IHS TECHNOLOGY NOVEMBER 2015

Data Center Security: Micro-Segmentation and Application Visibility

Jeff Wilson, Research Director, Cybersecurity Technology

Table of Contents

List of Exhibits

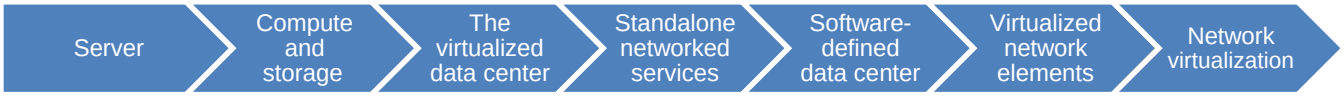
THE SOFTWARE-DEFINED DATA CENTER

Micro-segmentation, the core subject of this paper, is a new security architecture enabled by the creation of the software-defined data center (SDDC), so before we dive into micro-segmentation and the role of layer 7 visibility, it's important to step back and understand how we got here.

The SDDC begins with virtualization, a mature and well understood technology. PC virtualization goes back to the late 80s, though its roots are in IBM mainframes. Server virtualization as we know it today stems from the launch of VMWare ESX and GSX server in 2001. In the nearly 15 years since the launch of ESX/GSX, companies of all types have leveraged the flexibility and efficiency of server virtualization, and many other components of data centers have become virtualized, including compute, storage, and a wide range of network applications and services.

The emergence of SDN and the concept of an orchestration layer take us us from a data center with disparate virtualized resources to a software-defined data center where complex services can be built, changed, and torn down in seconds or minutes. As we see in the timeline below, the SDDC is still just a stop on the way to full network virtualization; it is, however, an important stop.

Exhibit 1 **Virtualization Timeline**



The Open Networking Foundation (ONF) is the group dedicated to defining and promoting SDN technology, and it defines 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."

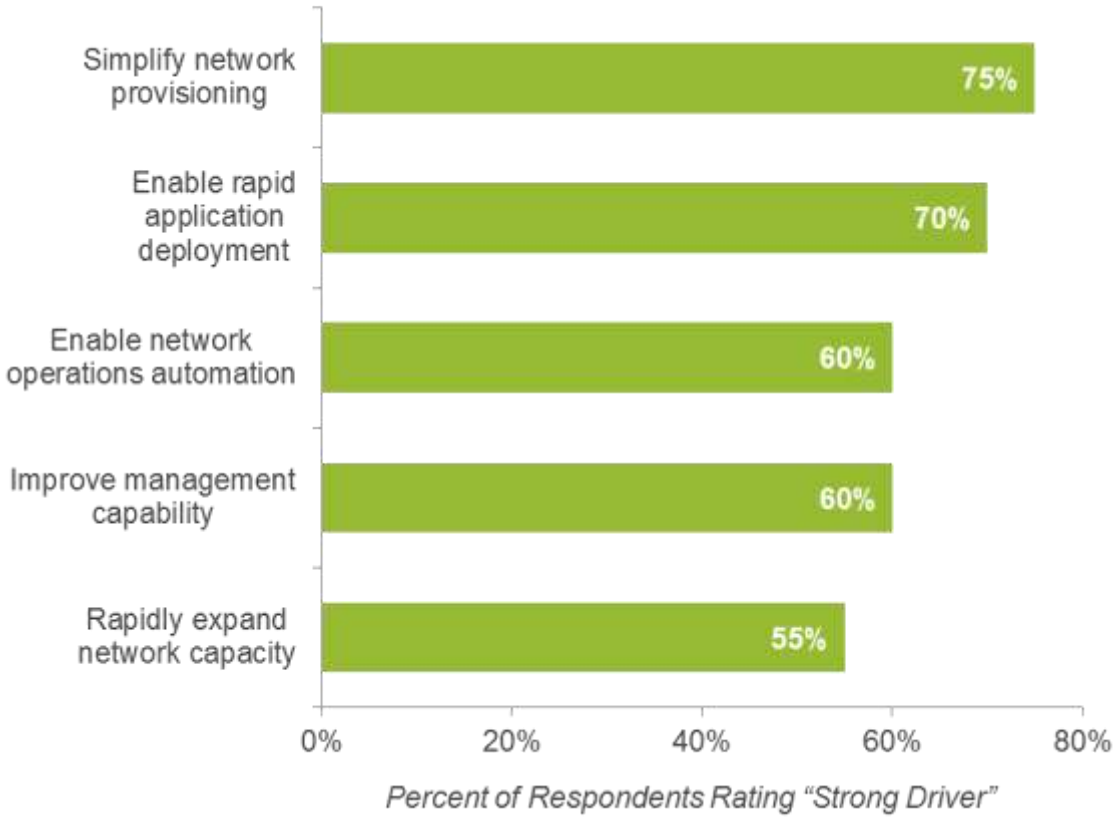
The control portion of the equation, now separate from forwarding, can perform many functions, generally referred to as "orchestration". A wide range of orchestration solutions have emerged, from open source projects like OpenStack to commercial SDN controllers from a vendors like Cisco and Juniper.

DRIVERS FOR SDN AND THE SOFTWARE-DEFINED DATA CENTER

Once a data center operator has virtualized compute, storage, servers, and network services and tied them all together with an orchestration platform, it has all the ingredients of a software-defined data center. The first question to ask, then, is why go through the significant effort of this transformation? We know operators are building software-defined data centers today, and SDN initiatives are at the core of the rebuild. We spoke to 20 of the biggest and most influential data center operators around the globe in our *SDN and NFV Strategies: Global Service Provider Survey* and asked them about drivers for rolling out SDN.

Simplifying network provisioning tops the list; it speeds time to market for new services and reduces operational costs. We believe that the results underscore the frustration service providers have with network provisioning, and they're looking at SDN to help them provide an overall management and operational framework that runs across multivendor equipment. Rapid application deployment and enabling network operations automation help decrease operating costs and speed up time-to-revenue, and not just by a little bit. Data center operators who have walked down the SDDC path already report the real ability to architect a new service and roll it out in days, and data center operators who can't offer that level of agility are losing customers.

Exhibit 2 **Key Drivers for SDN in the Data Center**



IHS Infonetics *Data Center SDN Strategies: Global Service Provider Survey,* October 2015

Due to the significant promise of decreased operations cost and increased revenue due to the scale and agility of the software-defined data center, operators are re-evaluating the architecture of every part of their data centers, and security architecture usually tops the to-do list.

SECURITY IN THE DATA CENTER, AND THE EMERGENCE OF MICRO-SEGMENTATION

The software-defined data center is inevitable, but what is the impact on security architecture? Since the early 2000s, data center operators have continually invested to harden the perimeter of the data center, increase the capacity of security solutions to match data center traffic, and deepen protection against the increasing number of security threats aimed at the data center. Now that operators are abstracting forwarding from control and virtualizing infrastructure and layering in orchestration and automation, there's an opportunity for data center security to reinvent itself along two axes:

- Data center operators can build out security services that are as **agile** as the rest of their infrastructure
- **Micro-segmentation** is now not only possible but likely more effective than old data center security architectures

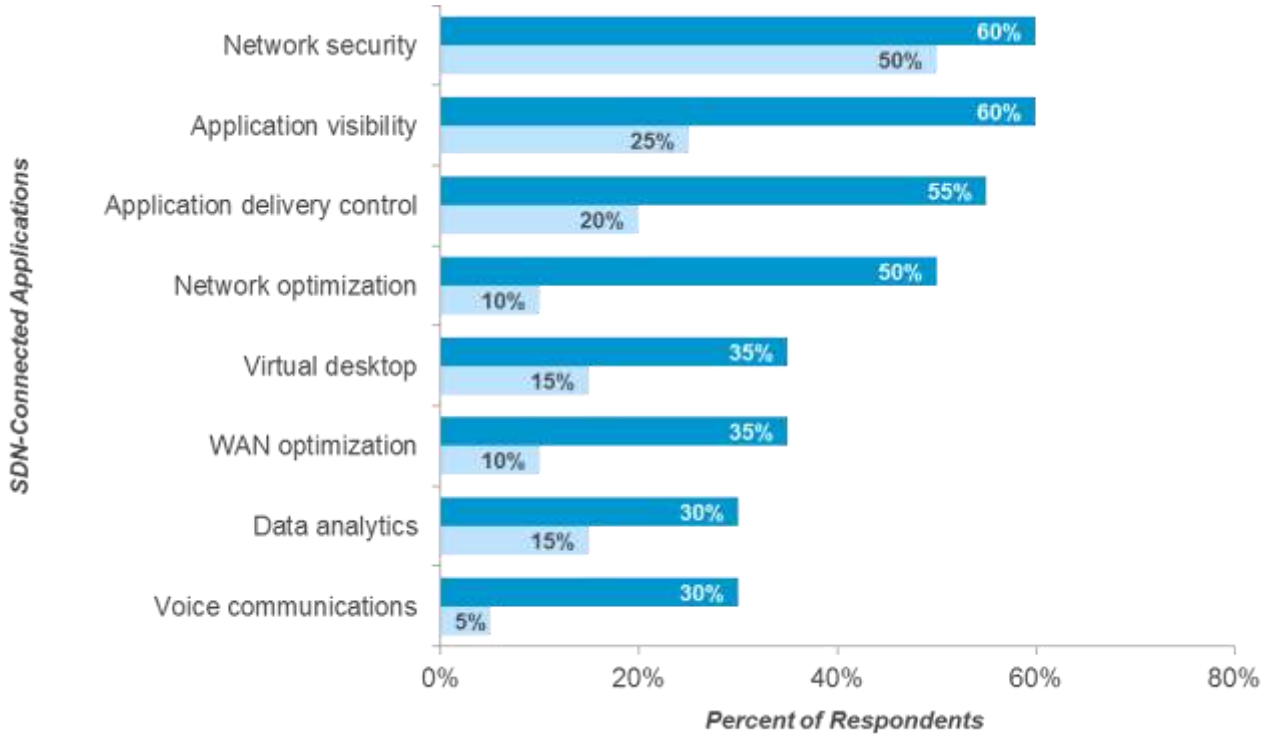
Security vendors have been working on adapting threat detection and mitigation solutions to work in virtualized (under a hypervisor) environments for years, typically building what they refer to as virtual appliance versions of their traditional hardware/software products. There is a wide range of appliances designed to work with multiple hypervisors and SDN controller interfaces available today. As soon as server virtualization was introduced, anyone who deployed it discovered the challenge of meeting the security scale requirements of a virtualized infrastructure and needed a way to secure traffic moving between virtual machines—this traffic was essentially invisible to existing threat mitigation tools.

The evolution of protection in the data center looks like this:

Exhibit 3 **Evolution of Data Center Security**

In the survey referenced earlier, when we asked service providers which SDN-enabled applications they were rolling out, network security (firewall) topped the list, followed by application visibility, which is a particularly difficult problem in the software-defined data center.

Exhibit 4 **Security is the Killer App in the SDDC**

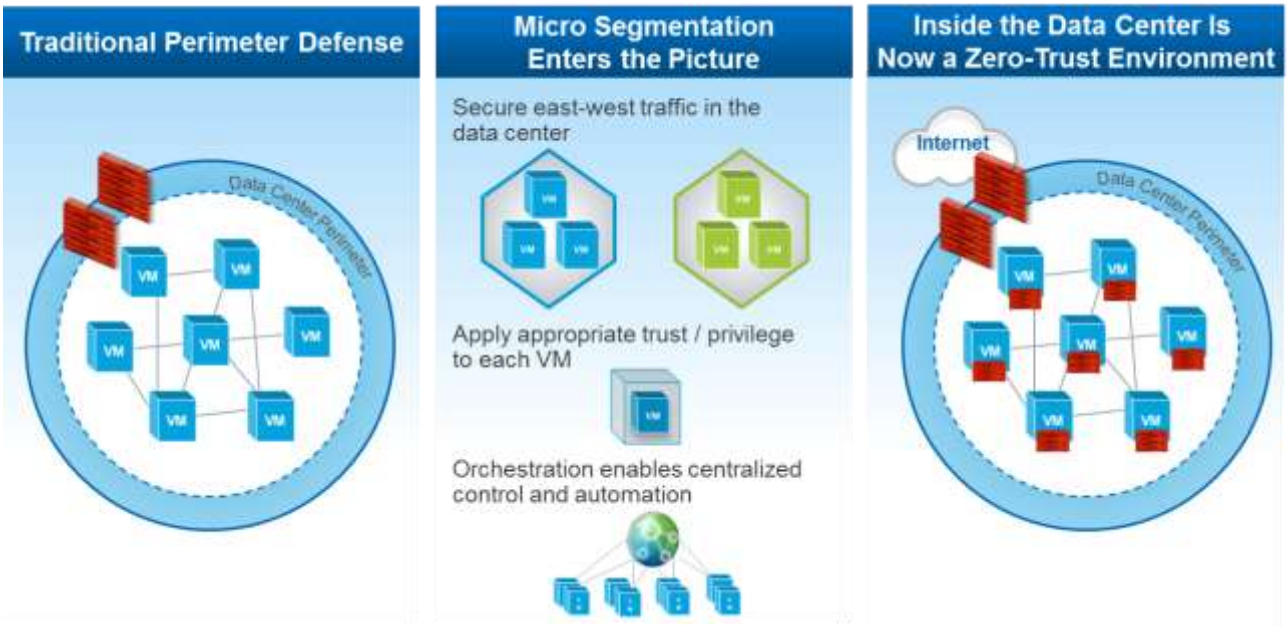


IHS Infonetics *Data Center SDN Strategies: Global Service Provider Survey,* October 2015

Traditional data center security (prior to infrastructure virtualization) involved building a very high performance hard shell around the perimeter of the data center (firewalls, DDoS mitigation), and then embedding some advanced threat (IPS) and analysis (SIEM) tools in the data center. Although data centers have been multi-tenant for a long time, the infrastructure wasn't shared the way it is in a SDDC, so internal segmentation was typically handled by VLANs. Occasionally hardware firewalls would be deployed inside the perimeter to provide a more secure segmentation, or when dedicated hosting or colocation customers ordered additional layers of security for their own services, but there was essentially trust, because the traffic itself was almost entirely moving north-south (in and out of the data center), and passing through security layers as it traveled.

As virtualization was rolled out in data center infrastructure, traffic patterns changed significantly; current estimates show that 3/4 of traffic in a data center is moving east-west, and it's running on shared infrastructure that previously lacked dedicated security controls. Virtual infrastructure, by design, provides isolation, but traffic still needs to be inspected for threats when it's moving east-west, because without inspections attackers can find one north-south vulnerability and use it as a launching point to move east-west through the entire data center.

Exhibit 5 **Micro-Segmentation Overview**



Micro-segmentation refers to the ability to run an instance of network security for every VM, firewalling every VM from every other and essentially creating a zero-trust network inside the data center. Perimeter security controls can and will still be used, but because of the orchestration and automation capabilities of hypervisors and SDN orchestration platforms, the change management portion of dealing with hundreds or thousands of individual firewalls attached to individual VMs can be done very easily. Micro-segmentation provides:

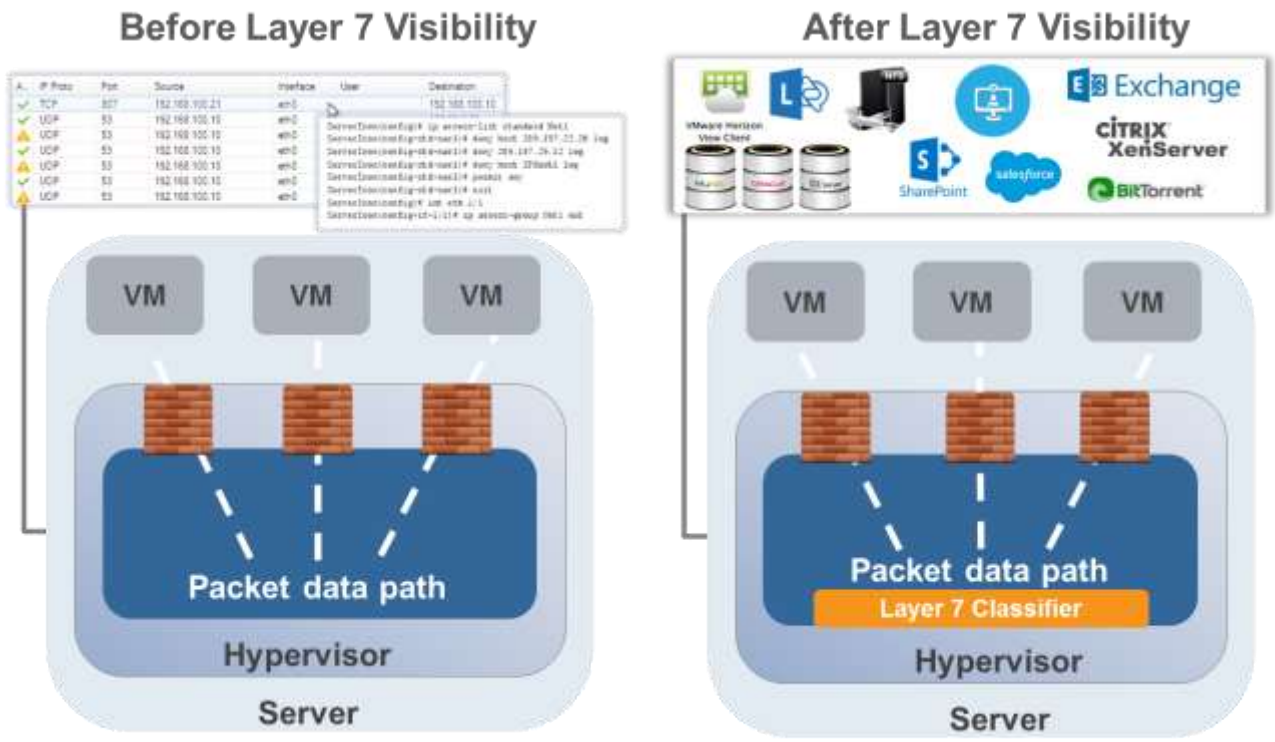
- Collapsed networking and application security layers
- Security controls that match the application and data requirements of each VM
- Security that follows VMs wherever they go without additional administration, and even spin up and down automatically the VMs spin up/down
- Inspection and containment for east-west traffic and threats

Theoretically, micro-segmentation is a major leap forward in protection and threat containment, but the first-generation solutions have limitations—the ability to identify and protect against attacks is highly dependent on the *volume* and *type* of traffic and application data. Adding security controls at layer 3 and 4 allows administrators to see and control traffic based on IP address, ports, and network-layer protocols; layer 7 visibility allows a view of individual application flows and even an understanding components of applications—allowing things like control of Facebook messaging separate from the rest of Facebook traffic. Doing deep inspection of content on a virtualized machine is complicated and potentially resource-intensive—so what can reasonably be done?

ADDING LAYER 7 VISIBILITY

Understanding the context of a given piece of traffic is critical to nearly every type of security solution on the market, and one of the most important bits of context for network traffic is visibility into which applications (and even specific modules within applications) are travelling across data centers. The advent of tools like next generation firewalls with application visibility and control have allowed administrators to build simple and elegant firewall policies focused on the business use of traffic and not on ports and IP addresses.

Exhibit 6 Adding Layer 7 Visibility: Before and After



A great attribute of many software-defined data centers is that are constructed using open and programmable tools with interfaces that allow information and policy to be shared. This creates an environment where new solutions can be assembled without having to change the underlying infrastructure. Although full next gen firewall solutions can be deployed in the SDDC to overlay basic firewalling function provided by platforms like VMware NSX, there are also layer 7 classification tools (based on deep packet Inspection and associated techniques) capable of running on hypervisors or in VMs to do the classification/organization of traffic.

Software-defined data centers are built on the open interfaces in security management tools, orchestration tools, hypervisors, and cloud networking platforms, so it's possible to construct a solution that provides the benefits of layer 7 classification without requiring purchase of new virtualized next gen firewalls (or other network security platforms). Most importantly, the SDDC architecture, when applied to security, allows buildout of data center security using an organization's preferred components for each function: firewall, monitoring, orchestration/management, layer 7 classification, advanced threat detection, and whatever other security functions are desired.

A layer 7 classifier can handle the task of organizing all of the traffic into useable application data, and then can provide its own policy creation interface or feed data to another policy interface or security management tool. Then the firewall on the virtual machine can interpret the policy and handle enforcement. However it's done, giving administrators the ability to easily apply application layer controls inside a data center is an incredibly powerful tool. All the benefits of layer 7 visibility in a traditional network architecture open up when adding layer 7 classification in a virtualized environment: administrators can see traffic based on applications or even components of applications, providing the ability to build a wide variety of security policies: from broad policies like "block all file sharing applications" to much more granular policies that can dig into individual components of applications and link up multiple enforcement points, analysis tools, and management/reporting consoles.

CONCLUSION

The overwhelming popularity of cloud services, driven by their scale and agility, has forced a re-architecting of data centers. A modern software-defined data center leverages virtualization, SDN, and orchestration/automation to allow data center operators nearly unlimited flexibility in the type of services that can be built and delivered to users faster than ever. With these changes have come necessary, and ultimately positive, changes in data center security architecture. Micro-segmentation augments a security perimeter and turns the SDDC into a zero-trust environment that is manageable; data center operators looking to enhance the capability of their existing micro-segmented data centers (or build new ones) can build more useful, more targeted, and ultimately more secure policies with the addition of layer 7 classification data.

WHITE PAPER AUTHOR

Jeff Wilson

Research Director, Cybersecurity Technology

IHS

+1 408.583.3337 | jeff.wilson@ihs.com

Twitter: @securityjeff

Commissioned by Qosmos to educate the industry about micro-segmentation in the data center and the role of layer 7 inspection, this paper was written autonomously by analyst Jeff Wilson based on IHS/Infonetics' independent research.

Join us for ***Securing the Data Center: The Role of Micro Segmentation***, a free educational webinar presented by IHS and Qosmos:

LIVE: Wednesday, November 18, 2015
8:00 AM PST, 11:00 AM EST, 16:00 UTC

REPLAY: Watch on-demand any time

Both the live event and replay can be accessed at:
http://event.on24.com/wcc/r/1065481/9B67B3BBCA1D6F19EA414001E1FFE4EF

QOSMOS

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:

IHS Sales: +1 844-301-7334
https://www.ihs.com/about/contact-us.html