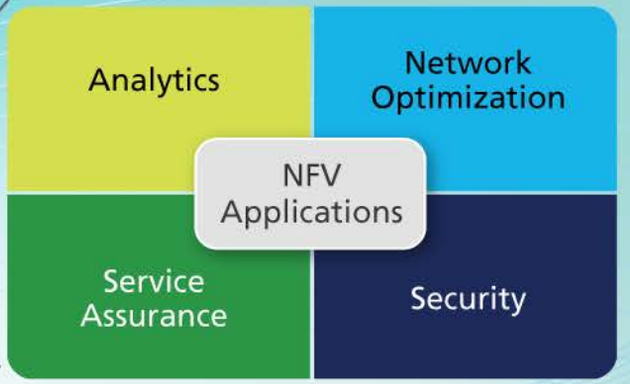


*Note: NFV Applications scan operate on the BTI 7800 Series [x.86/Linux] Applications Blade

BENEFITS:

- Open, standards-based
- End-to-end visibility & control
- Improved efficiencies & utilization
- Increased scale & performance
- Rapid service innovation
- Reduced opex

Component	BTI Applications Blade Options
CPU	x.86 options based on application specification



BTI Systems, Inc.

Corporate Headquarters
1000 Innovation Drive, Suite 200
Ottawa, Ontario K2K 3E7 Canada

US Headquarters
One Monarch Drive, Suite 105
Littleton, MA 01460 USA

btisystems.com

Cisco ACI: An Application Centric Approach to SDN

IT Trends and the Advent of Software Defined Networking

IT departments and lines of business are looking at cloud automation tools and software-defined networking (SDN) architectures to accelerate application delivery, reduce operating costs, and increase business agility. The success of an IT or cloud automation solution depends largely on the business policies that can be carried out by the infrastructure through the SDN architecture.

The emergence of SDN promised a new era of centrally managed, software-based automation tools that could accelerate network management, optimization, and remediation. Gartner has defined SDN as "a new approach to designing, building and operating networks that focuses on delivering business agility while lowering capital and operational costs." (*Source: "Ending the Confusion About Software-Defined Networking: A Taxonomy",* Gartner, March 2013)

The Cisco Application Centric Infrastructure (ACI) architecture, Cisco's expanded vision of SDN that encompasses the entire data center infrastructure, supports a more business-relevant application policy language than alternative software overlay solutions or traditional SDN designs. What makes the Cisco SDN policy model application-centric? And what are the benefits? First we need a comparison of ACI to traditional SDN designs.

A Comparison of ACI to Traditional SDN Architectures

Although traditional SDN and Cisco ACI have important differences, both have essentially the same architectural components and concepts for policy-based IT infrastructure automation:

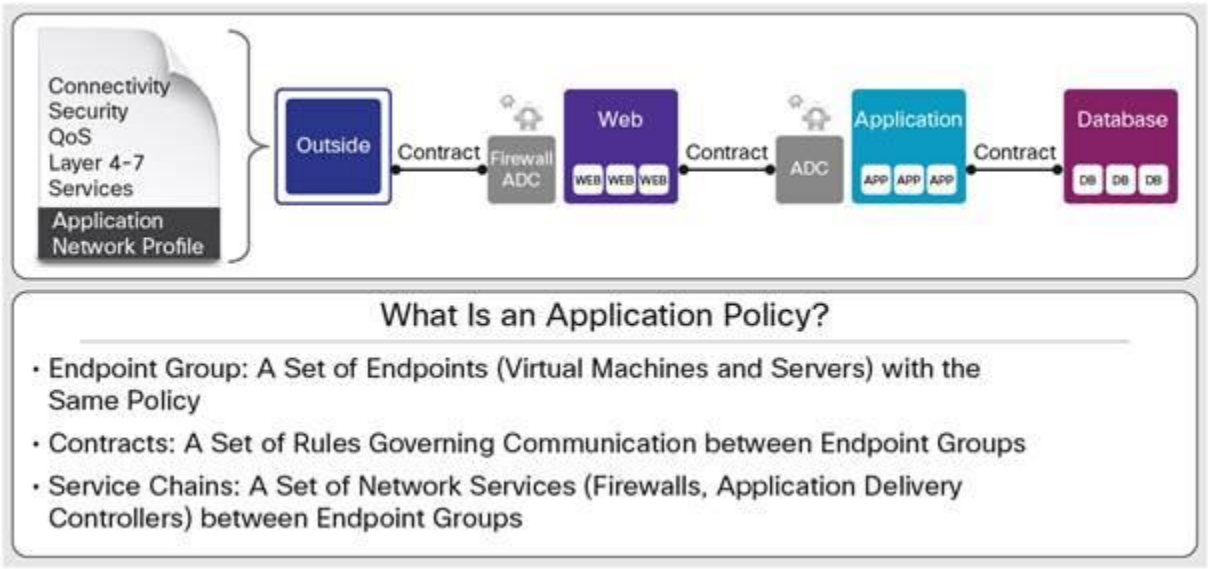
- A centralized policy store and infrastructure controller: In SDN and Cisco ACI, this feature is generally known as the controller (Cisco Application Policy Infrastructure Controller [APIC] for Cisco ACI).
- Programmable, or automated, network devices: All infrastructure devices, such as switches, application delivery controllers and firewalls, must be able to respond to and implement policies according to commands from the controller. This feature may involve agents running on the device, APIs in the devices themselves, or management hooks to the devices that are implemented in the controller.
- A controller southbound protocol to communicate with the managed or controlled devices and to communicate policy information: Initially, the OpenFlow protocol was used in SDN architecture, and vendors released OpenFlow-compliant switches. In Cisco ACI, OpFlex is the primary protocol used, although other mechanisms for integrating devices into the Cisco ACI policy model are supported.
- Northbound controller interfaces for integrating higher-level automation solutions on top of the policy and controller framework, including workflow automation tools and analytics: Modern SDN controllers, as does Cisco APIC, include northbound APIs allowing for the integration of OpenStack or other vendor-specific cloud automation tools (e.g., Cisco UCS Director).

What's unique about ACI is that the policy language (the rules that tell your cloud infrastructure what to do) is not modeled on arcane networking concepts like VLAN's and IP addresses, but on application requirements, and especially how application workloads can and can't communicate, and what kind of services they are entitled to. Policies are applied to classes of applications or workloads (e.g., the web tier of an application), also called endpoint groups (EPG), which can be either physical or virtual workloads (or containers).

An application policy will consist of the EPG's that make up the application, and the contracts and services between the EPG's. This is fundamentally all we need to automate the deployment, provisioning and optimization of our application network anywhere, on any cloud resources we want.

The result is an SDN-automated infrastructure that extends beyond just network devices, to include layer 4-7 application services like load balancers, as well as security devices and policies for IPS and firewall components. Because applications are the best reflection of business activity, an application-centric policy is ideal to align IT with business policies, and to automate policies that reflect real business and application requirements.

Figure – Cisco ACI provisions the entire network infrastructure through application polices managed in a centralized SDN controller, the APIC.



For More Information

For more information, please visit http://cisco.com/go/aci.

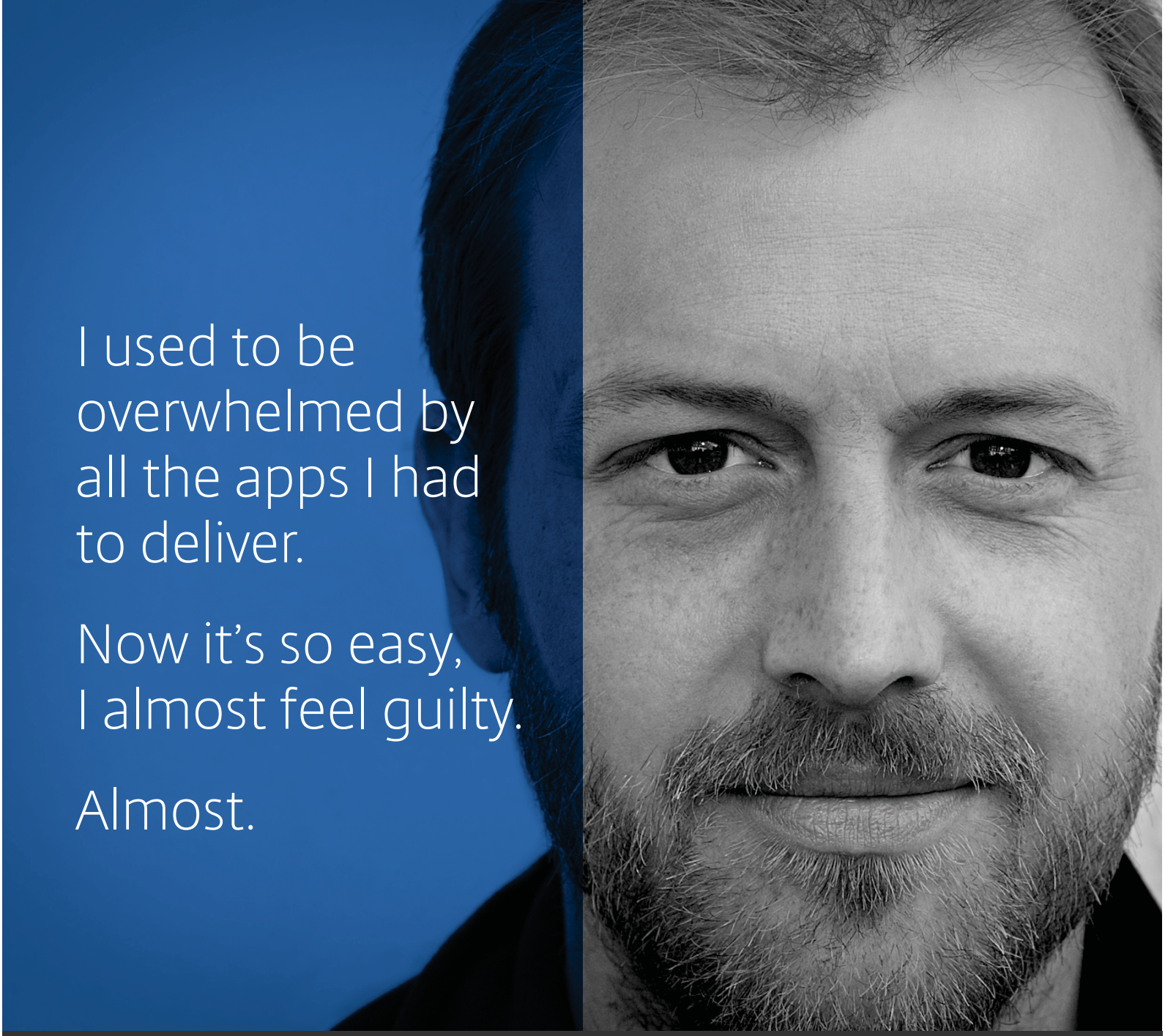
Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-728045-00 05/13



NetScaler with TriScale harnesses the power of software so you can effortlessly customize your app delivery for any business need.

NetScaler with TriScale
SOFTWARE SMART. HARDWARE STRONG.

CITRIX®

www.citrix.com/netscaler

Enterprise SDN and Carrier NFV: Distant Cousins or Twins?

It's not unusual to hear SDN and NFV mentioned together as part of a broad, conceptual discussion about network virtualization. But in practical use, the two represent entirely different worlds—SDN having been born out of the needs of large enterprises principally focused on data center virtualization, and NFV being embraced by telcos and communication service providers for virtualizing service delivery.

One major reason enterprise and carrier technology, including SDN and NFV, are treated as fundamentally different is that the IT goals driving enterprises and carriers are noticeably dissimilar. Add to that the historic differences in vocabulary, infrastructure, and scale between the two camps, and it's not surprising most IT professionals still think of these worlds as wholly unrelated.

But as IT evolves toward virtualization and convergence, the fact is that undeniable similarities have started to emerge. In fact, there are common infrastructural elements striking enough to raise the question: should we think of enterprise SDN and carrier NFV as distant cousins, or are they actually more like twins?

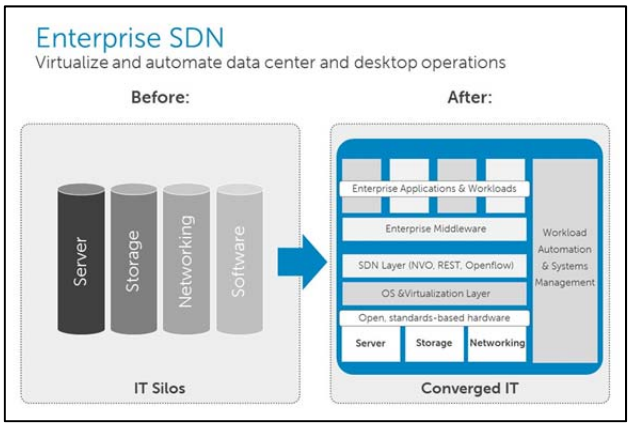
OPERATIONAL NEEDS DRIVE ENTERPRISE SDN ADOPTION

Data centers have been virtualizing server and storage functions using software and hypervisors from VMware, Microsoft Hyper-V, and Red Hat/OpenStack for years now. Virtual machines (VMs) give enterprise data centers the flexibility and agility they need to scale and operate efficiently on a day-to-day basis while also reducing the amount of physical infrastructure required.

Naturally, IT teams have begun applying the same philosophy to networking, seeking the greatest level of virtualization, automation, and programmability possible to simplify their back-end operations.

In many cases, this involves the deployment of virtual switching technology (aka vSwitches) and networking them along with physical switches to create more efficient workflows for applications and workloads.

Right now, there are three common approaches to virtualizing networking infrastructure and and introducing greater levels of programmability and automation.



1. Network virtualization overlay (NVO)
NVO stitches the data center's vSwitches together by building tunnels (VXLAN, NV-GRE, etc.) through the physical switch infrastructure, requiring no additional effort at the physical switch level.

2. Controller-based solutions (ex: Openflow)
Controller-based solutions change what takes place in the physical switch by establishing a protocol among the deployed physical switches and a controller. The controller can then be used to program all the switches in any way desired for policy control.

3. Programmable solution (ex: REST)
Other IT teams prefer to use programmatic or scripting languages, such as Puppet or Chef, to interface with their infrastructure and automate operations. Rather than a controller that speaks to multiple devices, they implement a programmatic language to define and implement policies across the infrastructure. .

Each of these approaches has arisen from challenges that are inherent in operating large-scale data centers. Meanwhile, carriers have their own reasons for virtualizing their infrastructure.

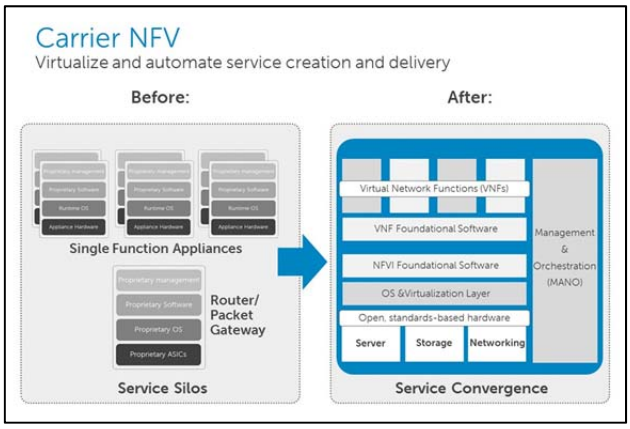
SERVICE DELIVERY GOALS DRIVE CARRIER NFV ADOPTION

Traditionally, when a carrier delivers IP services, data packets are sent from customer site or device to a carrier's router or switch, and then daisy-chained through a set of boxes performing additional service-related functions.

Just as it sounds, this process of service creation and delivery has been very physical in nature, involving many pieces of equipment, cables, and

moving parts and requiring similarly large number of staff for rollout and support.

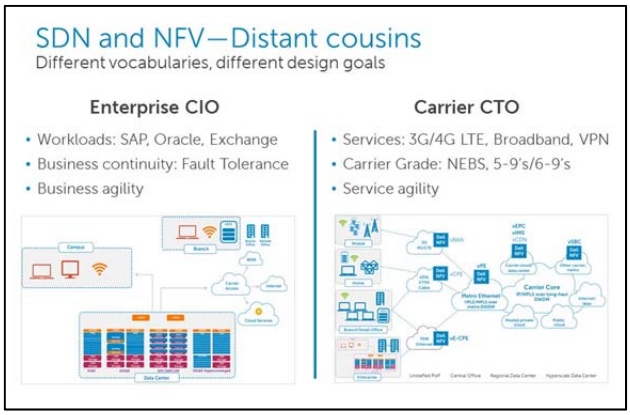
Carriers globally are now turning to virtualization and in particular NFV as a way to simplify and automate service delivery infrastructure, while also introducing greater agility for new service creation and delivery. For carriers, then, the drivers for virtualization are to improve both CAPEX and OPEX structures, making existing service delivery more cost effective, and enabling new, high-margin, services quickly.



THE LANGUAGE BARRIER

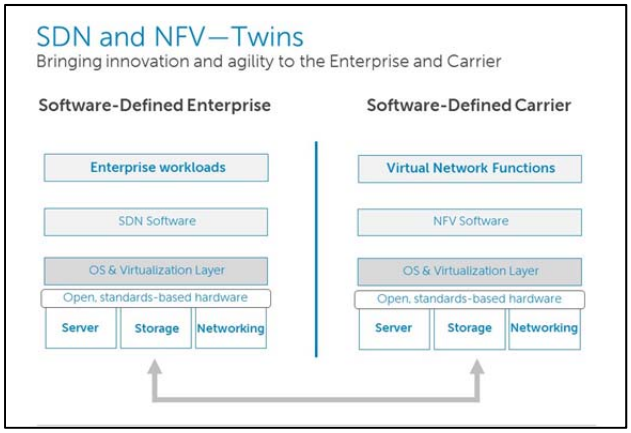
To further compound these differences, enterprise SDN and carrier NFV generally fall under the purview of different executive roles—typically the CIO at enterprises and the CTO for carriers.

There are also fundamental differences in the vocabulary surrounding each. Instead of *workloads*, carriers are concerned with *services*, and instead of *business continuity*, carriers are interested in *carrier-grade* 5-9's and 6-9's *technology*.



DISTANT COUSINS OR TWINS?

Considering this laundry list of differences, you might wonder how we can propose that enterprise SDN and carrier NFV are actually twins. It's not until you look at their technological DNA that you start to see the remarkable similarities.



As the above image shows, beneath the disparate business goals and terminology, the infrastructures that support enterprise SDN and carrier NFV are practically identical.

At its core, in both enterprise SDN and carrier NFV, exists x86 server-centric DNA that forms the foundation of the converged infrastructure for compute, storage and networking. Yet, just as twins share the same DNA but can have very different personalities based on environmental factors, enterprise SDN and carrier NFV are really only distinguishable at the application level (e.g. enterprise application vs. carrier VNF)

COMMON TRAITS FOR THE FUTURE

The full implications of this shift in perspective remain to be discovered, but a couple of opportunities immediately arise when we recognize the structural similarities of enterprise SDN and carrier NFV:

1. Carriers who are new to network virtualization can learn best practices from Web 2.0 and large enterprises who have already made significant strides in that area and apply in context..

2. Organizations that operate both production and provisioned infrastructure—enterprise-style for their own operations and carrier-style to provide services—can cross-pollenate, leveraging common technology assets, best-practices, and purchasing power.

While the vocabulary and topologies may never fully converge, the thinking can, having the potential to open new doors for positive collaboration and greater operational efficiencies. Recognizing the common traits behind enterprise SDN and carrier NFV is the first step.

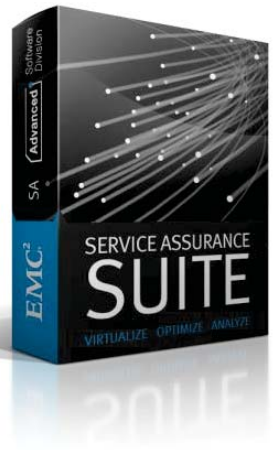
Software-Defined Networking

Are your management tools prepared?

Software-Defined Networking (SDN) and Network Virtualization (NV) are quickly becoming priorities because of the promise to dynamically manage traffic loads while lowering costs in response to changing business requirements…

Are you prepared for this evolution?

EMC understands these challenges. Designed to manage physical, virtual and cloud environments, the EMC Service Assurance Suite helps IT operations teams manage infrastructure across each phase of this evolution.

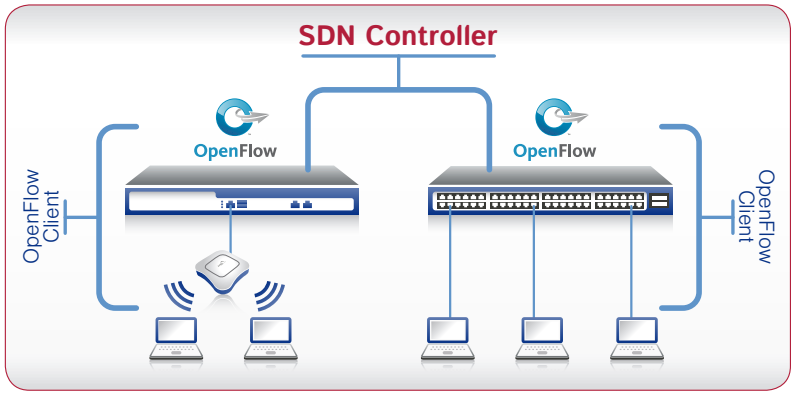


Empower your IT operations team to visualize, analyze, and optimize your service-delivery infrastructure. Learn more at www.emc.com/sa.

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, email us at asd@emc.com or call 866-438-3622.

EMC²

Delivering the promise of SDN across wired/wireless networks



As the enterprise network edge transitions to an all wireless network, software-defined networking (SDN) and OpenFlow are emerging as a way to bring new levels of agility to organizations beyond the data center where SDN first gained traction.

The rapid acceptance of SDN and this new approach to design, build and manage data centers addresses the top challenges experienced by organization related to networks: namely, too many manual processes, and difficulties changing configurations. SDN tackles these challenges in the data center, but SDN can equally address the same issues for the enterprise campus. Without bringing SDN to the edge of the network, its true promise is lost.

Meru is leading the way being the first wireless vendor to receive a Certificate of Conformance through the ONF OpenFlow™ Conformance Testing Program within our wireless LAN controllers to enable third-party control all the way down to the access point. This provides customers with confidence in the products that they adopt will provide multi-vendor support.

Meru is also collaborating with IT giants such as NEC to enable seamless interoperability between the NEC ProgrammableFlow® Networking Suite and Meru 802.11ac intelligent Wi-Fi solutions. NEC and Meru are the world's first vendors to receive OpenFlow Conformance Certification respectively as a wired and wireless vendor - a natural pairing.

Meru has introduced Meru Center, a network application management platform, unifying network applications under a single platform and permits easy activation of pre-installed network tools.

With Meru Center, new SDN applications are delivered via the Meru App Store. This library function hosts a growing set of qualified applications that may be selected and installed on a user's network. Initial Meru SDN applications available will include:

Meru Collaborator
An SDN application that integrates with Microsoft's Lync unified communication solution with the ability to detect QoS (quality of service) issues on a heterogeneous wired/wireless network, deliver prescriptive resolution options and prioritize traffic across multi-vendor wired and wireless networks.

Meru Personal Bonjour
An application that minimizes Bonjour broadcast storms of Apple related devices across unified networks and advertises services only to the correct users according to established policies.

Making SDN a Reality for Wi-Fi

The promise of SDN is that networks will no longer be closed, proprietary, and difficult to manage. Meru is taking a leadership position in the emerging wireless market for SDN, and is committed to delivering the most robust SDN Wi-Fi solution in the market while providing a best-of-breed wireless solution.

With innovative solutions from Meru and a robust SDN ecosystem, organizations can meet the unprecedented demand for Wi-Fi with ease.

Click for more information

Meru delivers an all-wireless network that fully supports the enterprise, delivering a consistent, interactive experience for all users. No matter what applications they are running. No matter how many other users are on the network. For more information, visit **www.merunetworks.com** or email your questions to: meruinfo@merunetworks.com.

Meru Networks®
Corporate Headquarters
894 Ross Drive
Sunnyvale, CA 94089
T +1 (408) 215-5300
F +1 (408) 215-5301
E meruinfo@merunetworks.com

Extending Service Performance Management into SDN and NFV Environments

Solution Benefits

- Holistic end-to-end visibility into physical, virtual, and hybrid service delivery infrastructure
- Proactive service triage helps resolve problems in real time and assures a positive customer/user experience
- Comprehensive service performance management platform across voice, data, and video services and applications
- Ultra high scalability assures service delivery across any size of service provider and enterprise infrastructure

Problem Overview

While the strategic importance of delivering IP-based services is constantly increasing, enterprises and service providers are being pressured to find ways to deliver these services faster, with higher quality, and more cost effectively. To achieve these goals, enterprises and service providers are gradually migrating their data center workloads onto a virtual infrastructure.

To realize the full potential of virtualization CapEx and OpEx efficiencies, enterprises and service providers need a comprehensive service delivery monitoring tool which offers end-to-end visibility across physical, virtual, and hybrid environments. To be truly beneficial, the tool needs to offer proactive service triage capabilities to reduce the mean-time-to-resolution, by identifying the root cause of service degradations and outages in real time.

Unfortunately, the traditional bottom-up triage methodology based on multi-vendor silo-specific Network Performance Management (NPM) and Application Performance Management (APM) tools is ineffective. It does not offer service level triage capabilities to key organizations, and lacks the ability to provide a view of the overall service.

The bottom-up triage methodology relies on disparate sets of data collected from multiple silo-specific tools, which makes it virtually impossible to gain an end-to-end holistic view of the service performance. Furthermore, these datasets lack the insight on the interrelationships and dependencies between service delivery components and therefore inhibit service triage activities. The overall result of relying on the bottom-up triage methodology is drastically increased service unavailability, reduced quality of end-user experience and loss in worker productivity.

Solution Overview

NetScout offers efficient service triage based on pervasive end-to-end visibility across physical, virtual, and hybrid service delivery environments. The triage is performed proactively by detecting service degradations in real time and is based on one cohesive, consistent set of metadata, for service provider and enterprise services. This metadata is generated by the patented Adaptive Session Intelligence™ (ASI) technology running in both virtual environments as well as nGenius® Intelligent Data Sources, and offers meaningful and contextual view of all interrelationships and dependencies across all service delivery components in physical, virtual, and hybrid environments.

NetScout's pervasive and scalable data collection is established by instrumenting strategic access points across the service delivery infrastructure using physical and virtual appliances. The packet flow data collection and aggregation is passive and non-intrusive and can scale to collect any required volumes of data across physical, virtual, and hybrid environments.

The nGeniusONE™ Performance Management platform aggregates, correlates, and contextually analyzes the metadata gathered from the nGenius Intelligent Data Sources in both physical and virtual environments. It then creates real-time holistic views of service performance, establishes performance baselines, and facilitates service-oriented troubleshooting workflows.

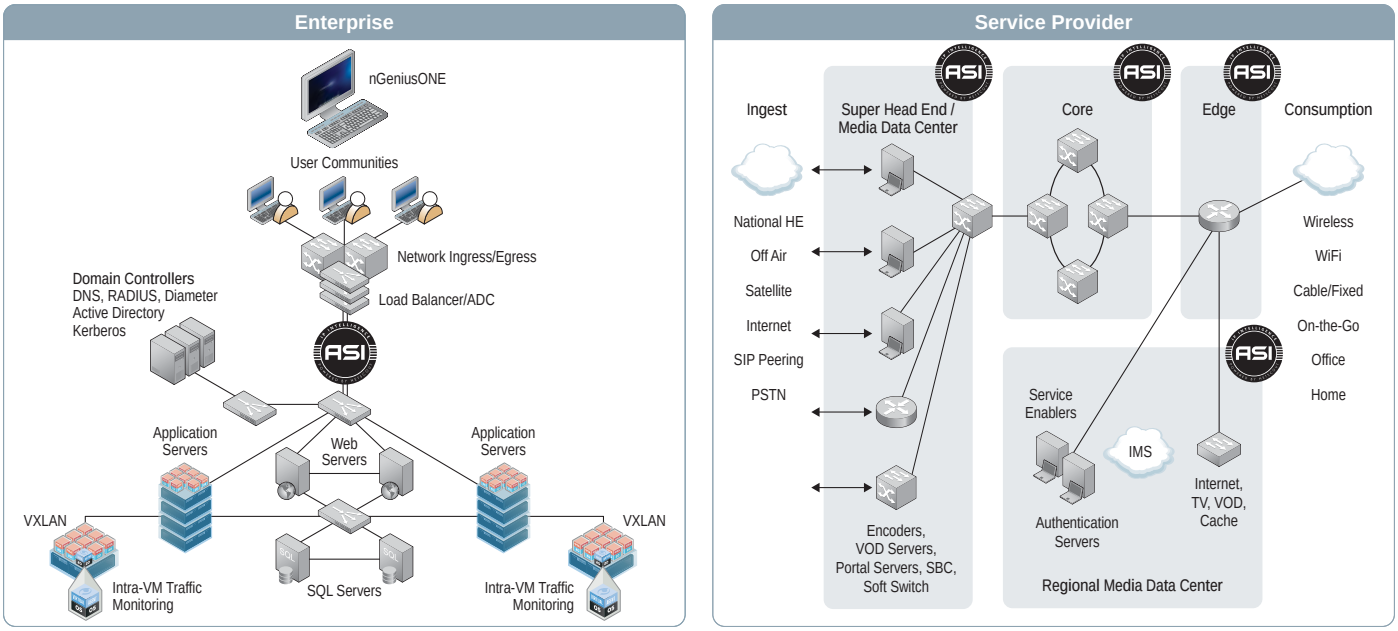


Figure 1: Service Instrumentation in Enterprise and Service Provider Environments.

Core Technologies

NetScout's unique ability to gain a pervasive end-to-end visibility into the service delivery environment, and offer proactive service triage is attributed to the following architectural principles and technologies:

- Utilize Packet Flow Data
- Provide Scalable Packet Flow Access
- Adaptive Session Intelligence (ASI)

Utilize Packet Flow Data

NetScout uses packet flow data as the foundation for generating highly scalable metadata that enables a comprehensive real time and historic view of all service components including physical and virtual networks, n-tier applications, workloads, protocols, servers, databases, users, and devices.

Provide Scalable Packet Flow Access

NetScout physical and virtual TAP network monitoring devices provide comprehensive and reliable access to packet flow data and establish strategic service visibility points across the entire service delivery infrastructure. The nGenius Packet Flow Switches (PFS) filter, aggregate, and distribute the targeted data to the nGenius Intelligent Data Sources in a transparent, selective, and efficient manner.

Adaptive Session Intelligence (ASI)

ASI is patented technology which uses a rich packet-flow data Deep Packet Inspection (DPI) engine to generate highly scalable metadata that enables a comprehensive real time and historic view of service, network, application, and server performance. This powerful deep packet inspection and data mining engine runs on nGenius Intelligent Data Sources, generating metadata based upon actual session traffic in real time as the packets cross physical or virtual links. The generated metadata provides important metrics such as application traffic volumes, application server response times, server throughputs, aggregate error counts, error codes specific to application servers and domain, as well as other data related to network and application performance. The ASI technology is the foundation of a highly scalable service delivery monitoring architecture which seamlessly collects, normalizes, correlates, and contextually analyzes data for all business services.

Service Delivery Monitoring in SDN Environments

NetScout has partnered with VMware, the global leader in virtualization and cloud infrastructure, to provide service delivery monitoring solutions in VMware NSX™ environments. These solutions enable NetScout to gain full visibility into applications traversing NSX environments in the following use cases:

- **Traffic between the VMs on the same hypervisor** is monitored by embedding NetScout's ASI patented technology into a virtual machine (VM) probe, which resides on the same hypervisor as the monitored VMs. NetScout's VM either analyzes the intra-VM traffic in a self-contained virtualized probe mode or redirects the traffic to an external nGenius Intelligent Data Source for analysis.
- **Traffic between VMs that reside in different hypervisors** is monitored by the nGenius Intelligent Data Sources that decode the VXLAN encapsulation and access the original packet flow data between the VMs.
- **Multi-tier East-West and North-South Data Center traffic** is monitored by collecting data from a combination of multi-tier physical and virtual service delivery environments, correlating, and contextually analyzing all the interrelationships and dependencies across all monitored service delivery components. These include n-tier applications, workloads, protocols, servers, databases, users, and devices.

Solution Benefits

NetScout's ability to provide end-to-end visibility into multi-tier physical, virtual, and hybrid service delivery environments combined with proactive service triage, helps address the key problems associated with silo-specific, component-based, bottom-up performance management approaches.

Attribute	Bottom-Up Triage Problems	NetScout's Solution	IT Benefits
End-to-End Visibility	• Point visibility into individual service delivery components from a variety of multi-vendor silo-specific tools. Lacks the necessary insight into interrelationships of service delivery components.	• Holistic end-to-end visibility into service delivery infrastructure using one cohesive, consistent set of data, for service provider and enterprise services delivered in physical and virtual environments.	• Optimize experience of user communities and customers. • Comprehensive solution from a single vendor. • Full visibility into services running in physical, virtual, and hybrid environments.
Effective Service Triage	• Reactive and time consuming triage results in poor user experience, and extended service downtime impacting multiple users.	• Proactive service triage helps resolve service degradation in real time, before a large number of users are impacted.	• Increase service uptime and end-user productivity. • Support more services with existing IT resources. • Reduce time wasted in war rooms.
Scalability	• Lacks scalability required to assure delivery of modern business services for service providers and enterprises.	• Scales to assure service delivery across any size of service provider and enterprise infrastructure.	• Optimize your investment in performance management by gradually expanding the solution over time.

About NetScout Systems, Inc.

NetScout Systems, Inc. (NASDAQ:NTCT) is the market leader in application and network performance management solutions that enable enterprise and service provider organizations to assure the quality of the user experience for business and mobile services. Used by 92 percent of Fortune 100 organizations and more than 165 service providers worldwide, NetScout's technology helps these organizations proactively manage service delivery and identify emerging performance problems, helping to quickly resolve issues that cause business disruptions or negatively impact users of information technology. For more information about NetScout, visit www.netscout.com.

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

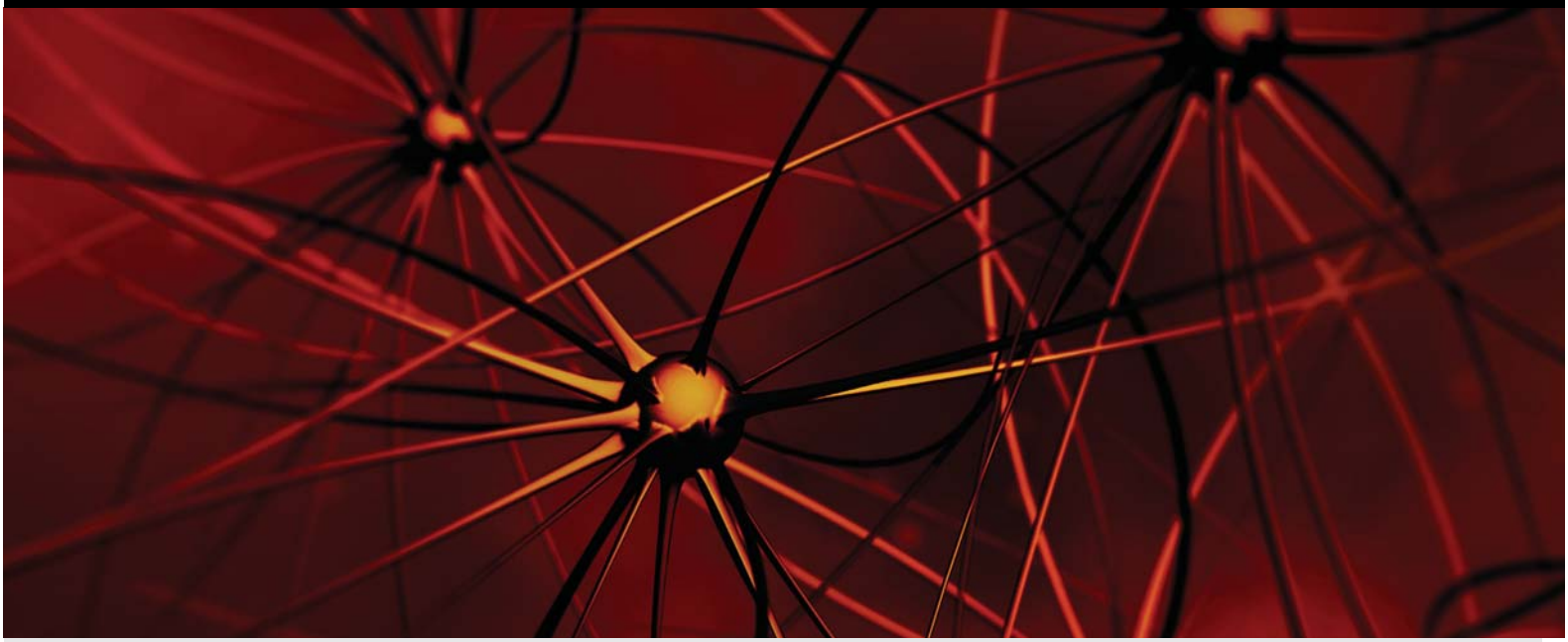
Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000

nuagenetworks

@nuagenetworks



The Cloud Network Unbound

Virtualized and automated networking across datacenters and branch offices

Cloud computing is changing the way enterprises access and consume data. To remain competitive, businesses know they must be able to react quickly to market changes. The cloud addresses their need for speed, agility and responsiveness. Unfortunately, today's data communications networks aren't keeping pace. In fact, they're struggling to deliver consistent, on-demand connectivity and things are only going to get more challenging. Fortunately, Nuage Networks has a solution.

Nuage Networks leverages Software Defined Networking (SDN) to unleash the power of the cloud, giving enterprises the freedom and flexibility to:

- Connect sites, workgroups and applications faster, more securely and more cost effectively
- React to change easily
- Respond to growth seamlessly

Nuage Networks makes the network as responsive as your business needs it to be — from the datacenter to remote locations.

Our solutions close the gap between the network and cloud-based consumption models, creating an infrastructure in which network resources are as readily consumable as compute and storage resources. Our approach enables enterprises to transform the way they build and use their networks, which has a profound effect inside and across multiple datacenters and across the wide area network.

Imagine the possibilities when network resources are easily consumable. A Nuage Networks datacenter network is as dynamic, automated and virtualized as the server infrastructure, and supports the needs of applications with instantaneous network connectivity.

Take advantage of a fully virtualized services platform

Cloud-based datacenters have unshackled the IT environment, making it possible for applications to request additional compute and storage on an as-needed basis. Extending the reach of virtualized network services from the datacenter to remote locations further enhances the enterprise's ability to respond to business imperatives at cloud speed. Peak demands can be provisioned "just in time", which lowers operational costs and makes it possible to share compute resources across applications. Geography is taken out of the equation.

Nuage Networks SDN solutions enable you to react to changes in your datacenter or at branch locations with speed, agility, and flexibility. Our solutions seamlessly connect your datacenters and the wide area network, so networking across the whole environment is fluid and responsive to changing business conditions.

By improving efficiency, resiliency and security, our products enable networks to be built and operated at any scale – from a single rack to Fortune 500 scale.

Our SDN solutions work closely together and deployment is flexible, so you can focus on the area most in need of help.

Responsive datacenter networking

Build robust and highly scalable networking infrastructures with the **Nuage Networks Virtualized Services Platform (VSP)**. These new infrastructures will let you instantaneously deliver compute, storage and networking resources securely to thousands of user groups.

Virtual private networking on your terms

The **Nuage Networks Virtualized Network Services (VNS)** enables you to respond faster and with greater agility to changes in your wide are network environment. A self-serve portal allows enterprise end users to self-manage moves, adds and changes, significantly reducing the time and effort required to manage the wide area network.

Nuage Networks SDN solutions are specifically designed to:

Simplify operations for rapid service instantiation	Address changing business requirements with flexible, adaptable services	Support massive scalability and hybrid models with secure, open infrastructure
■ Define network service requirements in clear, IT-friendly language ■ Bring services up using automated, policy-based instantiation of network connectivity ■ Dramatically reduce time to service and limit potential for errors	■ Adapt datacenters and private networks dynamically ■ Detect newly created and updated virtual machines within the datacenter and respond automatically by adapting network services according to established policies, instantly making available new applications to all users regardless of location	■ Benefit from distributed, policy-based approach that allows multiple virtualization platforms to interoperate over a single network ■ Optimize the datacenter network and private network by separating service definition from service instantiation

Nuage Networks SDN solution components

Nuage Networks VSP is the first network virtualization platform to address modern datacenter requirements for multi-tenancy, full-featured routing and security at scale. It is a software solution that transforms the physical network into a simple to manage, rack-once and wire-once, vendor-independent IP backplane. As a result, network resources within and across datacenters can be treated as an elastic resource pool of capacity that can be consumed and repurposed on demand.

Nuage Networks VSP integrates seamlessly with wide area business VPN services. It is also particularly effective when deployed with Nuage Networks VNS for a cloud-optimize network that spans the datacenter right out to your remote locations.

NU•ÂHJ: FROM FRENCH, MEANING "CLOUD"

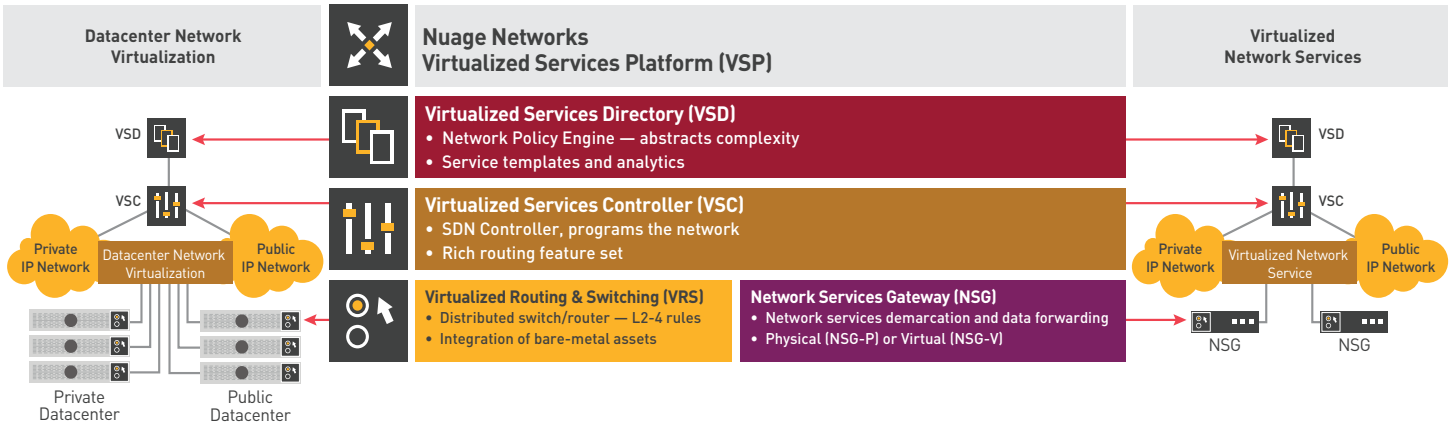
The cloud can be more than what it is. In fact, it needs to be. When we founded Nuage Networks, it was with the idea that it's time for the cloud to come of age. From the beginning we recognized the unique challenges that cloud service providers and large enterprises face delivering and managing large, multi-tenant clouds. While the virtualization of compute and storage has evolved quickly, the network simply has not kept up. The result is that today your cloud is being held back. And so is your business.

When we started Nuage Networks, it was with the mission that we could empower our customers to finally deliver on the true promise of the cloud. We envision a world in which IT and IP are no longer in conflict, but rather work in concert to propel your business and elevate the cloud for every one of your customers. We see a world where innovation isn't hampered by infrastructure, and network resources are as effortlessly consumable as compute and storage.

To make this vision a reality, Nuage Networks brings a unique combination of ground breaking technologies and unmatched networking expertise. This enables us to create solutions that do more than provide incremental improvement. It allows us to introduce radically new thinking and pick up where others have left off, delivering a massively scalable SDN solution that ensures the datacenter and wide area network are able to respond instantly to demand and are boundary-less.

Our mission is to help you harness the full value of the cloud.

Nuage Networks SDN Portfolio



nuagenetworks

PICA8 OPEN NETWORKING

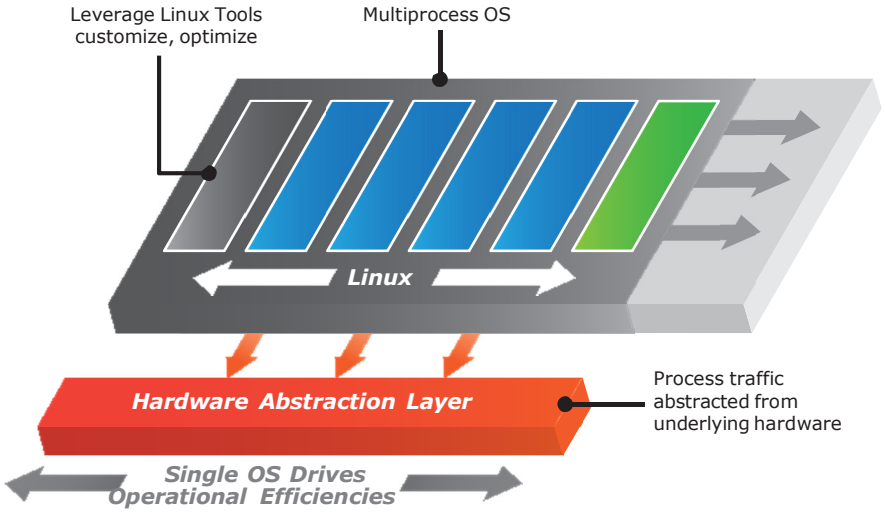
WWW.PICA8.COM

PicOS Overview

PicOS™ is the first bare metal compatible network operating system that:

- Enables customers to seamlessly and easily integrate conventional networking and SDN.
- Provides extensive support for traditional switching and routing protocols that is extendable by SDN and OpenFlow capacity through Pica8's hardware accelerated Open-vSwitch (OVS).
- Offers a unique, comprehensive and flexible configuration management environment from either a Linux shell, a feature-rich command line interface (CLI) or a comprehensive set of APIs (JSON RPC and OpenFlow).

PicOS runs as an application in user space in an un-modified Linux kernel, thereby leveraging kernel thread protection, and compatible with DevOps tools such as Chef and Puppet that are popular with server and system administrators.



* Only OpenFlow features available in hardware are supported, to ensure optimum performance

PicOS - Three Editions to Leverage

A base configuration starts with the Linux Switching OS package. For additional functionality, select either the Routing or OpenFlow Editions, or the PicOS Bundle depending on your use case.

Features Included	Required PicOS Editions		
	Linux Switching OS	Routing	OpenFlow
• Network operation system using user space standard Debian Linux environment • Leverage vast array of standard Linux tools as a common management and operations framework • Zero Touch Provisioning (ZTP) functionality coupled with ONIE delivers a true bare metal to application environment • Rich Layer-2 protocol stack with MLAG, seamlessly integrating into existing architectures • Full Layer-2 & Layer-3 ACL support • IPv4 & IPv6 Static Routing	✓		
• Rich OSPF and BGP protocol stacks integrating into existing spine / leaf architectures • IPv6 routing protocol support (OSPFv3, MBGP) • Multicast PIM support • NAT (depends on ASIC support) • VXLAN network virtualization (depends on ASIC support)	✓	✓	
• Leading OpenFlow 1.4 support through OVS 2.0 • Deliver true seamless migration to SDN through CrossFlow mode (Layer-2 / Layer-3 and OpenFlow simultaneously) • Leveraging OpenFlow to control MPLS, GRE, NVGRE or VXLAN tunnels, delivering on the promise of open programmability • Support for all major OpenFlow controllers (for example: OpenStack Neutron ML2, OpenDaylight, Ryu)	✓		✓
PICOS Bundle	✓	✓	✓

Radware's Software Defined Networking Solutions: Enable Network Wide Services via SDN Applications and NFV

Radware SDN applications improve application security, performance and availability by programming the SDN to collect data and optimally forward traffic to deliver network services. The native component of the new network stack introduced by SDN includes the data plane networking devices and the control plane SDN controllers. The Radware SDN applications constructing the SDN application control plane, interact with the SDN controller using dedicated SDN drivers and work together with the Radware systems' using the Radware API to collect data throughout the application infrastructure using specific data collection drivers.

With Radware SDN applications, ADC and security services transform from device-based solutions requiring a static traffic forwarding configuration, to network wide services that intelligently divert traffic to service engines. Network services can scale to support larger networks at lower capital and operational cost. By building SDN applications that continuously interact with the SDN control plane and program the network (and by leveraging the Radware Virtual Application Delivery Infrastructure (VADI) architecture – which enables pooling of disperse resources to operate uniformly) Radware enables an anywhere and everywhere network service paradigm.

Key benefits from the Radware SDN network service infrastructure include:

- **More intelligent application delivery and security decisions** throughout the network break existing network barriers when developing business applications. Every application everywhere is entitled for advanced services.
- **Simpler implementation** of network services allows improved operational efficiency of network management alongside application changes. Not every project needs to become a networking project.
- **Lower overall network service solution costs** – as network service delivery is partially offloaded to the SDN, there is no need to invest in excess network service appliances and capacity. Deploy network services as needed, and use by many tenants and applications throughout the datacenter.
- **Greater scalability** – scale your network services throughout the network. No more limited areas are protected or load balanced. Offer uniform services throughout the SDN.
- **Easier operation** – changing and managing security and ADC functionality becomes simpler as the deployment operates as if it is centralized. Not only does SDN streamline network operations, but Radware SDN applications streamline network service operations. In addition, API to various orchestration systems enables to improve the overall control and automation of network services.

DDoS Protection as a Native SDN Application

DefenseFlow is an SDN application that enables network operators to program the network to provide DDoS protection as a native network service. DefenseFlow features an adaptive behavioral-based DoS attack detection engine and a traffic diversion mechanism that utilizes the programmable characteristics of the software defined network elements for attack cleansing. Designed as part of the Radware SDN application framework, DefenseFlow delivers a security control plane and operates in traditional network environments while enabling to migrate to customer's future, SDN-based networks.

Legacy DDoS protection solutions that make use of scrubbing centers are costly: need hardware detectors in every network location; BGP for traffic diversion; and GRE tunnels to forward the traffic to its designated network object. With SDN, a DDoS protection solution turns into a software application that adds intelligence to the network – no need for additional hardware, BGP or GRE operations.

DefenseFlow equips network operators with the following key advantages:

- **Unprecedented coverage against** all type of network DDoS attacks
- **Best design for attack mitigation**
  - Attack detection is always performed out of path (OOP)
  - During attack only suspicious traffic is diverted through the mitigation device
- **Most scalable mitigation solution – DefensePro mitigation devices can be placed in any location, DefenseFlow diverts the traffic to the nearest mitigation device.**

- **Centralized security control plane including control part of Radware's Attack Mitigation Network (AMN)**

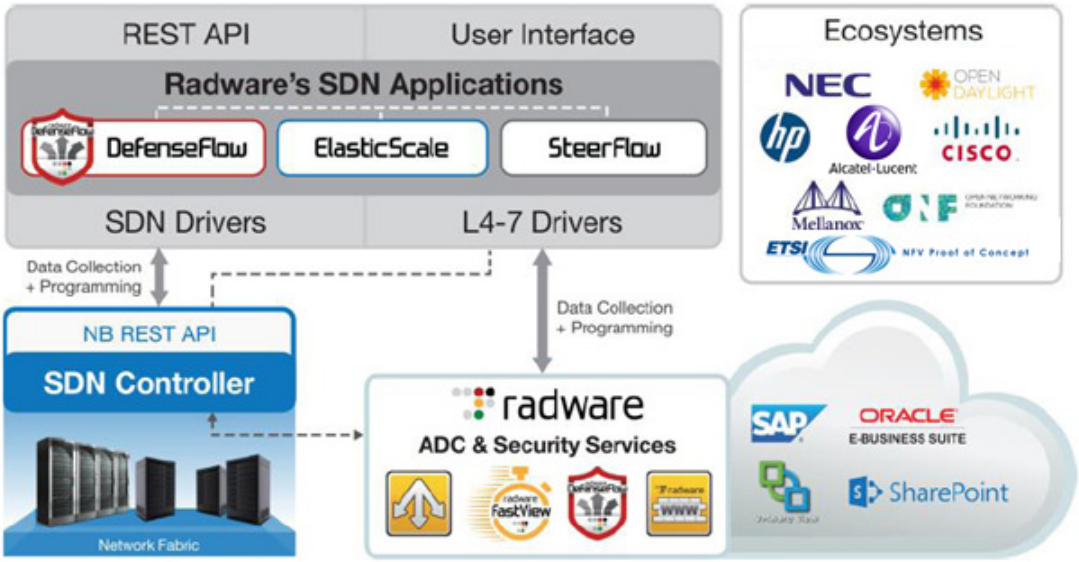
SDN & NFV for a Scalable Application Delivery Network

The Network Functions Virtualization (NFV) initiative was formed in order to enable the standardization of network equipment by leveraging commercially off-the-shelf (COTS) hardware and running advanced network function software on them. Radware is proudly introducing Alteon VA for NFV – the industry's first and only ADC designed from the ground up to run in NFV environments. Targeted mainly at carriers but also at high-end online businesses, Alteon NFV provides unique value proposition including CAPEX/OPEX reduction, eliminate "vendor lock", high performance, high-end scalability and greater network service agility.

Radware's ElasticScale is an SDN application that wraps existing network service virtual appliances, including Alteon NFV, and provides provisioning and traffic distribution logic to consistently deliver network services in an elastic demand environment. ElasticScale can be utilized for service provider internal services, managed services to end customers and can help providers adopt network function virtualization paradigms.

ElasticScale offers network operators the following key features and benefits:

- Ultra scalable traffic steering solution (80Gbps-1Tbps and beyond)
- Based on industry leading, carrier grade Alteon load balancing product line
- Support for leading hypervisors (oXen/KVM/Hyper-V/ESXi)
- Compatible with leading SDN controllers; OpenDaylight, Cisco XNC, NEC pFlow & HP Flare
- Seamless integration with OpenStack and vCloud Director
- Runs over any physical SDN network equipment



Partnering for Success: Our SDN Ecosystem

The SDN eco-system is a critical focus for Radware. Through partnerships with the industry's leading SDN forums and vendors, Radware can ensure customers that our application delivery and security solutions integrate successfully into target architectures. Radware is an active contributor in the following industry and vendor SDN initiatives: Cisco Application Centric Infrastructure (ACI), HP Virtual Application Networks, NEC, Mellanox, Alcatel Lucent, ETSI, Open Daylight Project, and the Open Networking Forum (ONF). Radware is also a member of VMware's NSX partner ecosystem for network functions virtualization (NFV).

Learn More

To learn more about how Radware's SDN solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.