IHS INFONETICS WHITE PAPER

Delivering Security Virtually Everywhere with SDN and NFV

July 2015

By Research Director Jeff Wilson

Table of Contents

List of Exhibits

INTRODUCTION

Without a doubt, SDN and NFV are among the most-discussed and frequently confused topics in all of networking. Though SDN and NFV have applicability beyond security, their implementation has serious impact on security architecture, and will enable a new generation of security services.

From its academic beginnings at Stanford University in 2005 to practical applications in data centers and telecommunications carrier networks during the past 4 years, **SDNs (software defined networks)** show the potential to solve significant operational problems. The Open Networking Foundation (ONF) is the group dedicated to defining and promoting SDN technology, and they define SDN as "an emerging network architecture where network control is decoupled from forwarding and is directly programmable. This migration of control, formerly tightly bound in individual network devices, into accessible computing devices enables the underlying infrastructure to be abstracted for applications and network services, which can treat the network as a logical or virtual entity." This sounds simple enough, and security is certainly one of the "services" that can be paired with logical or virtual network infrastructure.

The first important point to make about SDN is that it works in physical networks and virtual networks. Logical networks—where traditional network infrastructure (like switches and routers) is configured logically using technology like VLANs—are widely deployed today, and will be the starting place for many early SDN deployments.

To get to fully virtual networks, where all network components run in software on top of common hardware, we have to take the first step, which is **NFV (network functions virtualization).** NFV was initiated by service providers, who want to be in the driver's seat to move the industry and all vendors in the same direction—to move network functions off specialized network hardware onto commercial servers, with a goal of preventing vendor lock-in. Standards for NFV are being curated by the ETSI (European Telecommunications Standards Institute), and their work in NFV is focused on helping major telecommunications service providers streamline their networks and shed their dependence on specific vendors' hardware for key functions like BRAS, message routing, DPI, SGSN/GGSN, carrier NAT, and you guessed it—security.

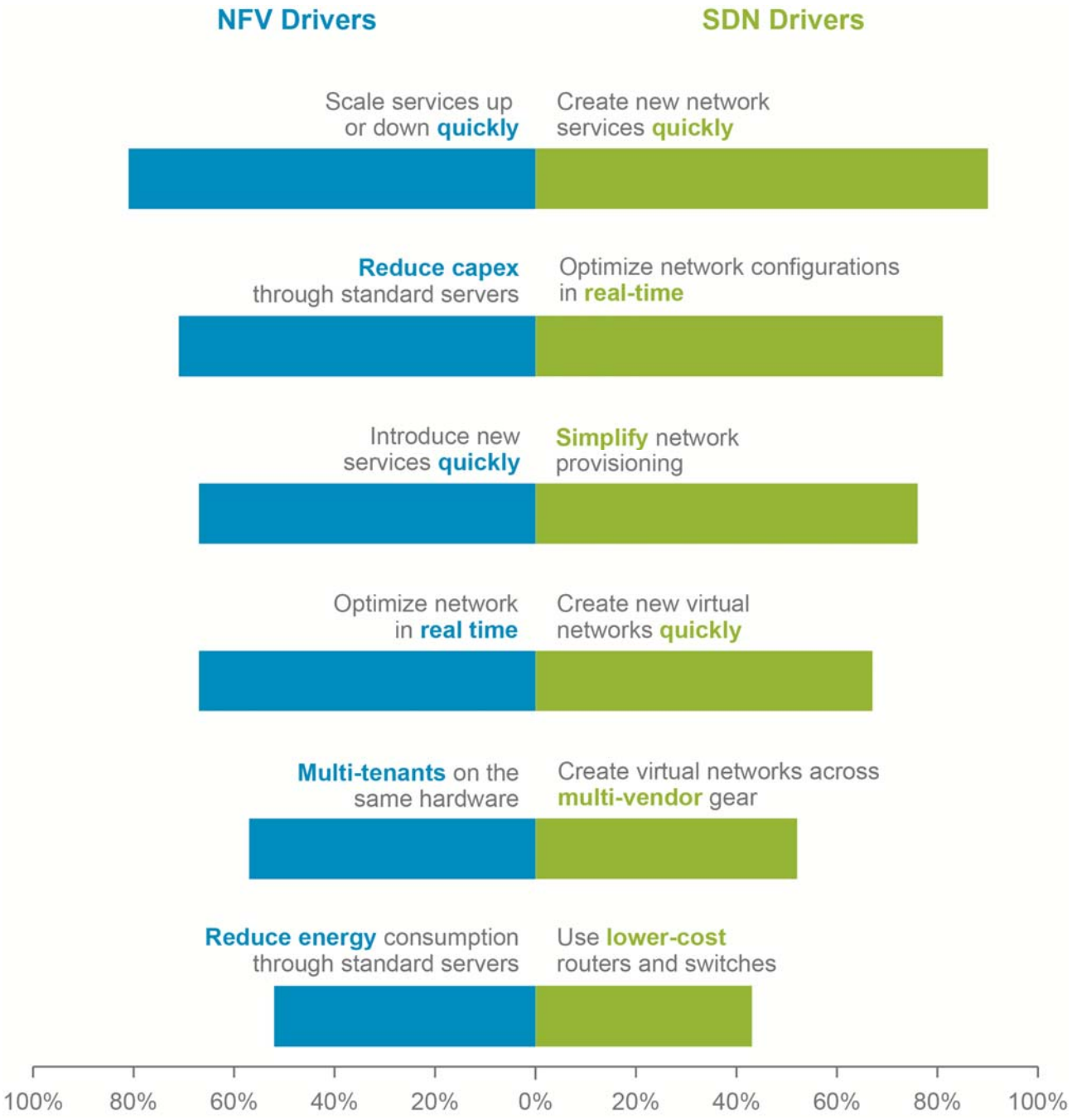
So in the end, SDN and NFV are complementary technologies and architectural initiatives aimed in the same direction: to make networks and network services more agile.

DRIVERS FOR SERVICE PROVIDERS

SDN is an architecture that abstracts control from forwarding, allowing for physical or virtual networks and services for enterprise campus and data center networks as well as large service provider data centers and telecommunications networks. Large service providers will use SDN technology (particularly SDN orchestration tools like controllers, which essentially become the brains of an SDN deployment) to provision their infrastructure and services once their network functions have been virtualized per NFV.

Service providers around the globe are very motivated to roll out solutions that leverage SDN and NFV as quickly as possible because they expect significant improvements in cost and agility, as outlined in the chart below, an excerpt from our *SDN and NFV Strategies: Global Service Provider Survey*.

Exhibit 1 **Service Provider SDN and NFV Drivers**



IHS Infonetics SDN and NFV Strategies: Global Service Provider Survey, July 2013

Looking down the list of drivers for SDN and NFV, we see that many of these benefits can be directly applied to security, and for many providers tinkering with SDN and NFV, security is among the first applications they look to deploy. With SDN and NFV in place, service providers can offer customers things like on demand advanced malware protection, cloud-based URL filtering, web application security for a cloud-based application testing and development environment, and granular customization per-application or per-tenant.

THE ROLE OF SECURITY IN SDN AND NFV

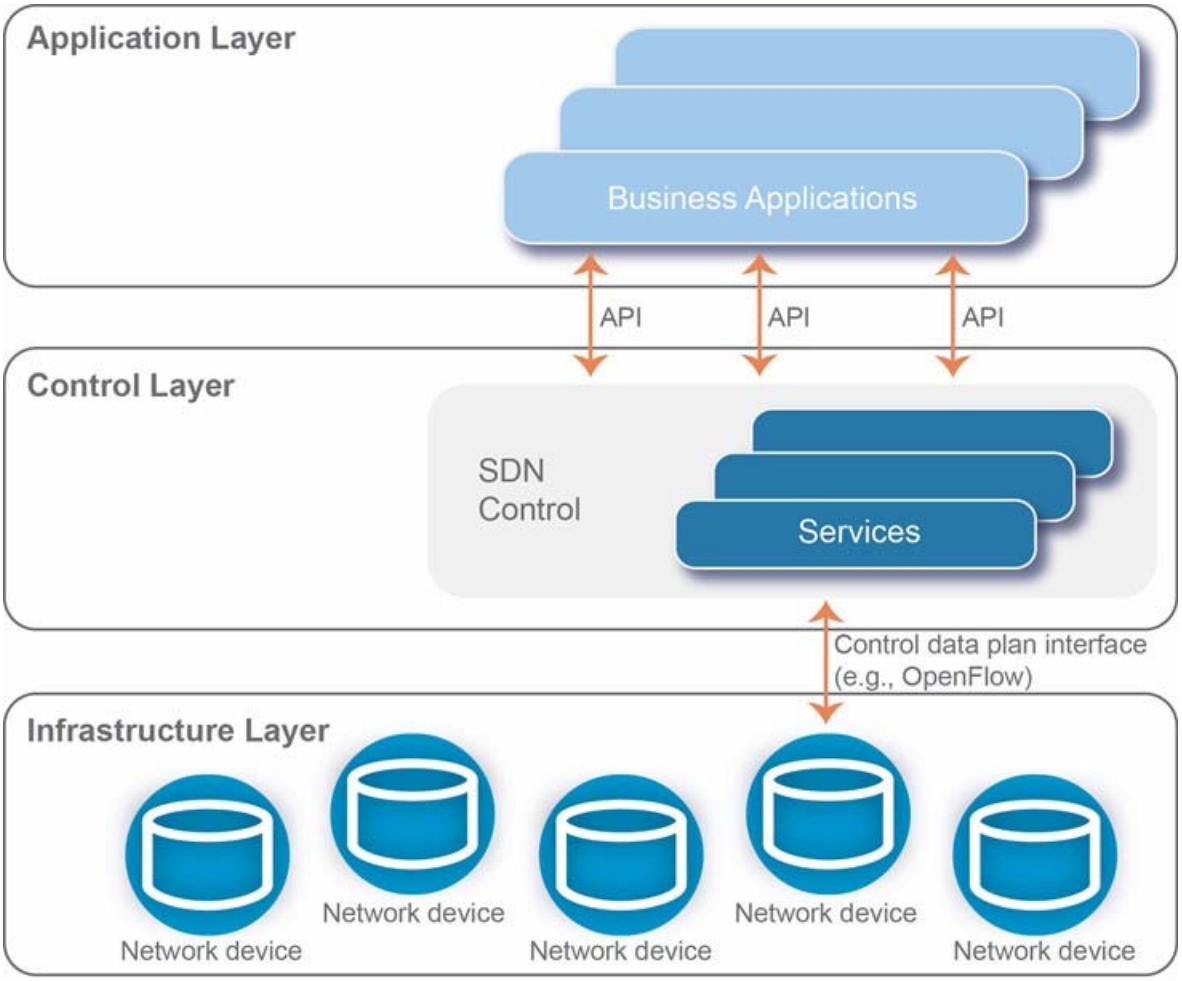
Though SDN and NFV are hot topics in networking, and will force vendors who build networking products and applications to offer new form factors and re-architect some of their solutions, security vendors have been working on adapting threat detection and mitigation solutions to work in virtualized (under a hypervisor) environments for over 5 years, typically building what they refer to as virtual appliance versions of their traditional hardware/software products.

The reason for this is quite simple: as soon as server virtualization was introduced, anyone who deployed it realized they were challenged to meet the security scale requirements of their virtualized infrastructure, and they needed a way to secure traffic moving between virtual machines—this traffic was essentially invisible to their existing threat mitigation tools. Buyers leaned on their preferred security vendors to deliver the same types of control (firewalling, anti-virus, intrusion prevention, etc.) inside the virtualized environment as outside, and thus the virtual security appliance was born.

Initially, virtual security appliances needed to be hypervisor aware, to interface directly with the buyer's chosen hypervisor so that a single virtual appliance could work in concert with the hypervisor to deliver customized security to each instance it was protecting. Security vendors had to invest resources to map their security products to the hypervisor API(s) to attain multitenant capability and visibility into east-west traffic.

As the market moves toward SDN and NFV, it is fairly easy for most security vendors to adjust the work they did building virtual appliances for hypervisors like vSphere, XenServer, or Hyper-V to work with vendors' open or closed SDN orchestration tools and controllers such as OpenStack. In short, security vendors are ready to support rollouts of SDN and NFV. In the next exhibit, which shows the basic SDN architecture, security is simply one of the network services in the center, provisioned and managed by the SDN control layer and paired with business applications above and virtualized or logical infrastructure below. In the beginning, it's unlikely that SDN controllers will communicate directly with virtual security appliances (the hypervisor is generally the intermediary), but that is where the technology and products are headed.

Exhibit 2 **SDN Architecture**

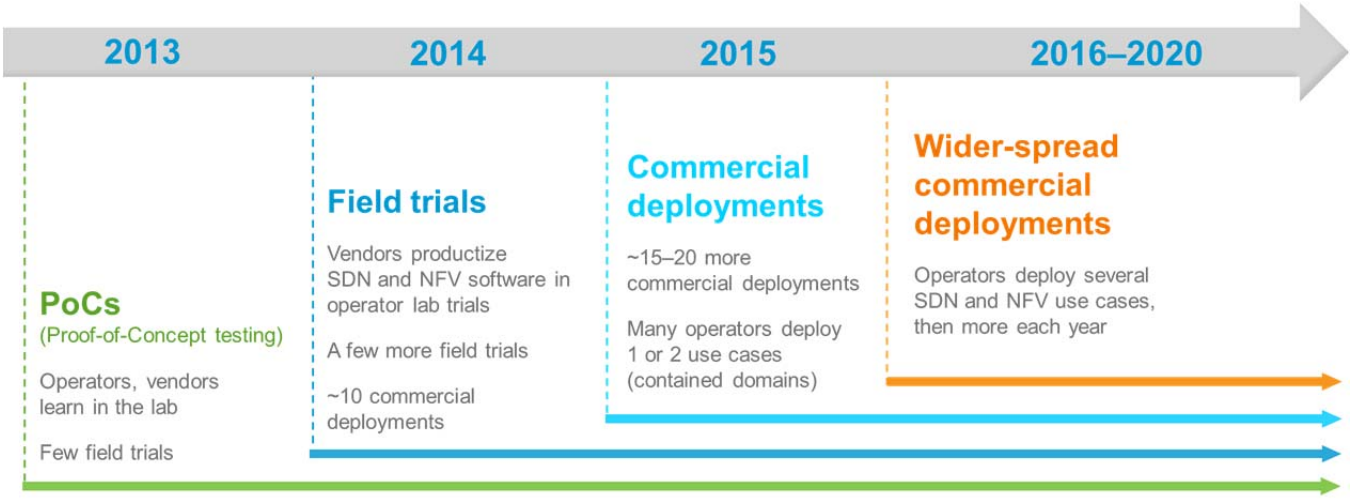


Source: Open Networking Foundation

Though the SDN controller infrastructure is the brain of the operation, the real power is in combining that orchestration capability with a wide variety of virtualized network functions (VNFs) to build customized services in a very easy way; that's the agility advantage of SDN and NFV. In security alone there are more than a dozen core functions that will become their own VNF, like firewall, web filtering, virus scanning, IPS, DDoS mitigation, web application firewall, network access control, DLP. These functions can be stitched together to building individual service offerings tailored to the customers need.

The range of solutions needed for a service provider to roll out SDN in their data centers, or to build networks and services that leverage full NFV are just starting to become widely available. As the timeline below shows, we're already into SDN/NFV field trials and some commercial deployments, and many of these trials have selected security as an early use case.

Exhibit 3 **Operator SDN and NFV Timeline, 2013–2020**



IHS Infonetics NFV Hardware and Software: Market Size and Forecasts, July 2015

To explore how SDN and NFV technology, standards, and architecture translate into security solutions for customers, we'll look at two cases: SDN in the data center to deliver a range of security tools to protect hosted/cloud infrastructure, and NFV in a large carrier network to deliver a virtual firewall to the perimeter of the customer's network, replacing a physical on-premises firewall.

SDN AND SECURITY IN THE DATA CENTER: DELIVERING FLEXIBLE CLOUD SERVICES

As the traditional hosting market (dedicated, shared, and colocation) rapidly transitions to full-featured public and private cloud services, hosting and cloud providers are looking to:

- Save money on the infrastructure they build and maintain to deliver services
- Increase the speed with which they can add to or change services
- Deliver a richer set of services to their customers

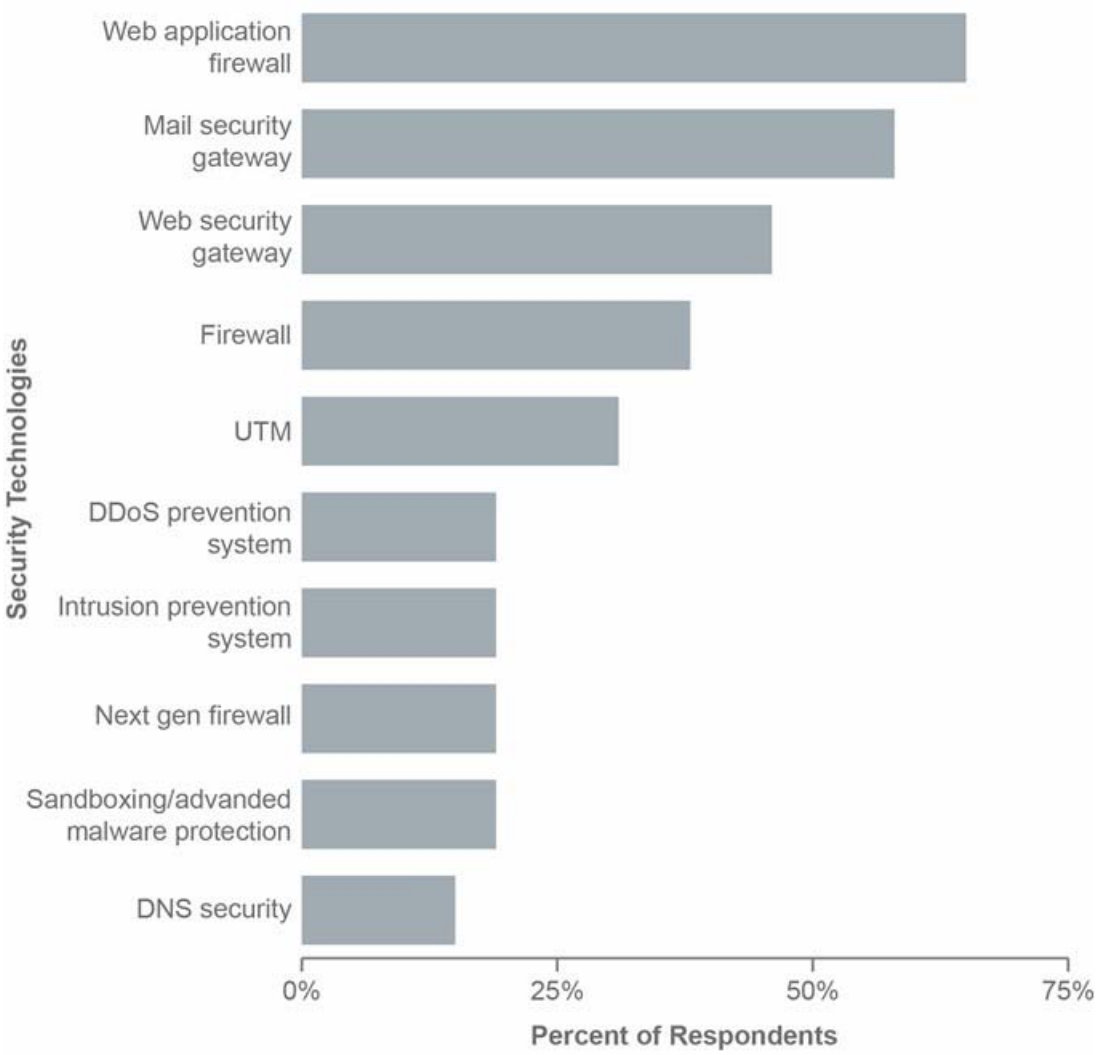
To achieve these goals, many have virtualized much of their infrastructure, and are looking to SDN orchestration platforms to help them provision and manage services. In the old days, if a customer wanted to deploy a server with a custom web-based application, but they required a specific type of security in front of that application (specific vendor or product), they had to buy colocation space, or find a hosting provider that offered dedicated hosting services and the ability to install a security appliance into the rack with their application. After that was done, they had to figure out a way to parse management of those tools between the hosting provider and the customer; not terribly agile at all.

Today, things are very different; many cloud providers offer services that can be purchased online and automatically provisioned (compute, storage, applications) and can automatically bundle virtualized security solutions that are provisioned simultaneously. Using SDN technology, cloud providers enable customers deploying a single web application on cloud infrastructure to automatically provision a virtual web application firewall (WAF) simultaneously and without human intervention. That WAF can be managed by the customer, and will follow the web application wherever it goes. In the case of something like a test deployment of a new web application, the WAF can be provisioned during testing, and easily shut down once the test is over, at no real operating cost for the hosting provider.

In more complex cases, customers looking to cloud providers to outsource portions of their network infrastructure can now buy compute, storage, and even networks, and then deploy and manage network-level security solutions (firewalls, IPS, even DDoS mitigation) virtually. To the buyer, these security tools look exactly like their hardware counterparts, but they're provisioned by the SDN controller/hypervisor and follow the virtual infrastructure wherever it goes. Solutions like this are available today from a wide range of large hosting and cloud providers (including Microsoft Azure, Amazon Web Services, and others).

In our 2014 study of 26 of the largest and most influential cloud/hosting service providers around the globe, we found plans to offer a wide range of virtual security appliance solutions to customers, with many providers offering multiple platforms from multiple vendors. With these virtual appliance platforms in place, cloud/hosting providers can begin to build customized security service offerings for their customers; we can see already that many providers have the ability to offer web application firewalls, mail security, web filtering, firewall, and DDoS mitigation via virtual appliances.

Exhibit 4 Virtual Appliances Deployed in Service Provider Data Centers



IHS Infonetics Cloud & Data Center Security Strategies & Vendor Leadership: Global Service Provider Survey, Dec. 2014

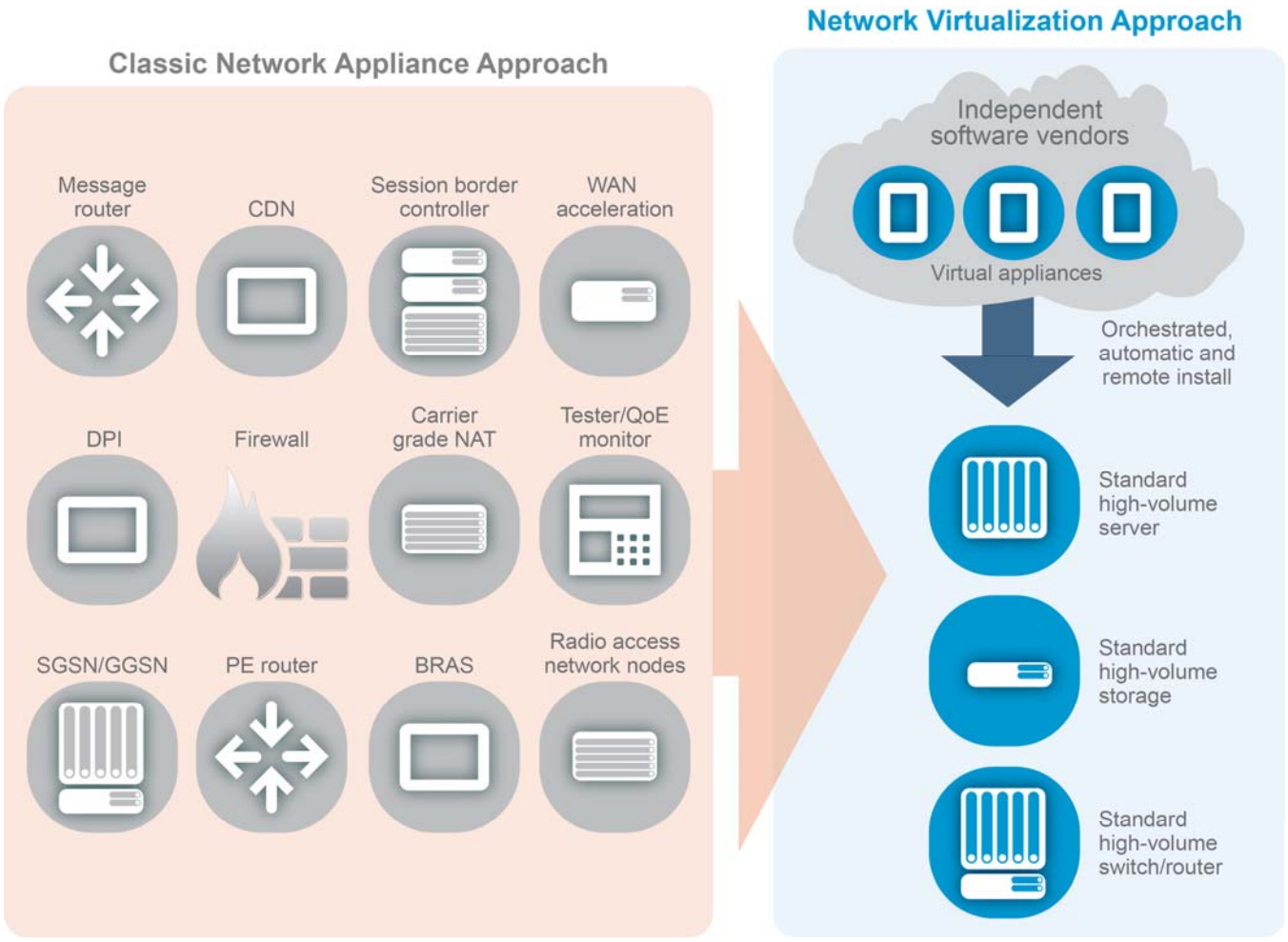
The momentum behind SDN in service provider data centers to deliver agile services (including a wide range of security services) is only going to grow, and the development done to support large providers is trickling down to enterprise customers who are starting to dabble with SDN in their own data centers and campus networks. When the time comes for enterprises to deploy security solutions for their SDN-enabled environments, they'll find a fairly mature product set from the market in general, and their current vendors for different security appliances will likely be offering virtual appliance solutions already.

NFV AND SECURITY: DELIVERING SERVICES TO CUSTOMERS AND VIRTUALIZING INFRASTRUCTURE

The case for NFV and security is simple to make. Virtualizing infrastructure of all types and allowing providers to deploy network functions and services on common hardware just makes sense. As you can see in the diagram below, the problems carriers are looking to solve with NFV are broad, and virtualizing network functions is really only one part. They'll use technology developed for SDN to provide the orchestration and automation portion of the vision.

Security is among hundreds of pieces of network infrastructure that ultimately will be virtualized as providers get more serious about NFV. The diagram below includes firewall, but in truth carriers will look to virtualize every bit of security technology they've deployed, from a single security appliance at the customer edge to the Gi/SGi firewalls they use to protect mobile backhaul networks, and everything in between.

Exhibit 5 **The Move to NFV**



The long-term vision for providers deploying NFV network-wide is similar to the use-cases for the SDN-enabled data center; agile deployment of revenue generating services, and the ability to match virtualized security to virtualized network infrastructure, making sure the appropriate security functions follow the network wherever it goes.

From a practical standpoint, this means, for example, enabling providers to place a common hardware device (any device capable of running a virtual machine) on the customer premises, then automatically deploy a wide range of services to that hardware device (or even allow the customer to deploy and manage as needed), so CPE services like routing, firewall, voice/UC, and WAN optimization can be delivered without having to send out discreet appliances for each function.

It also means allowing providers to use common hardware to build tailored security solutions for very specific environments. Mobile providers can combine security and mobile network functions into one tool in the backhaul network and leverage common hardware platforms to build massively scalable threat analytics and mitigation solutions for their transport networks, changing vendors and functions as needed without having to roll out new hardware each time.

CONCLUSION

The move to SDN and NFV is underway now; for most service providers the benefits are impossible to ignore.

- **Service agility for shorter time to revenue:** Service providers can quickly add, drop, and change the services they offer by using SDN control software and VNFs on commercial servers, rather than having to invest in new, specialized network hardware and manually reconfigure the network to deploy each new service. With SDN and NFV, service providers can cost-effectively test new services on small groups of customers, modify the service and give it another try, or simply scrap it without too great an investment if it's not working out. SDN can be deployed alongside existing network infrastructure, migrating customers gradually.
- **Global view of the network for provisioning across multi-vendor, multi-layer, and multiple network domains**: Rather than relying on each vendor's management system to view the status of traffic and equipment in their networks, carriers want to use SDN to make all the equipment from various vendors in their network visible, configurable, and manageable, from a single console so that services can be easily created and deployed across the entire network. The fine-grained control offered by SDN will enable carriers to run their networks at higher utilization while minimizing the equipment they need. This translates into considerable capex and opex reductions.

Many security technology vendors, including market-leading vendors like Check Point, Cisco, and Juniper, are far down the path in developing virtual appliance solutions for enterprises and service providers who began demanding security as soon as they started to deploy server virtualization. As a result, many of these security vendors are uniquely positioned to be first-movers in the SDN/NFV application business.

Security technology companies are not done innovating, and security tools for virtualized environments will evolve. Since the goal of SDN and NFV is to flatten visibility and control, it's not hard to imagine a world where the operating systems that run individual service platforms go away, and each discreet function of an existing security appliance becomes a service operated by the controller/orchestration infrastructure, allowing for better visibility and ultimate granularity in deployment. Using SDN and NFV to deliver security offers an unprecedented blend of centralized control and distributed enforcement.

WHITE PAPER AUTHOR

Jeff Wilson

Research Director, Cybersecurity Technology

IHS

+1 408.583.3337 | jeff.wilson@ihs.com

Twitter: @securityjeff

Commissioned by Juniper to educate the industry about the role of security in SDN and NFV, this paper was written autonomously by analyst Jeff Wilson based on IHS/Infonetics' independent research.

ABOUT IHS INFONETICS

Infonetics Research, now part of IHS (NYSE: IHS), is an international market research and consulting analyst firm serving the communications industry since 1990. A leader in defining and tracking emerging and established technologies in all world regions, Infonetics helps clients plan, strategize, and compete more effectively.

REPORT REPRINTS AND CUSTOM RESEARCH

To learn about distributing excerpts from IHS Infonetics reports or custom research, please contact:

The Americas:
+1 855 323-3363
+1 719 265-1535
Technology_US@ihs.com

Europe, Middle East, Africa (EMEA):
+44 1344 328300
Technology_EMEA@ihs.com

Asia Pacific:
+604 291-3600
Technology_APAC@ihs.com