SDN & Security: The Future Is Now

By George V. Hulme

MAY 2017 | US$25 | S180517

Channel Partners™

SDN & Security: The Future Is Now

By George V. Hulme

MAY 2017 | US$25 | S180517

Channel Partners™

Table of Contents

Channel Partners™

About the Author

GEORGE V. HULME is an internationally recognized security and business technology writer. For more than 20 years, he has written about business, technology and IT security topics. From March 2000 through March 2005, as senior editor at InformationWeek magazine, Hulme covered the IT security and homeland security beats. His work has appeared in CSO Online, Computerworld, Network Computing, Government Computer News, Network World, San Francisco Examiner, TechWeb, VARBusiness and dozens of other technology publications.

linkedin.com/in/georgehulme
@georgevhulme

SDN & Security: The Future Is Now

YOUR CUSTOMERS ARE LOOKING TO MAXIMIZE THEIR NETWORKING AND IT INVESTMENTS BY CUTTING COSTS AND increasing agility. Nowhere is this more visible than in the move to the cloud and, increasingly, virtualized environments using software-defined networking (SDN) and network function virtualization (NFV). A software-defined architecture not only cuts hardware costs but helps enterprises increase automation, embrace agile IT methodologies such as DevOps, and improve operations and security.

For your service provider partners, technologies such as NFV also deliver more competitive virtualized services to customers.

While highly virtualized environments certainly deliver many benefits, these deployments aren't without security risks. Before exploring them, however, it is important to cut through the hype around these technologies. As with cloud, suppliers are slapping the "software-defined" label on all sorts of offerings.

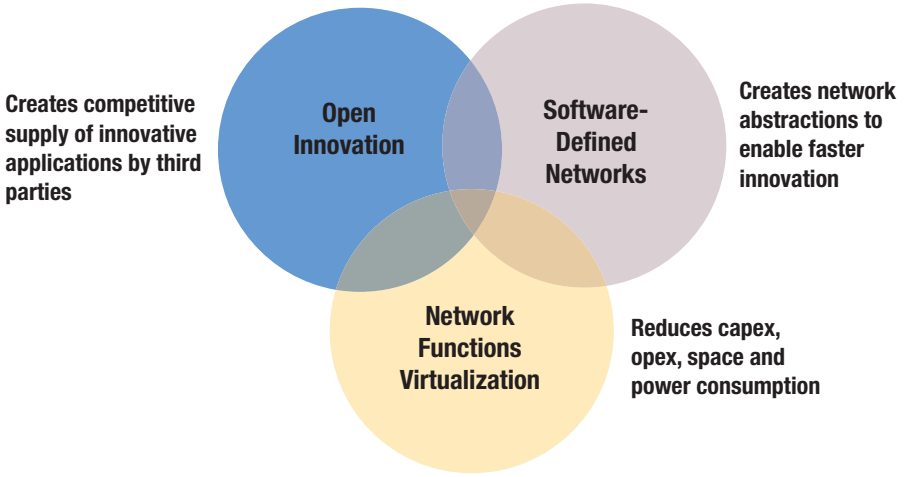
Here's the reality: With SDN, low-level network functionality is abstracted to simplify network configuration. This makes it easier to launch, change and manage networks on the fly without having to worry about underlying architecture.

While NFV uses virtualization to abstract the capabilities of network devices (functions) such as firewalls, intrusion-detection systems, accelerators, load balancers and more, removing the need to manage hardware appliances, NFV functions run within virtualized machines, just like any other virtualized workload. (Get our free primer on NFV and the channel for more background.)

We are discussing both SDN and NFV here — not because the technologies are identical, but because it is becoming increasingly popular for the concepts of NFV to be introduced to SDN architectures by enterprises and service providers alike.

When SDN Drives NFV

While it's perfectly possible to have NFV without the inclusion of a full-blown SDN, the two are often deployed together, and an SDN driving NFV is a very powerful combination.



Source: Nakul Nagralawala, Netmanias Tech-Blog

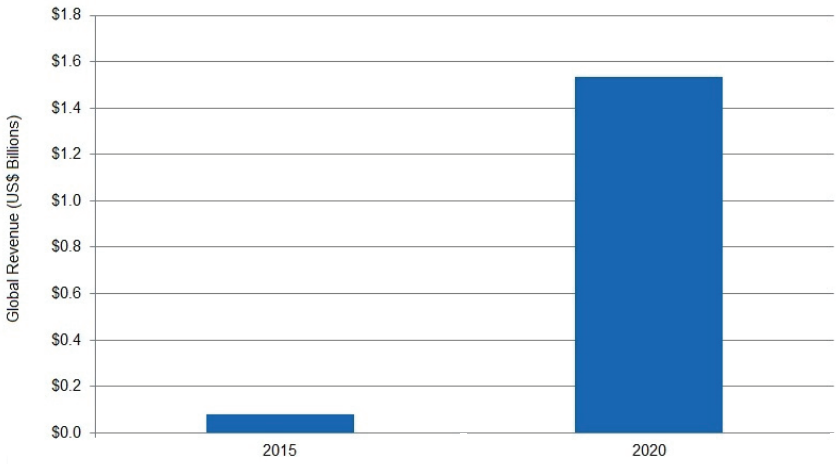
The move to SDN and NFV has an impact on everything to do with how networks and network services are deployed, managed, consumed and secured. That includes changing customers' security postures by introducing potential hypervisor vulnerabilities — in many instances, SDN/NFV controllers are more susceptible to denial-of-service attacks than traditional systems, and controllers provide a centralized point of compromise for associated services on the network.

And, of course, SDN/NFV architectures are vulnerable to traditional security threats such as software exploits, malware, identity-based attacks and similar.

There's quite an opportunity here for channel partners and service providers, according to research firm IHS Markit. Sales of applications specific to these environments, such as security and network management, are predicted to grow by nearly 54 percent annually through 2020, reaching $12.5 billion. While the growth of NFV will not be quite as rapid, it is still rising at a torrential pace: IHS expects the NFV hardware, software and services market to reach $15.5 billion by 2020, growing at a 42 percent clip.

vCPE Use Case Opportunity

In its 2016 "NFV Hardware, Software, and Services Annual Report," IHS Markit tracks what service providers spend on NFV hardware and software to deliver software-based services to customers via the consumer virtual customer premises equipment (vCPE) and enterprise vCPE use cases. The vCPE use case opportunity, including spending to deploy consumer and enterprise services, is forecast to reach over $1.5 billion worldwide by 2020.



Source: IHS

Most large service providers, including AT&T, CenturyLink and Verizon, have already virtualized their networks and customer-facing services and are now integrating NFV with their SDN installations to help customers attain the same benefits — improved IT resiliency, faster response to market demand for new services and lower costs through improved operations.

However, these benefits do not come without risks.

The Security Challenges of SDN and NFV

In recent years intra-data-center traffic, so called "east-west," has proliferated. This creates a situation where internal traffic is not protected or vetted by security defenses and traffic analyzers on the perimeter. This is part of the reason many security vendors now offer their applications as virtualized appliances.

This has been a successful strategy — many enterprises want virtualized security for their virtualized environments. But providers should realize that it is not just having discrete virtual network functions (VNFs) that provide the real value; rather, it's the synergy of being able to piece together many VNF functions, from security to systems management, to rapidly provide cost-effective and customized servers to individual customers.

Of course, when systems are virtualized, there are security pros as well as cons.

"Theoretically, SDN makes network management more efficient through centralization and automation, but, as we know, the ability to quickly create a complex infrastructure means it can quickly fall apart as well," says Alan Sharp-Paul, CEO and co-founder of resilient platform provider UpGuard. "Whether network configurations are on a hardware router or a piece of software running on a server, they're subject to the same kinds of misconfigurations, mismanagement and vulnerabilities."

Still, most networking experts agree that the upsides of centralized management and an increased ability to automate network and security tasks override potential issues — you just need to be cognizant of risks.

"From syncing high-availability clusters to maintaining consistency across continuous integration and delivery (CI/CD) pipelines and environments, keeping infrastructure alignment is crucial to stability and security," says Sharp-Paul. "While SDN/NFV introduce new challenges such as elastic network boundaries, more traditional ones, such as unchanged default passwords, still exist."

"It often doesn't take much — sometimes just one errant command or typo — to wreak havoc across a wide environment," he adds.

It's important to note that the risks associated with traditional architectures do not go away, and can even be exacerbated by SDN.

"Regardless if the network is virtualized, without the proper segmentation, Coke can see Pepsi's network traffic," says Tom Kee, principal engineer at identity-defined networking (IDN) provider Tempered Networks. "Most solutions currently on the market use some form of VPN technologies to create an overlay network, essentially creating a virtual private LAN to keep traffic content from prying eyes. But not all VPN solutions, in terms of authentication and encryption are the same, and it can be difficult to add new nodes and time-consuming to configure [them] correctly."

That's a service opportunity for partners, because these skills are expensive and scarce; few midsize or small companies will have them in-house.

SDN vs. NFV

SDN can be considered a series of network objects (such as switches, routers, firewalls) that deploy in a highly automated manner. NFV is the process of moving services (such as load balancing, firewalls and IPS) away from dedicated hardware into a virtualized environment.

Software-Defined Networking (SDN)		Network Function Virtualization (NFV)
Separate control and data, centralize control and programmability of network	Basic Concept	Relocated network functions from dedicated appliances to generic servers
Campus, data center / cloud	Target Location	Service provider network
Commodity servers and switches	Target Devices	Commodity servers and switches
Cloud orchestration and networking	Initial Applications	Routers, firewalls, gateways, CDN, WAN accelerators, SLA assurance
OpenFlow	New Protocols	None
Open Networking Foundation (ONF)	Formalization	ETSI NFV Working Group

Source: Nakul Nagralawala, Netmanias Tech-Blog

As SDN and NFV continue to improve operations and business support systems, vendors that embrace VNFs will be able to provide better data-driven services and support to customers through improved centralized control and monitoring.

Which leaves the question: How should partners help customers manage existing and new risks in SDN and NFV deployments?

How SDN Helps Security

"The good news is that the agility of a software-defined system makes deployment of security fixes much faster than ever before," says Rudy Musschebroeck, director for CCS solutions for telecom CommScope. "Security problems are not new, and techniques used to secure other technologies can be adapted to mitigate threats to SDN/NFVs. Even though the radical transformational nature of SDN/NFV on networking will create some security challenges in the early days due to the unknown possibilities, the industry has historically demonstrated these can be overcome."

You may hear the term "NFV forwarding graph" used to describe network functions, such as packet inspection, IPS, traffic optimization, protocol proxies (carrier-grade network address translation, or NAT) and other services. When you do, think encryption.

"Telcos are pushing more of the network functions to the edge of the network," says Kee. "While it is never really mentioned in the working groups, a service path should be encrypted and the identity of the network function should be cryptographically trusted. In other words, encrypted paths and trusted functions should always be a default for NFV forwarding graphs, rather than an optional network function."

Another important aspect of identity and trust is ensuring that termination points for the overlay network are trusted.

"Imagine if the software switch that provides an encrypted overlay service is stolen, offering the network equipment thief the opportunity to join the — presumably — secure corporate network?" says Kee. To mitigate such risks, the network operator needs to establish network access policies, he explains, such as a mutual authentication scheme between the switch and controller as a form of trusted cryptographic identity at installation and during startups.

"This is the first safeguard, but cannot be the only mechanism" Kee says. "For example, if the switch goes offline for no good reason and comes back online with a different underlay address, a policy should be enacted to remove trust and quarantine that segment of the network."

It is also important that network operators consider the nature of the endpoints connected to the network, as when, for instance, WAN endpoints are wireless.

"Not all branch offices or an array of gas pumps can be connected with an Ethernet cable," says Kee. "It's more likely that these types of devices are going to use 4G, Wi-Fi or a satcom link, and with these shared mediums, extra precautions are required to prevent compromising the system."

While SDN and NFV change the nature of security challenges, they also help to improve security in many ways and better deliver security functionality in modern software-defined architectures.

Delivering Security Services

So, what types of services should channel providers deliver, and from which suppliers?

It comes down to the basics: Choose partners that will provide optimal uptime and the tools needed for comprehensive management and security policy enforcement.

"Major network configurations outages have been a huge problem for enterprises due to the speed at which their systems operate," says UpGuard's Sharp-Paul. "Enterprises should be in search of software that allows them to validate network configurations and promote visibility into what they have. By automating and continuously running these tests, you can validate that the infrastructure you're operating is secure and compatible with your greater business goals. Because in the end, that's what IT risks really are — business risks."

This is especially so as customers' applications, networks and services run on hardware and cloud infrastructure provided by carriers and cloud providers. As customer traffic will traverse third-party equipment, it is even more important to attach the services to an encrypted overlay before it hits the provider's wire, says Tempered Networks' Kee, adding that controls should be seamlessly manageable across multiple providers via redundant network controllers.

Additionally, telecommunication providers need to be transparent about how they secure their virtualized network services, says Jan Johansson, director of product management at network visibility and traffic monitoring technology vendor Gigamon. That policy needs to be explicit and embrace virtualization, he says, and partners must understand who is in charge of executing it, so that there are clear points of accountability in the chain of command when issues arise.

The last thing you want when problems arise is finger-pointing, and that doesn't change in a software-defined infrastructure. Ensure there will be no questions about how issues will be resolved, Johansson says.

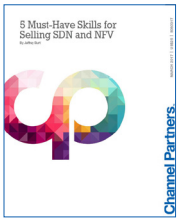
Mike O'Malley, vice president of carrier strategy and business development at Radware, adds that providers need to offer complete defenses against multivector attacks that extend Layer 4 through Layer 7 — including distributed denial-of-service attacks. Insist on web application firewalls and SSL protection against encrypted attacks. "These solutions need to be backed 24/7 by experts who are knowledgeable on the latest attack trends and are able to virtualize all these solutions into a cloud environment and provide automated policy through SDN to manage the network with the lowest operational costs," says O'Malley.

SDN/NFV Global Forecast

In its "Software Defined Networking (SDN) Market & Network Function Virtualization" report, MarketsandMarkets forecasts the SDN and NFV market to grow from $2.02 billion in 2015 to $45.12 billion in 2020. This represents a CAGR of 86.1 percent. In terms of regions, North America is expected to lead the market; Asia-Pacific including Japan is the fastest-growing market and is expected to soon replace Europe as the second-biggest contributor in the market.

With that advice, O'Malley gets to the heart of the promise of SDN and NFV: Service providers and channel partners can simplify maintenance and operation costs, thus improving their own development pipelines with VNFs and microservices, which will further improve the stack of security services they provide their customers. With potential payoffs like that, it is no wonder SDN and NFV are expected to grow more than 40 percent annually.

Related Reports



5 Must-Have Skills for Selling SDN and NFV

Carriers, open-source consortiums and big IT vendors have laid the groundwork for SDN and NFV. Demand is there, so what's stopping widespread use? Complexity, a skills shortage and confusion. Channel partners who can clear all that up can write their own tickets.

Channel Guide to NFV: Faster, Better, Higher-Margin Services

Services delivered in a software-defined model — from firewalls to UC to SD-WAN — represent significant opportunity for channel partners. In this Report, we provide a primer in network functions virtualization (NFV) and related technologies, tips on how to sell customers on the concept and recommendations for moving your business into the virtual era.