The 2016 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:

A10

CISCO

Hewlett Packard Enterprise

MASERGY
Performance Beyond Expectations

NETSCOUT™
Guardians of the Connected World

Sonus

Gold Sponsors:

radware

SevOne

Produced by:

Webtorials

Table of Contents

Introduction

Over the last couple of years, the hottest topics in networking have been Software Defined Networking (SDN) and Network Functions Virtualization (NFV). While both enterprises and service providers have shown great interest in these topics, the vast majority of organizations are still either on the sidelines or in the analysis stage of adoption. The primary goals of **The 2016 Guide to SDN & NFV** (The Guide) are to eliminate the confusion that surrounds SDN and NFV and to accelerate the analysis and potential adoption of these new architectural approaches.

The Guide will be published both in its entirety and in a serial fashion. This document is the eighth of the serial publications and it will present an executive summary of the preceding seven publications. Below is a listing of all of the publications that comprise The Guide:

1. A SDN Status Update
2. The Use Cases and Business Case for SDN
3. The Operational Impediments to Implementing SDN
4. A NFV Status Update
5. Architectural Considerations and Use Cases for NFV
6. The Operational Impediments to Implementing NFV
7. The SDN and NFV Ecosystem
8. An Executive Summary of The Guide

The Guide is based in part on *The 2015 Guide to SDN and NFV* (The 2015 Guide). To limit the size of The Guide, some of the introductory material, such as a description of the basic SDN architecture that was contained in The 2015 Guide has been eliminated. The 2015 Guide, however, is still available online.

This guide contains the results of two surveys. One of the surveys focused on SDN, was administered in October 2015 and was completed by 131 IT professionals. The other survey focused on NFV, was administered in December 2015 and January 2016 and was completed by 144 IT professionals.

A SDN Status Update

The survey data indicated that the majority of organizations are actively involved in analyzing, trialing or using SDN in production. However, that was true a year ago and comparing this year's survey data with last year's data indicates that SDN remains stuck on the edge of crossing the chasm from being used primarily by early adopters to where it is widely used and that it will likely be on the edge for at least another year or two.

One thing that has changed in the last year is the amount of resources that has gone into creating open source solutions. According to Dan Pitt, executive director of the Open Networking Foundation (ONF), the growing interest in SDN-related open source projects will accelerate the adoption of SDN. His belief in the importance of open source based solutions is the reason why in February 2015 the ONF launched an open source community and code repository called OpenSourceSDN.org. The role of this community is to sponsor and develop open SDN solutions in order to provide greater adoption of open SDN.

The interest in open source has led to a situation where there are multiple open source-based SDN controllers including one from ON.Lab and one from the OpenDaylight (ODL) Project. The ON.Lab is a non-profit organization whose mission is to "bring openness and innovation to the Internet and Cloud for the public good". One of the ON.Lab's primary projects is ONOS (Open Network Operating System) – an open source SDN operating system for service providers. In September 2015 ON.Lab released the fourth version of ONOS, code named Drake. According to ON.Lab "Drake adds new security, configuration and application level feature sets with improvements to the northbound and southbound including REST, API and GUI additions and upgrades throughout. In addition to contributing to ONF's Atrium, ONOS has expanded collaboration with other open source communities to develop new distributions including work with the CloudRouter® Project and it will soon be part of the Open Platform for NFV Project (OPNFV)." In October 2015 the ONOS project joined the Linux Foundation.

The ODL Project, which was founded in April 2013, is a collaborative open source project that is also hosted by The Linux Foundation. The goal of the project is to facilitate a community-led, industry-supported open source framework, including code and architecture, to accelerate and advance a common, robust SDN platform and to create a solid foundation for NFV. Towards that end, the ODL project claims that a number of vendors use ODL code as the basis of their SDN products[1] and that its code is also used by the OPNFV platform. In June 2015 the consortium announced the availability of its third software release, called Lithium.

An important area where progress is being made relative to the evolution of SDN is the North Bound Interface (NBI) that sits between a SDN controller and the business applications and network services that utilize the controller. In 2013 the ONF established a working group to focus on the NBI. Given that traditional standards activities are widely viewed as not being agile enough for the current environment, the goal of the working group was not to develop a standard for the NBI in the traditional sense of the term *standard*. Rather, the goal was to develop a rough consensus and collaboration around community developed NBIs.

Dave Lenrow is the chair of the ONF's NBI working group. Lenrow said that the ONF's NBI initiative is "Essentially doing an experiment in collaborative agile development with open source projects. Instead of spending years trying to prove on paper that our architecture works we throw some experimental API

[1] https://www.opendaylight.org/solutions-provider-directory

stuff to multiple OSS projects (e.g., ODL, ONOS) and let implementers provide feedback on what works and what doesn't with a *fast fail* approach. Our members want ONF as a neutral third party to define the basic software artifacts (e.g., Information model, principles of operation) that get implemented on many vendor's solutions."

The Drivers and Inhibitors of SDN

Unlike the situation last year, there is currently as much interest in either implementing SDN in the WAN or using a SDN-based WAN service as there is in implementing SDN in the data center. Given the breadth of SDN-based use cases described in The Guide, it is becoming difficult to talk about SDN without specifying if that is SDN deployed in the data center, the WAN or the branch/campus.

Table 1 lists the 5 top drivers of implementing SDN in varying segments of the network.

Table 1: Top 5 Drivers

Data Center	WAN	Branch and Campus
Support the dynamic movement, replication and allocation of virtual resources	Ease the administrative burden of configuration and provisioning	Ease the administrative burden of configuration and provisioning
Ease the administrative burden of configuration and provisioning	Better utilize network resources	Better utilize network resources
Better utilize network resources	Perform traffic engineering with an end-to-end view of the network	More easily scale network functionality
Perform traffic engineering with an end-to-end view of the network	More easily scale network functionality	Support the dynamic movement, replication and allocation of virtual resources
More easily scale network functionality	Support the dynamic movement, replication and allocation of virtual resources	Reduce OPEX

Table 2 lists the 5 top inhibitors of implementing SDN in varying segments of the network.

Table 2: Top 5 Inhibitors

Data Center	WAN	Branch and Campus
Concerns about how we would integrate SDN into the rest of our infrastructure	Concerns about how we would integrate SDN into the rest of our infrastructure	Concerns about how we would integrate SDN into the rest of our infrastructure
The immaturity of the enabling technologies	The lack of a compelling business case	The lack of a compelling business case
The confusion and lack of definition in terms of vendors strategies	The immaturity of the enabling technologies	Possible security vulnerabilities
Other technology and/or business priorities	The immaturity of the current products	The immaturity of the current products
The lack of a compelling business case	Possible security vulnerabilities	Other technology and/or business priorities

Easing the administrative burden of configuration and provisioning tends to be the primary driver of SDN adoption and concerns about how it would be integrated into the rest of the infrastructure is the primary inhibitor. After that, the drivers and inhibitors for SDN vary somewhat based on whether SDN is deployed in the data center, the WAN or the branch/campus.

The Operational Impediments to Implementing SDN

SDN has the potential to make implementing effective security easier and it has the potential to make that harder. 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.

Some of the security challenges that are associated with SDN include:

- 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 underlying network infrastructure must be capable of enduring occasional periods where the SDN controller is unavailable, yet ensure that any new flows will be synchronized once the devices resume communications with the controller.

The Guide contains a set of questions that network organizations should ask vendors relative to the security of their SDN solution.

The Guide describes OpenStack and points out that orchestration engines such as OpenStack are important to both SDN and NFV. As explained in The Guide, 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;
- Attach Network Services to a VM or chain Network Services between VMs.

The Guide 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:

- There is a combination of physical and virtual resources that is changing dynamically.
- 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 Guide contains a set of questions that network organizations should ask vendors relative to the security of their SDN solution.

The Guide also 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.

Almost a third of the survey respondents indicated their belief that over the next two years that the ongoing adoption of software-based IT functionality will have either a significant or a very significant impact on the structure of their IT organization. In addition, over a quarter of the survey respondents indicated their belief that over the next two years that the ongoing adoption of software-based IT functionality will have either a significant or a very significant impact on their jobs. The Guide indicated the types of changes that the survey respondents expect to see.

A NFV Status Update

Roughly three years ago an Industry Specifications Group (ISG) for Network Functions Virtualization (NFV ISG) was formed under the auspices of the European Telecommunications Standards Institute (ETSI NFV ISG). That ETSI group has primarily championed the interest that Communications Service Providers (CSPs) have with NFV. More recently, the Open the Open Networking User Group (ONUG) has emerged to champion the corresponding interest that enterprises have with what the group refers to as Network Services Virtualization (NSV).

There clearly are differences between what ETSI is trying to accomplish with NFV and what ONUG is trying to accomplish with NSV. For example, CSPs hope to virtualize some functionality that few if any enterprise organizations implement and their need for scale far surpasses what is needed by the vast majority of enterprise organizations. In addition, CSPs are notably more likely to have a requirement to link the usage of virtualized network functions to their billing systems than do enterprise organizations. However, if you change at most a few words in how ONUG describes the NSV use case it sounds exactly like what ETSI and others are trying to achieve with NFV. As a result, it makes sense to look at NFV as being applicable to both CSPs and enterprise organizations.

Until recently, many people regarded SDN and NFV as separate initiatives. That is changing. Some of the ways that ETSI believes that NFV and SDN complement each other include:

- The SDN controller fits well into the broader concept of a network controller in an NFV-Infrastructure (NFVI) network domain as defined in ETSI's NFV architectural framework.
- SDN can play a significant role in the orchestration of the NFV Infrastructure resources, both physical and virtual, enabling functionality such as provisioning, configuration of network connectivity, bandwidth allocation, automation of operations, monitoring, security, and policy control.
- SDN can provide the network virtualization required to support multi-tenant NFVIs.

The survey data supported the notion that the perception of the relationship between SDN and NFV is changing. For example, the vast majority of the survey respondents indicated their belief that SDN and NFV are complimentary activities. In addition, only a small percentage of survey respondents indicated that they believe that SDN and NFV are totally independent activities.

The adoption of NFV looks similar to the adoption of SDN. For example, currently only a modest number of IT organizations have implemented NFV in a production network while a somewhat large percentage of IT organizations are currently in varying stages of analyzing NFV. While the state of adoption is similar, the factors driving and inhibiting the adoption of NFV are not very similar to the ones driving and inhibiting the adoption of SDN. For example, by a wide margin, the primary factor driving interest in NFV is the reduction in the time it takes to deploy new services. There isn't a single dominant inhibitor to the adoption of NFV, but a number of inhibitors of roughly equal value. This includes:

- The lack of a compelling business case;
- Concerns about end-to-end service provisioning;
- Concerns about security vulnerabilities;
- The immaturity of the current products;
- The need to reskill our employee base.

NFV: Architectural Considerations and Use Cases

Before an organization adopts NFV they need to address some key considerations relative to how they will architect their data center to support NFV and related initiatives.

The architectural considerations that are discussed in The Guide are:

- Big Bang vs. Piecemeal Approach;
- Software Modularity;
- Technology Considerations;
- Software-Centric Design;
- The Role of Open Source;
- Relationship with SDN;
- Programmatic interfaces;
- A Fresh Approach to High Availability;
- The (potential) end of Moore's Law.

Unfortunately, the survey data indicates that two thirds of IT organizations have made little or no progress towards the development of a NFV architecture. The survey data also indicates that while some organizations are starting to make process towards the development of a NFV architecture, the majority are not.

The Guide discusses nine potential use cases for NFV that have been defined by the ESTI NFV ISG.

Those use cases are:

- NFV Infrastructure as a Service;
- Virtual Network Functions as a Service;
- Virtualization of the Home Environment;
- VNF Forwarding Graph;
- Virtual Network Platform as a Service;
- Virtualization of Mobile Core Network and IP Multimedia Subsystem;
- Virtualization of the Mobile Base Station;
- Virtualization of Content Delivery Networks;
- Virtualization of Fixed Access Network Functions.

NFV: Operational Impediments

The Guide discusses a number of the management challenges that are associated with NFV. Those challenges are the:

- Dynamic relationships between software and hardware components;
- Dynamic changes to physical/virtual device configurations;
- Many-to-Many relationships between network services and the underlying infrastructure:
- Hybrid physical/virtual infrastructures that need to be managed;
- Evolving performance monitoring challenges;
- Fact that network services may span multiple service providers;
- Fact that VNFs will be new types of components in the network;
- Need for tighter IT and Network Operations collaboration;
- Expanding hybrid environments;
- Need for a shared information model;
- Growing need and importance of a policy based architecture.

The survey data showed that there is broad recognition on the part of IT organizations that the adoption of NFV creates new management challenges such as the ones listed above. However, the data also indicated that the vast majority of IT organizations have made little or no progress relative to determining how they will respond to NFV-related management challenges. On a somewhat optimistic note, the data indicated that over the next year the vast majority of IT organizations will spend at least a modest amount of time working on developing an approach to how they will respond to NFV-related management challenges.

Similar to the situation with SDN, the adoption of NFV has the potential to impact the role of network organizations and network professionals. That fact was recognized by the survey respondents, roughly a third of whom indicated their belief 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. In addition, roughly 40% of the survey respondents indicated their belief that over the next two years the adoption of NFV is likely to have a significant or very significant impact on the skill base of their organization. The Guide indicated the types of changes the survey respondents expected to see.

The SDN and NFV Ecosystem

The Guide 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 Guide 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;
- Providers of SDN Controllers;
- Providers of Telcom Service Provider's Infrastructure/ Optical Networking;
- Server Virtualization Vendors.

The Guide 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 Guide 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

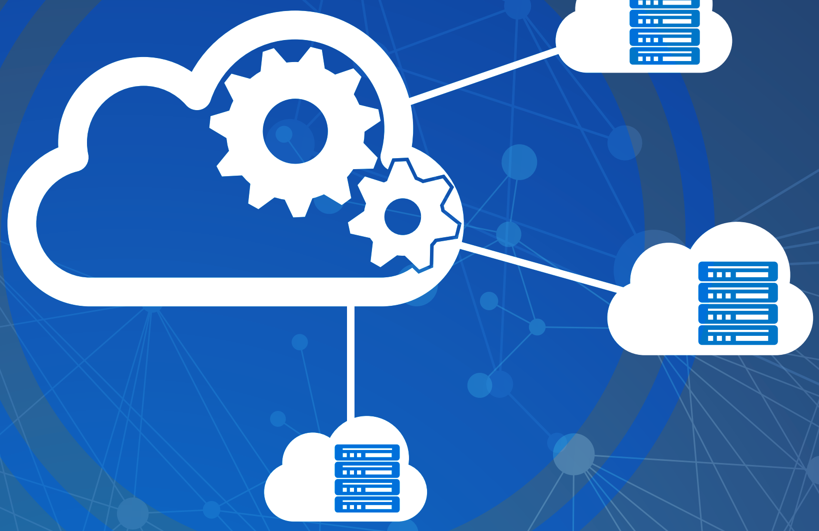
Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.

AUTOMATE YOUR CLOUD WITH aCLOUD SERVICES ARCHITECTURE

Integrate dynamic services into your Cloud Data Center

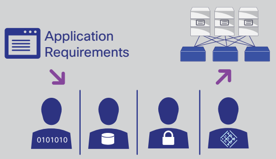
www.a10networks.com

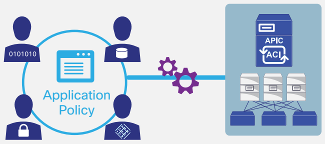


Why Choose Application Centric Infrastructure (ACI)?

Application Deployment at the Speed of Business

Without ACI	With ACI
New Application	New Application
	Simpler
IT administrators work in silos. Weeks	**Faster** IT admins work at the application level. Hours
There is no shared architectural model.	**Efficient** Shared model for policy automation.





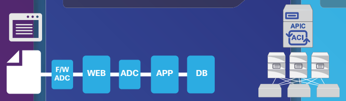
ACI cuts deployment time and effort.

Optimal Design

Application Policy

- Connectivity
- Reliability
- Compliance
- Performance
- L4-L7 Services
- Utilization

Faster Deployment



Application Network Profile

- Test
- Certify
- Adapt
- Provision

Simplified Operations

Application Topology

- Monitor
- Troubleshoot
- Optimize
- Scale Out

What does ACI deliver?

- Automation and Visibility
- Performance and Scale
- Security
- Openness

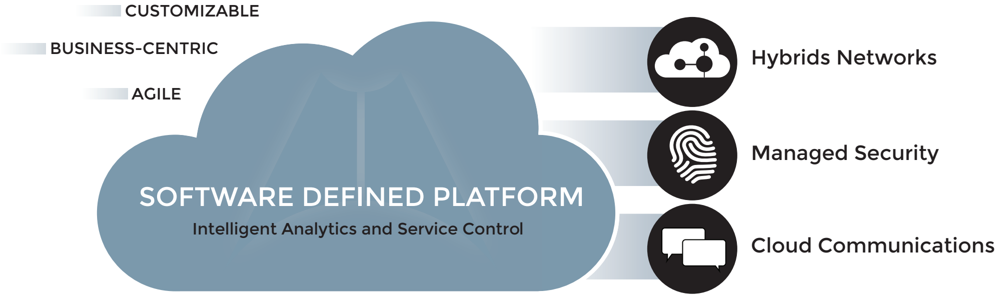
CISCO

Redefine the Power of IT with ACI

Learn more at www.cisco.com/go/aci

Masergy's Software Defined Platform Delivers the Flexibility Enterprises Require

The enterprise WAN is fast becoming the source of serious innovation. Consider it the central nervous system of corporations and their ability to support even the most advanced and demanding business-critical applications. A modern network should be agile enough to adapt to your rapidly changing business needs.



This WAN innovation is being enabled by a Software Defined Networking (SDN) architecture, which enables administrators to rapidly change configurations as performance requirements demand.

Putting theory into practice, Masergy's Software Defined Platform accelerates IT transformation by providing the foundation for an open, automated and programmable network fabric. Our Software Defined Platform is the foundation for our three essential solutions: hybrid networking, managed security and cloud communications.

SDN enables us to build intelligent analytics, automation and service control into all of our solutions.

Here are some of the many benefits of our Software Defined Platform:

- A high-availability, highly resilient hybrid network environment that provides an optimal client and application experience
- A secure, hybrid WAN architecture that permits dynamic traffic engineering across both private and public domains, delivering seamless performance and consistent manageability
- Administrators are afforded full visibility into business-critical applications and the ability to prioritize traffic based on performance, security and business policy needs
- Remote sites and branch offices can be added to the corporate network quickly and with little-to-no on-site administration

VIRTUALIZATION

Network Function Virtualization (NFV) as a central tenant of our Software Defined Platform. NFV is poised to transform the world of networking as part of a larger shift from rigid, legacy networks where hardware and software are proprietary and tightly integrated, to modern networks that are software-driven and programmable. This gives network architects and administrators a new way to design, deploy and manage network capabilities.

Masergy has implemented NFV in its recently introduced Managed Network Functions f(n). We offer a family of fully managed, distributed network functions that can be delivered in the way that best suits your needs, whether that's on premises, in the cloud, or virtualized via software.

The solution offers Virtual Functions f(n) that lets companies add routing and firewall capabilities in software on their existing Masergy network interface device, eliminating the need for proprietary network appliances and on-site administration.

Our Premise Function f(n), is a complete lifecycle management solution for enterprises, which covers essential on-premises networking functions, including routers, firewalls and session-border controllers. And a third component, Cloud Functions f(n), help companies deliver essential network functions as cloud services over the Masergy network.

> *"Masergy was able to custom design our hybrid network to meet our unique application performance requirements. It's outcome-based approach and ongoing superior support have convinced us we selected the right partner for our needs."*
>
> Patrick Tisdale, CIO – McKenna, Long & Aldridge, LLP

FLEXIBLE BY DESIGN

SDN transforms enterprise networks into modular, scalable assets that can be assembled and rearranged as business needs require. It also reduces IT complexity through automation.

Masergy is helping customers accelerate their IT transformation efforts, providing the foundation for an open, automated and programmable environment. This, in turn, frees up IT staff to focus on strategic, business-driven innovations and less time "keeping the lights on."

MASERGY
Performance Beyond Expecations

For more information, please visit https://www.masergy.com

Compared with legacy approaches, Masergy's NFV offers three compelling advantages:

1. **Extended Flexibility:** Masergy's Managed Functions f(n) gives enterprises complete control over their distributed network resources–plus the ability to scale up new services and decommission outmoded network capabilities as business needs change.
2. **Rapid Deployment:** NFV lets organizations add, remove, configure and modify network services in real time. Rather than ordering and shipping network appliances to branch offices and remote locations, it lets you take advantage of innovative new services and deploy them over your network via software updates.
3. **Lower Costs:** Our managed Network Functions f(n) reduces CAPEX because an organization no longer needs to purchase specialized hardware in many instances. And OPEX drops because of the way NFV lowers the need for dedicated hardware, support personnel and equipment maintenance.

Contact us for a free consultation.

Corporate Headquarters (USA):
2740 North Dallas Parkway, Suite 260
Plano, TX 75093 USA
Phone: +1 (214) 442-5700
Fax: +1 (214) 442-5756

European Headquarters (UK):
29 Finsbury Circus
Salisbury House 5th Floor
London, EC2M 5QQ UK
Phone: +44 (0) 207 173 6900
Fax: +44 (0) 207 173 6899

Extending Service Assurance into SDN and NFV Environments

SOLUTION BENEFITS

NETSCOUT's Adaptive Service Intelligence™ (ASI) technology empowers enterprises and service providers to fully realize the benefits of SDN and NFV CapEx and OpEx efficiencies by reducing deployment risk.

- Accelerates migration to virtualized infrastructures with confidence.
- Provides service visibility without compromising user and customer experience.
- Protects and enhances performance of traditional, non-SDN/NFV, deployments.

Solution Core Functionality

NETSCOUT's nGeniusONE™ Service Assurance platform and ASI technology deliver real-time, actionable traffic-based intelligence capabilities.

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

Challenges

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 lower cost. 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 SDN and NFV CapEx and OpEx efficiencies, enterprises and service providers need a comprehensive service delivery monitoring capability which offers end-to-end visibility across physical, virtual, and hybrid environments. To be truly beneficial, the tool needs to offer rapid service triage capabilities to reduce the mean time to resolution (MTTR), 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 IT and Operations teams, and lacks the ability to provide an end-to-end 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 disparate 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 significantly increased mean time to resolution, drastically extended service outages, reduced quality of end-user experience or loss in worker productivity.

Solution Overview

NETSCOUT® offers rapid 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 using one cohesive, consistent set of metadata, based on packet flow data, for service provider and enterprise services. This metadata is generated by the patented Adaptive Service Intelligence technology running on NETSCOUT's physical and virtual 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 points across the service delivery infrastructure using physical and virtual appliances. The packet flow data collection and aggregation is passive and noninstrusive and can scale to collect any required volumes of data across physical, virtual, and hybrid environments.

The nGeniusONE Service Assurance platform aggregates, correlates, and contextually analyzes the metadata gathered from NETSCOUT's physical and virtual Intelligent Data Sources. It then creates real-time holistic views of service performance, establishes performance baselines, and facilitates service-oriented troubleshooting workflows.

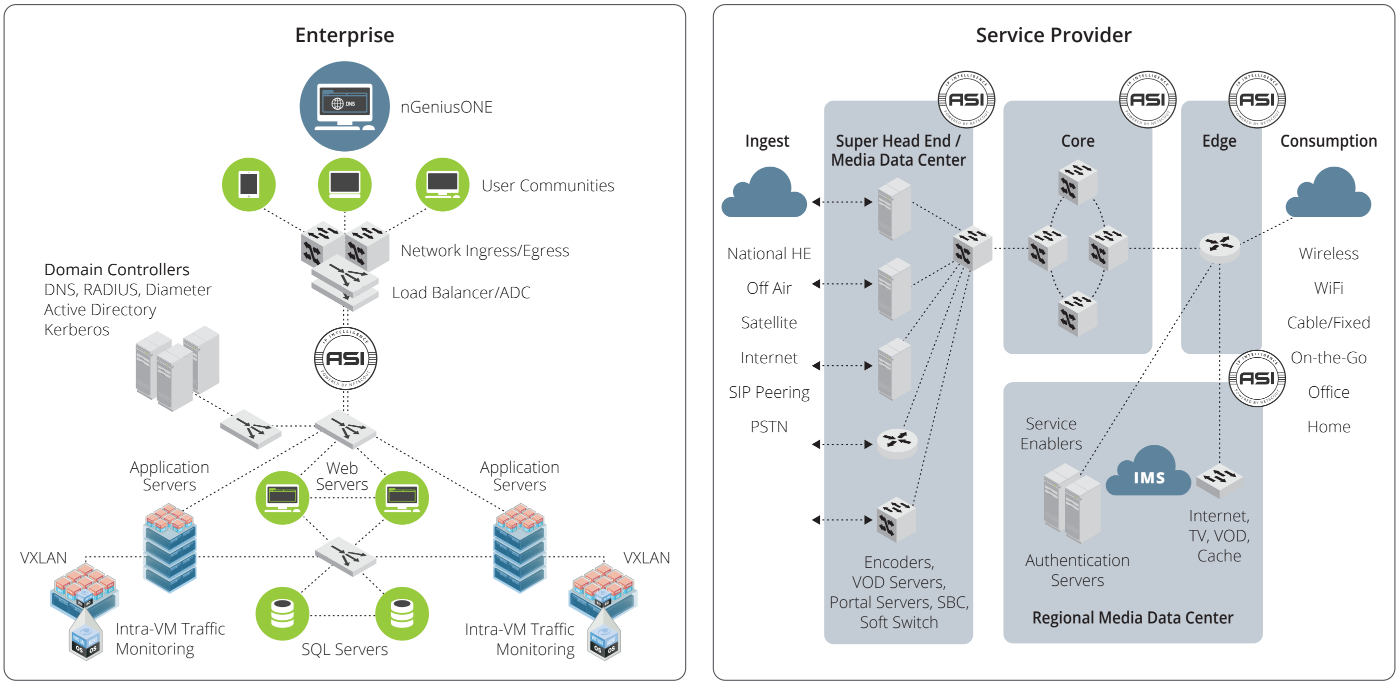


Figure 1: Service Instrumentation in Enterprise and Service Provider Environments.

Core Technologies

NETSCOUT's unique ability to gain a pervasive end-to-end visibility into the service delivery environment, and enable rapid service triage is centered on NETSCOUT's ASI technology, utilizing packet flow data, and providing scalable packet flow access.

Adaptive Service Intelligence (ASI)

Adaptive Service Intelligence is patented technology which uses rich packet-flow data to generate highly scalable metadata that enables a comprehensive real-time and historic view of service, network, application, and server performance. This powerful packet inspection and data mining engine runs on NETSCOUT's Intelligent Data Sources generating metadata based upon actual session traffic in real time as the packets cross physical or virtual links. NETSCOUT's ASI technology is the foundation of a highly scalable service delivery monitoring architecture which seamlessly collects, normalizes, correlates, and contextually analyzes data for all services: voice, data, and video.

Leverage 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 Packet Flow Switches and TAPs provide the foundation for a scalable monitoring architecture needed for service assurance. NETSCOUT's nGenius Packet Flow Switches (PFS) filter, aggregate, and distribute the targeted data to NETSCOUT's Intelligent Data Sources in a transparent, selective, and efficient manner. 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.

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 integrating NETSCOUT's ASI technology into a virtual machine (VM), functioning as a virtual Intelligent Data Source. NETSCOUT's VM either analyzes the intra-VM traffic in a self-contained virtualized mode or redirects the traffic to an external NETSCOUT Intelligent Data Source for analysis.
- **Traffic between VMs that reside in different hypervisors** is monitored by NETSCOUT 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 Comparison

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.
Rapid Service Triage	Reactive and time-consuming triage result in poor user experience, and extended service downtime impacting multiple users.	Rapid service triage helps resolve service degradation in real time before large numbers 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 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 return on investment in performance management by gradually expanding the solution over time.

About NETSCOUT Systems, Inc.

NETSCOUT Systems, Inc. (NASDAQ:NTCT) is a market leader in real-time service assurance and cybersecurity solutions for today's most demanding service provider, enterprise and government networks. NETSCOUT's Adaptive Service Intelligence (ASI) technology continuously monitors the service delivery environment to identify performance issues and provides insight into network-based security threats, helping teams to quickly resolve issues that can cause business disruptions or impact user experience. NETSCOUT delivers unmatched service visibility and protects the digital infrastructure that supports our connected world. To learn more, visit www.netscout.com.

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

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

Radware SDN applications improve application security, performance, and availability by integrating ADC and security intelligence with SDN to optimally analyze and forward traffic enhancing network services. Radware SDN applications integrate with the SDN application control plane and interact with the SDN controller to work with the Radware technologies throughout the application infrastructure.

Radware SDN-enabled ADC and security services transform applications from device-based solutions to become network wide services that intelligently divert traffic to service engines. Radware enhances SDN functions by leveraging our Virtual Application Delivery Infrastructure (VADI). This enables an EveryWare network service paradigm where applications are available anywhere and everywhere.

Key benefits of the Radware SDN network service infrastructure include:

- **Intelligent application delivery and security –** Optimal application service delivery
- **Easy implementation -** Improved operational efficiency of network management
- **Lower overall network service solution costs** – Deploy network services as needed
- **Greater scalability** – Scale network services throughout the network
- **Easier operational control** – Streamline network operations

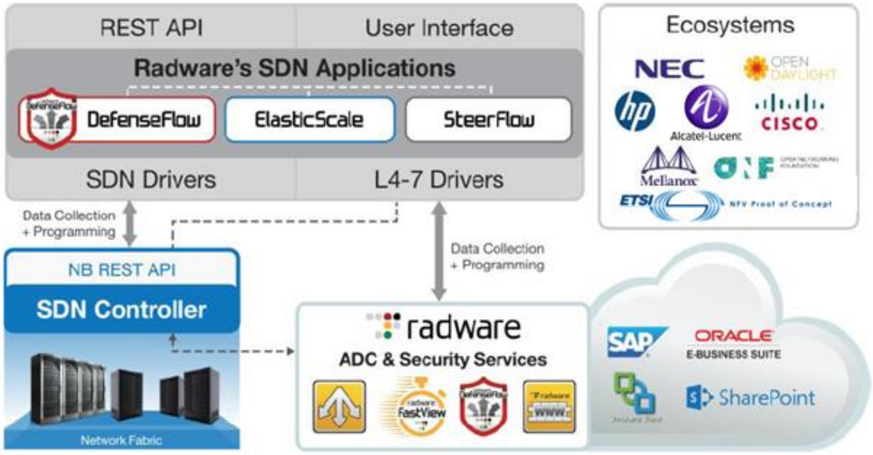
DDoS Protection as a Native SDN Application

DefenseFlow is an SDN application features an adaptive, behavioral-based DoS attack detection engine and a traffic steering mechanism taking advantage of the software defined network elements for attack mitigation. DefenseFlow delivers a necessary security control plane for SDN-based networks.

SDN & NFV for a Scalable Application Delivery Network

Radware offers Alteon VA for NFV – the industry's first and highest performing ADC designed from the ground up to run in NFV environments. Alteon NFV provides a unique value proposition consisting of CAPEX/OPEX reduction, vendor agnostic technologies, high performance, enhanced scalability, orchestrated elasticity, and improved network service agility.

Radware's ElasticScale is an SDN application that wraps existing network service virtual appliances, including Alteon NFV to consistently deliver network services in an elastic network environment. ElasticScale can be utilized to help providers adopt network functions virtualization paradigms.



Partnering for Success: Our SDN and NFV Ecosystem

The SDN and NFV eco-systems are a critical focus for Radware. Through partnerships with the industry's leading SDN and NFV consortiums and vendors, Radware ensures customers that our application delivery and security solutions integrate successfully into target architectures.

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.

Securing End-User Quality of Experience from the Cloud

There are many applications an enterprise will consider as mission-critical to their business. While it varies by enterprise, some example applications include customized CRM, web-based retail, accounting, and billing. Sonus has a long and successful history of securing and optimizing the end-user experience for real-time communications. As applications continue to migrate to the Cloud, Sonus is applying that knowledge to optimize mission-critical applications that are sensitive to IP transport.

As both service providers and enterprises look to embrace cloud-based environments, there remain some significant challenges that need to be addressed with respect to security, interoperability, portability, quality of service, quality of experience, and performance guarantees.

In a cloud-based environment, service providers must offer connectivity to an enterprise customer that is extremely resilient in order for mission-critical applications to be trusted and operated. The traditional way of provisioning, managing, and selling their network assets is no longer dynamic enough to keep up with the new demands of data center connectivity for the enterprise. Service providers have some challenges. They have to deal with competitive pressures that drive down pricing, yet also be responsive with the delivery of network resources and bandwidth connectivity that mission-critical applications require.

As enterprises will choose between various competing service providers, an additional important differentiator that needs to be addressed is perceived service quality. A service provider should be able to transparently monitor and react quickly to any service quality problems before an enterprise is aware. An optimal Quality of Experience (QoE), when end-users judge the usability of an application based on their own experience, must be achieved, while constraining the application to behave as efficiently as possible to minimize operational costs.

For today's enterprises/CIOs, they need connectivity solutions that allow them to manage their networks more intelligently and dynamically, defining end-to-end policies that align transport with mission-critical applications to deliver a high QoE within their tight operational budgets. The ability to understand and manage QoE for end-users provides a great opportunity to set themselves apart.

What is necessary to meet these needs for both service providers and enterprises requires new approaches that guarantee adherence to concerns on security, as well as to industry requirements for lifecycle management of the services and network resources.

Combining the Intelligence of the Session and Network Control Layers

Sonus provides a solution that combines session layer intelligence with software-defined networking intelligence at the network layer.

Sonus' Session Border Controller (SBC) SWe, integrated with VellOS, Sonus' virtualized network control platform, enables the sharing of security, and policy management information between the session layer and the network control layer. The application-specific intelligence from the Sonus SBC SWe, combined with VellOS' knowledge of traffic flows at the network control layer, gives service providers the ability to offer much higher levels of quality of service than ever before, guaranteeing bandwidth for specific mission-critical applications.

The Sonus solution provides a holistic, systems approach to security—providing a security perimeter in real-time at the network edge. As a result, enterprises can make informed choices and dynamically compose and personalize services in a secure way through transparent interaction with the IP session and transport layer.

The Sonus solution enables delivery of mission-critical applications with an assurance of service level agreements (SLAs) without over-burdening the network. With this holistic view of how one network can intelligently optimize packet flows based on application prioritization, a service provider or enterprise will have a solution that monitors service parameters (like throughput) and automatically proactively react if network conditions may result in QoE degradation.

The combination of the Sonus SBC SWe and VellOS enables a guarantee of SLAs for specified bandwidth in real time for mission-critical applications. By integrating session layer intelligence with network control intelligence, data center network connectivity and cloud-based service delivery are optimized.

About Sonus Networks

Sonus enables and secures real-time communications so the world's leading service providers and enterprises can embrace the next generation of SIP and 4G/LTE solutions, including VoIP, video, instant messaging, and online collaboration. With customers in more than 50 countries and nearly two decades of experience, Sonus offers a complete portfolio of hardware-based and virtualized Session Border Controllers (SBCs), Diameter Signaling Controllers (DSCs), Cloud Exchange Networking Platform, policy/routing servers, and media and signaling gateways. For more information, visit www.sonus.net or call 1-855-GO-SONUS. Sonus is a registered trademark of Sonus Networks, Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Sonus Networks North American Headquarters

4 Technology Park Drive
Westford, MA 01886
U.S.A.
Tel: +1-855-GO-SONUS

Sonus Networks APAC Headquarters

1 Fullerton Road #02-01
One Fullerton
Singapore 049213
Singapore
Tel: +65-68325589

Sonus Networks EMEA Headquarters

Edison House
Edison Road
Dorcan, Swindon
Wiltshire
SN3 5JX
Tel: +44-14-0378-8114

Sonus Networks CALA Headquarters

Homero No. 1933-902
Col. Los Morales, C.P. 11510
Mexico City, Mexico
Distrito Federal
Mexico Tel: +52-55-1950-3036
Int'l Tel: +1-978-614-8741

To learn more, call Sonus at 855-GO-SONUS
or visit us online at www.sonus.net

Microsoft Partner
Gold Communications

Voice
Unified Communications
Business Productivity Solutions
Midmarket Solution Provider

The content in this document is for informational purposes only and is subject to change by Sonus Networks without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Sonus Networks assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Sonus Networks, Sonus Networks has no obligation to develop or deliver any future release or upgrade, or any feature, enhancement, or function.

Sonus™
Cloud communications made smarter