The 2016 Guide to SDN and NFV

Part 3: The Operational Impediments to Implementing SDN

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 third of the serial publications. It will focus on describing the operational impediments to the broad adoption of SDN. 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. The Use Cases and Business Considerations 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 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.

The Guide contains the results of a survey that was distributed in October 2015. Throughout The Guide the 131 network professionals who completed the survey will be referred to as The Survey Respondents.

The Operational Implications

> ***One of the implications of adopting SDN is that is increases the need for a DevOps model.***

A detailed discussion of DevOps is contained in a subsequent chapter of The Guide.

Security

Background

Two examples of how SDN can enhance security were already discussed. In one of those examples, security services were implemented based on OpenFlow-based access switches filtering packets as they enter the network. In the second example, role based access is implemented by deploying a role-based resource allocation application that leverages the control information and capability of the SDN controller. Another security related use case is to leverage the control information and capability of the SDN controller to provide DDoS protection.

Some of the security challenges related to SDN are described in *SDN Security Considerations in the Data Center*. As pointed out in that document:

- 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.

Other security-related considerations include that IT organizations should:

- Implement measures to deal with possible control flow saturation (controller DDOS) attacks;
- Harden the SDN controller's operating system to ensure availability of the controller function;
- Implement effective authentication and authorization procedures that govern operator access to the controller.

SDN creates security opportunities and security challenges.

Vendor Questions

Below are some of the questions that network organizations should ask vendors relative to the security of their SDN solution.

- What functionality does your solution support in order to ensure the security of end-to-end communications?
- How are the components of your solution designed for security? For example, what steps have been taken to harden the SDN controller's operating system?
- What functionality does your solution support in order to ensure the security of communications between the components of your solution?
- What capability does your solution have to detect security breaches?
- How does your solution logically separate traffic?
- What measures are available to deal with possible control flow saturation (controller DDOS) attacks?
- Describe any SDN-based solutions that are available both to detect the communications patterns of spurious traffic (e.g., botnets, spam, and spyware) from internal end systems and to block or quarantine the source.
- How does your solution make implementing security notably less complex than the traditional ways of implementing security?
- What tests have been run to verify the effectiveness of the security measures that have been taken? Is it possible to see those test results?

Cloud Orchestration

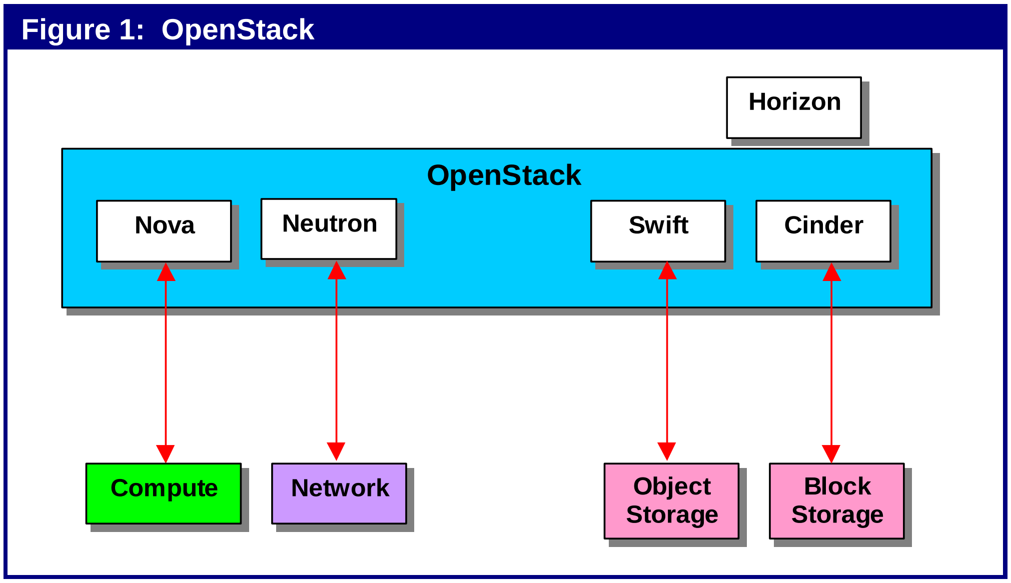
Cloud Orchestration platforms have evolved as a means of automating and facilitating the process of configuring pools of data center resources in order to provide a range of cloud or cloud-like services, such as Infrastructure as a Service (IaaS) solutions. The Orchestrator's role is to manipulate the basic resources of the data center (i.e., VMs, networks, storage, and applications) at a very high level of abstraction to create the service. Orchestration is most effective when the data center is fully virtualized, facilitating software control, reconfiguration and automation. As a result, there is a natural affinity between Orchestration and SDN controllers.

OpenStack is a cloud computing orchestration project offering free open source software released under the terms of the Apache License. The project is managed by the OpenStack Foundation, a non-profit corporate entity established in September 2012 to promote OpenStack software and its community. Apache CloudStack is another open source Apache Licensed orchestration system. Eucalyptus is a third open source orchestrator with tight technical ties to Amazon Web Services (AWS).

In addition, there are a number of proprietary orchestrators that offer open APIs to allow integration across vendor boundaries. These include VMware's vCloud Director and IBM's SmartCloud Orchestrator.

Figure 1 shows a block diagram of the OpenStack system, including the OpenStack modules that are used to control resource pools in the data center, including Horizon and Neutron.

Figure 1: OpenStack



Horizon is the OpenStack Dashboard that provides administrators and users a graphical interface to access, provision and automate cloud-based resources. The dashboard is one of several ways users can interact with OpenStack resources. Developers can automate access or build tools to manage resources using the native OpenStack API or the EC2 compatibility API. The dashboard also provides a self-service portal for users to provision their own resources within set limits.

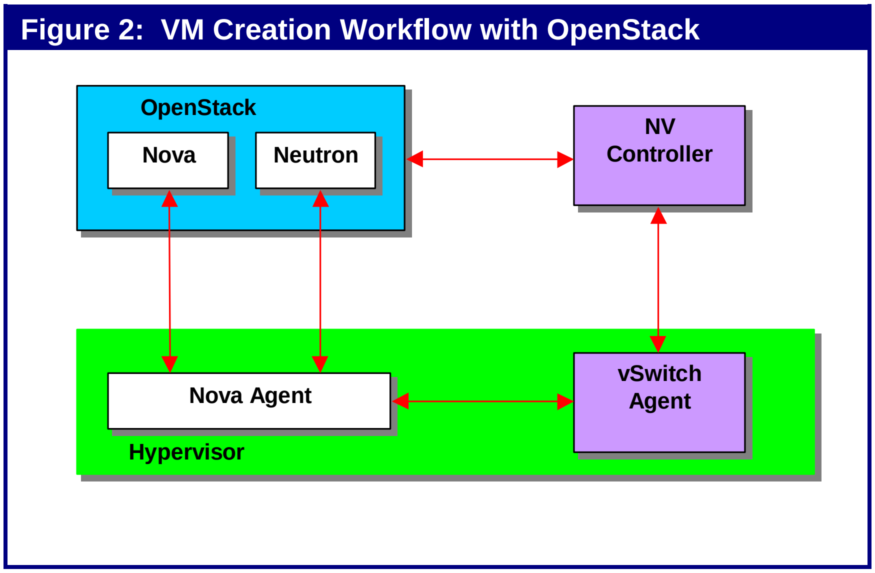
Neutron (formerly called Quantum) allows users to create their own networks, provide connectivity for servers and devices, and control traffic. With appropriate Neutron plug-ins, administrators can take advantage of various SDN solutions to allow for multi-tenancy and scalability. A number of drivers/plugins are included with the OpenStack source code. OpenStack networking also has an extension framework allowing additional network services, such as intrusion detection systems (IDS), load balancing, firewalls and virtual private networks (VPNs) to be deployed and managed.

In conjunction with the Orchestrator, the role of the SDN controller is to translate the abstract model created on the Orchestrator into the appropriate configuration of the virtual and physical resources that will deliver the desired service. For example, the Orchestrator 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.

Figure 2 provides a high level depiction of how an orchestrator (OpenStack) and an overlay-based SDN controller might interact to place a VM into service within a VN.

Figure 2: VM Creation Workflow with OpenStack



The **Nova** compute module in OpenStack instructs the Nova Agent in the hypervisor to create the VM. The Nova agent communicates with the Neutron module in OpenStack to learn the network attributes of the VM. The Nova agent then informs the vSwitch agent to configure the virtual network for the VM and then the controller provides the route table entries needed by the vSwitch.

Management

Background

As described in a preceding section of The Guide, one of the two primary factors driving the deployment of SDN is the belief on the part of network organizations that implementing SDN will ease the burden of configuration and provisioning. However, as described below, the adoption of SDN also creates management challenges. This leads to the conclusion that:

SDN creates both management opportunities and management challenges.

A related conclusion is that:

> ***In SDN environments the challenges associated with end-to-end service performance management are more demanding than they are in traditional network environments.***

This follows because in a SDN environment there is a need to monitor additional components, such as SDN controllers, in an environment that is a combination of physical and virtual resources and which is changing dynamically. From a service performance management perspective, the SDN controller can be viewed as a *service enabler* that needs to be instrumented and monitored just as any other application server. Whether it is OpenFlow or some other protocol that enables communications between the SDN controller and the network elements that protocol needs to be monitored the same way as any other protocol. In similar fashion, the combination of virtual and physical network elements need to be instrumented end-to-end and monitored across the entire infrastructure. One of the management challenges that applies across multiple tiers of the SDN architecture is the requirement to manage the messaging that goes between tiers; e.g., between the application tier and the control tier as well as between the control tier and the infrastructure tier.

At the infrastructure tier, one of the primary challenges is to perform element management potentially of both virtual and physical network elements. One of the management challenges at the control layer results from the fact that the controller is in the data path for new flows entering the network. During periods when many new flows are being created, the controller can potentially become a performance bottleneck adding significant latency for flow initiation. Performance management systems need visibility not only into application performance but also controller performance in processing flows. A set of management challenges that occurs at the application layer stem from the requirement to ensure acceptable performance. One thing this means is that network management organizations must have visibility into the SLA requirements of the application so that resources can be dynamically allocated to meet those requirements if that is appropriate.

Due to the mobility of VMs or the need to change QoS settings, topology changes can occur in a matter of seconds rather than the days or weeks required for changing software/hardware relationships in traditional networks. In order to accommodate and leverage the virtualization technologies:

Network management organizations need tools that enable them to be able to dynamically discover, procure, allocate and reconfigure network resources.

Looking at network virtualization as an application of SDN, another one of the performance management challenges stems from the fact that one of the primary benefits of overlay-based SDN solutions is the ability to support multiple virtual networks that run on top of a physical network. As a result:

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 also 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.

Given the challenges described above as well as the requirement to integrate the traditional legacy environment with the emerging software-centric environment:

Applications and services need to be instrumented end-to-end.

The physical and virtual environments should be instrumented independently and network management organizations should have the ability to contextually correlate and consolidate the two management datasets into one consistent and cohesive dataset which offers operational insight into the end-to-end service delivery.

Vendor Questions

Below are some of the questions that network organizations should ask vendors relative to the management of their SDN solution.

- How extensive is the management functionality that you provide. Include in your answer:
  - The type of management data that is gathered and where it is gathered;
  - Where the management data is stored and where it is processed;
  - How your solution performs monitoring of network and application performance;
  - The level of visibility that your solution provides into network and application performance;
  - The ability of your solution to enable rapid root cause analysis;
  - The level of visibility that your solution provides into the performance of applications and services acquired from a cloud provider;
  - The type and the extent of analytics that are part of your solution.
- What functionality does your solution provide to enable a company to implement and support SLAs for varying types of applications?
- How does your solution provide event correlation and fault management?
- Describe the integration or potential integration that exists between the management tool that you provide to manage your solution and other common business intelligence, security and management tools, whether provided by your company or by a third party.
- Describe the integration or potential integration of your solution with leading orchestration solutions.
- What type of management interface do you provide into your SDC controller? For example, is it based on REST? On something else?
- Describe the ability of your solution to monitor the SDN controller. Include in that description your ability to monitor functionality such as CPU utilization as well as flow throughput and latency. Also describe the statistics you collect on ports, queues, groups and meters; and the error types, codes and descriptors you report on.

- What type of management interface do you provide into your management tool? For example, is it based on REST? On something else?
- Describe the ability of your solution to monitor the network elements in your solution. Include in that description the key performance metrics that you monitor and report on. Also, can the performance data gathered by SDN switches (e.g., counters and meters) be integrated with data from traditional performance management tools based on SFlow and SNMP?
- Describe how your solution monitors the messages that go between the SDN controller and the SDN switches.
- Describe the ability of your solution to provide visualization of traffic flows and service quality.

Organizational Impact

SDN can be viewed as being a part of a broader movement to implement all IT functionality in software, referred to as Software Defined Everything (SDE). The primary drivers of the SDE movement are the need to support a more agile IT operational model as well as increasingly more agile business processes.

As described in *The Changing Role of the IT & Network Professional*, the adoption of a 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 told that SDN is part of a broader movement to implement all IT functionality in software, referred to as Software Defined Everything (SDE). The Survey Respondents were asked how much of an impact they thought that the SDE movement will have on the structure of their company's IT organization over the next two years. Their answers are shown in **Table 1**.

Table 1: Impact of SDN on Organizational Structure

Impact	Percentage of Responses
Very Significant Impact	11%
Significant Impact	19%
Moderate Impact	17%
Some Impact	24%
No Impact	8%
Don't Know	21%

Almost a third of the survey respondents believe that over the next two years the ongoing adoption of software-based IT functionality will have either a significant or very significant impact on the structure of their IT organization.

When asked to indicate the type of organizational changes that would likely occur, the responses included that there would likely be:

- An accelerated transition to highly dynamic and flexible cloud architectures;
- Greater investment in logical architectures, systems design thinking and business virtualization;
- An impact on design and purchasing decisions;
- More focus on business processes;
- A redefinition of roles and responsibilities;
- A reorganization based on IT and DevOps skills.

In addition, the Survey Respondents were asked how much of an impact they thought that the SDE movement will have on the nature of their jobs over the next two years. Their answers are shown in **Table 2**.

Table 2: Impact of SDN on Jobs

Impact	Percentage of Responses
Very Significant Impact	10%
Significant Impact	19%
Moderate Impact	18%
Some Impact	24%
No Impact	11%
Don't Know	18%

Over a quarter of the survey respondents believe that over the next two years the ongoing adoption of software-based IT functionality will have either a significant or very significant impact on their jobs.

When asked to indicate the type of changes that would likely occur to their jobs, the responses included:

- We will spend less time configuring and more time planning;
- Our roles will blend and create some conflicts;
- How we design, deploy and manage networks will change;
- We will need to be re-trained on the skills necessary to support SDE;
- We will need to absorb new skills and evaluate a broader range of vendors;
- The skills needed will change from networking to programming and scripting.

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

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.

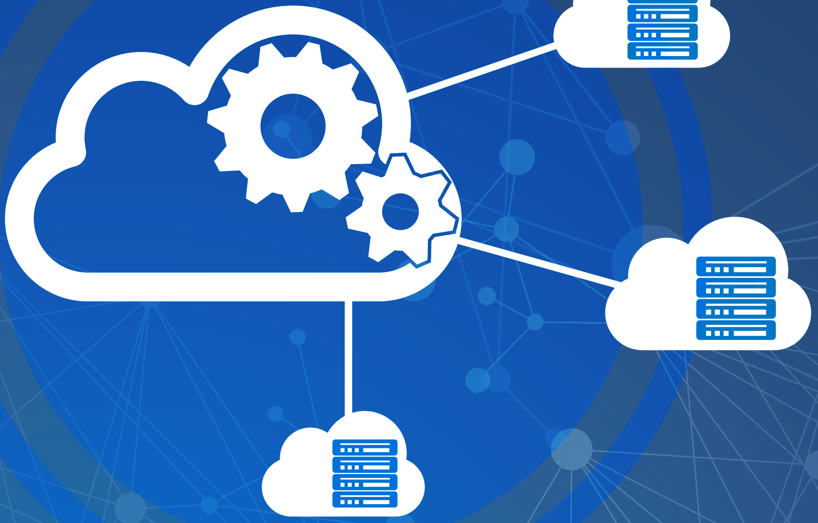
Division Cofounders:

Jim Metzler

Steven Taylor

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

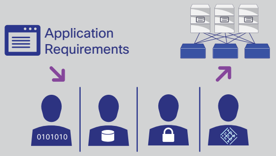
www.a10networks.com

Why Choose Application Centric Infrastructure (ACI)?

Application Deployment at the Speed of Business

Without ACI

New Application



IT administrators work in silos.

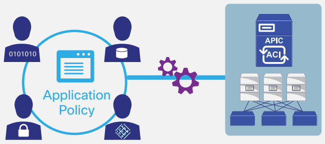
Weeks

There is no shared architectural model.

With ACI

New Application

Simpler



Faster

IT admins work at the application level.

Hours

Efficient

Shared model for policy automation.

ACI cuts deployment time and effort.

Optimal Design

Application Policy

Connectivity

Reliability

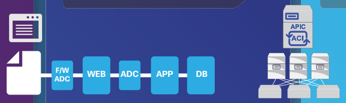
Compliance

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

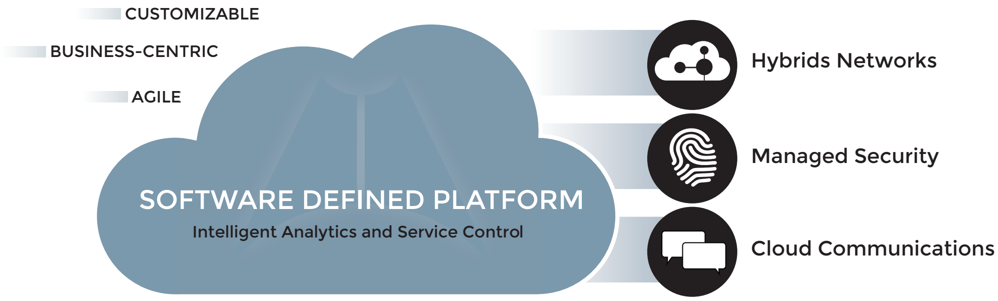
CISCO

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

SOFTWARE-DEFINED SOLUTIONS THAT ADAPT TO THE DEMANDS OF YOUR BUSINESS

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

NETSCOUT

Extending Service Assurance into SDN and NFV Environments

SOLUTION BENEFITS

NETSCOUT's Adaptive Service Intelligence^{TM} (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^{TM} 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.

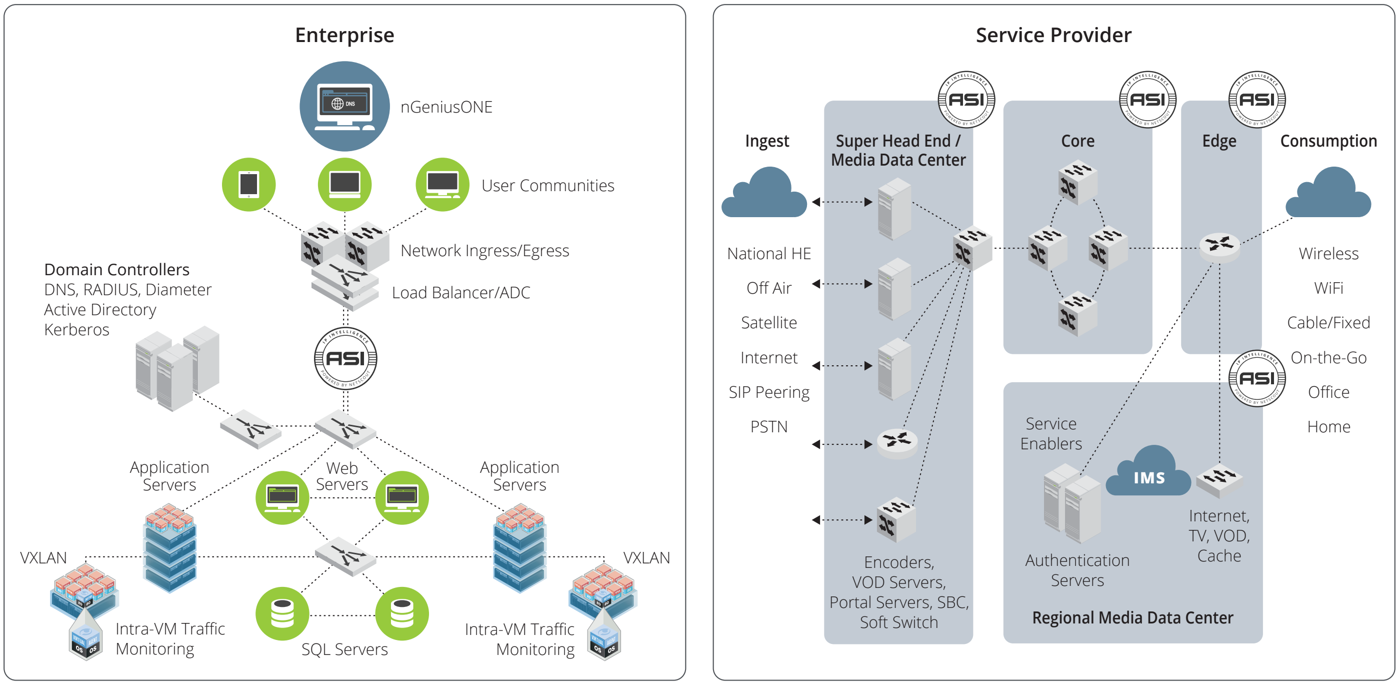


Figure 1: Service Instrumentation in Enterprise and Service Provider Environments.

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.

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

radware

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

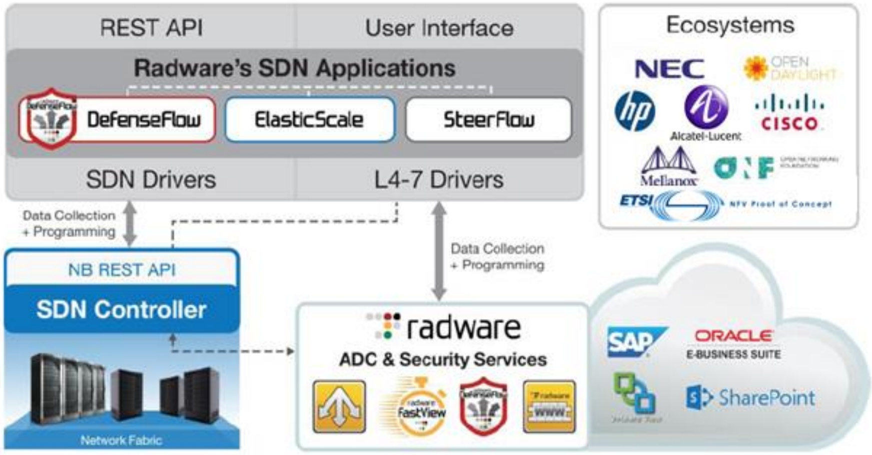
DDoS Protection as a Native SDN Application

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

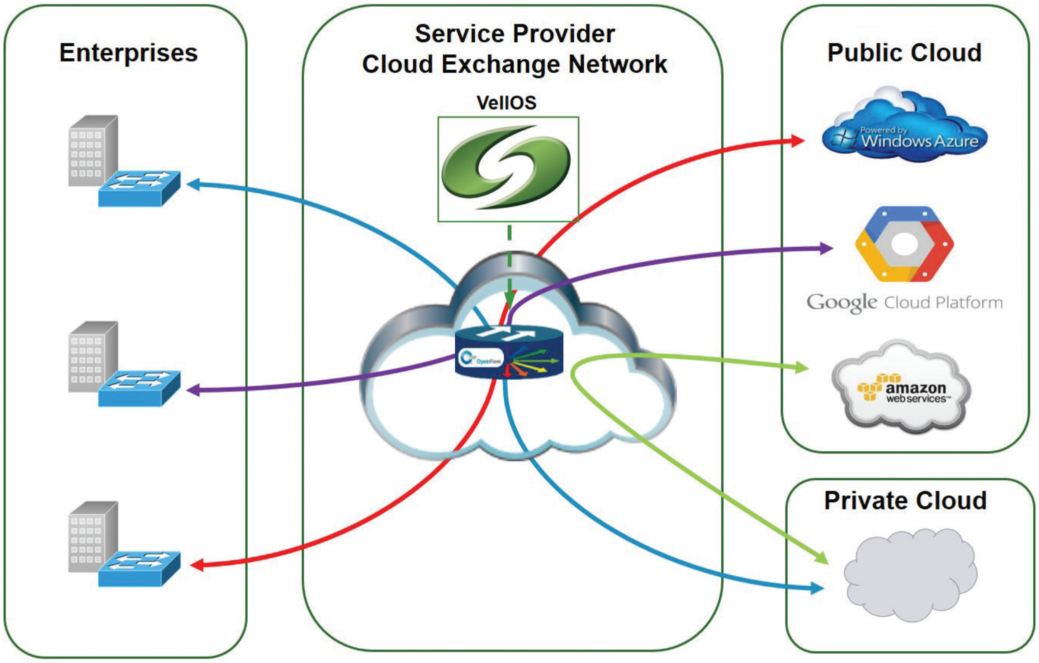
To learn more about how Radware's SDN solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.

VellOS® Cloud Exchange Networking Platform
New Cloud Services for Service Providers; Efficient Cloud Networking for Enterprises

As enterprises and service providers discover the value of cloud networking architectures, they seek technology that transcends traditional networking products and wide area networks (WANs). Traditional networking infrastructure is inadequate to address the requirements of migrating applications and data to Cloud environments. With limited capability to cost-effectively handle rapidly changing traffic dynamics, the infrastructure cannot optimize network resources, and is cumbersome to perform network-wide policy and configuration management.

VellOS is a market-leading, virtualized software-defined platform in a new class of Cloud exchange networking products that integrates private, hybrid, and public clouds into a seamless IT environment. VellOS unifies the control of the optical, Ethernet, and virtual networking planes under common open software, enabling real-time network visibility, control, and optimization.

With the application-aware network intelligence provided by VellOS, enterprises and service providers can orchestrate and dynamically deliver just-in-time data center connectivity, improve business-critical application performance, ensure business continuity, and transition the WAN into a strategic asset. Via its policy-driven architecture and logically centralized resource control, VellOS simplifies network and application roll-out.



VellOS leverages SDN to transform the Cloud Exchange Network

Dynamic Data Center Interconnect

As enterprises place increasing emphasis on the Internet and Cloud-based services to support internal and external communications and transactions, Cloud deployments must have optimal network connectivity. There are three critical aspects the cloud exchange network must address. First, connectivity should be managed in real-time, based on business priorities, including those defined in business continuity plans. Second, traffic between Data Centers should be prioritized based on business priorities for each different application. Third, bandwidth utilization should be maximized, thereby reducing the cost of Data Center connectivity.

With VellOS, business policies are automatically translated into simplified provisioning and network infrastructure configuration, on-demand connectivity based on application requirements is orchestrated, and infrastructure changes are dynamically implemented.

VellOS makes it possible to achieve significant cost savings by maximizing bandwidth utilization, as well as ensuring the availability and continuity of mission-critical business applications. As a result, service providers and Cloud hosting providers can turn their Cloud exchange network into a revenue-generating opportunity by providing Data Center Interconnect as a "Network-as-a-Service".

Real-Time Service Quality for Unified Communications

Applications that deliver real-time unified communications (UC) have specific requirements for low latency, jitter, and packet loss. When provided from the Cloud and delivered across a cloud exchange network, these applications require policies that are application-aware to ensure bandwidth allocation and packet prioritization on a per-session basis. VellOS provides API interworking with various vendors' UC implementation, so that UC traffic will get priority over other IP application traffic across the cloud exchange network. This traffic prioritization is dynamic and can be performed at the granularity of each session, each user, or each UC application.

> "SDN is one of the most transformative business and technology trends the telecomm industry has seen in decades. Faster time-to-market for new services, faster provisioning, delivery, and upgrade times for existing services, and reduced human error and lower OPEX costs from software automation are the primary reasons for adopting SDN."
>
> – Sterling Perrin,
> Senior Analyst, Heavy Reading

Security

As applications and data migrate to the Cloud, solutions previously used to secure traffic across the corporate LAN or across private lines may no longer be viable. In situations where an application relies on the cloud exchange network for security, VellOS will block unknown traffic from accessing the cloud exchange network. Only traffic from known users or devices is allowed. Data will not flow across the cloud exchange network by default. Only provisioned IP addresses that are allowed to exchange data can ARP each other. Bandwidth allocation enforcement prevents traffic flooding, as well as ping, ARP, or LLDP floods. For ease of implementation, VellOS can integrate with an existing authorization/authentication solution to validate users.

Business Continuity and Disaster Recovery

As enterprises place increasing emphasis on Internet and Cloud-based services to support their business, they require a different business continuity paradigm for their data, applications, and transactions. These enterprises must ensure they have access to Cloud-based applications and Data Centers, even during disasters, for transparent and continuous operation. The availability of application and data must flow quickly to minimize any negative impact on business operations. With VellOS, business continuity/disaster recovery policies are automatically translated into simplified provisioning and network infrastructure configuration. This ensures cloud exchange network changes are rapidly implemented in the event of unforeseen or unplanned changes in network topology or network behavior.

About Sonus Networks

Sonus brings the next generation of Cloud-based SIP and 4G/VoLTE solutions to its customers by enabling and securing mission critical traffic for VoIP, video, IM and online collaboration. With Sonus, enterprises can intelligently secure and prioritize real-time communications, while service providers can deliver reliable, secure real-time services for mobile, UC and social applications. Sonus offers an award-winning portfolio of hardware-based and virtualized Session Border Controllers (SBCs), Diameter Signaling Controllers (DSCs), Cloud Exchange Networking Platform, Policy/Routing servers and media/signaling gateways. Visit www.sonus.net or call 1-855-GO-SONUS.

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