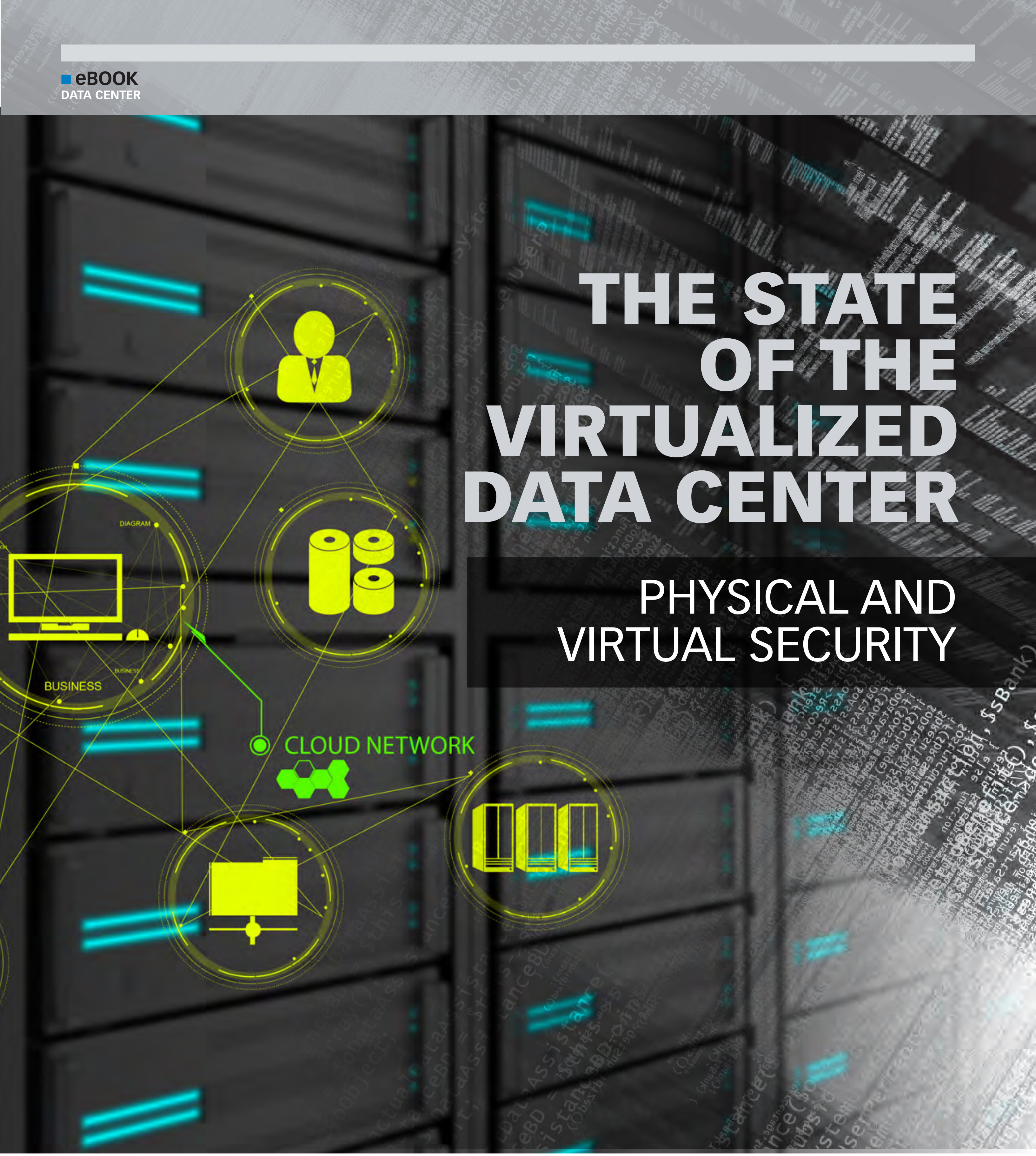
eBOOK
DATA CENTER



# THE STATE OF THE VIRTUALIZED DATA CENTER

## PHYSICAL AND VIRTUAL SECURITY

NETWORKWORLD
Custom Solutions Group

JUNIPER
NETWORKS

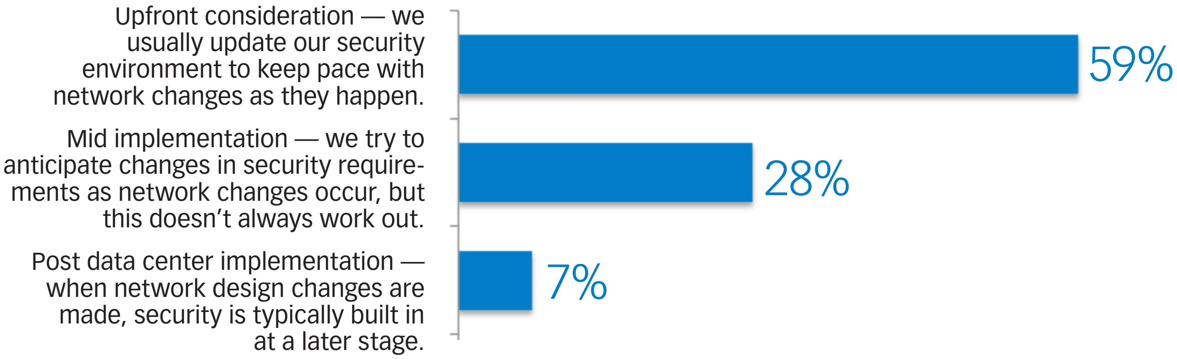
# PHYSICAL AND VIRTUAL SECURITY

Virtualization has changed the face of the data center. Today's data centers are a mix of physical servers and virtual workloads, and require a more pervasive range of security as a result. With nearly every organization implementing some degree of cloud computing, virtualization security is as integral a component as traditional firewalls are in today's networks.

This is evidenced by the results of the *Network World* survey. At 59 percent, the majority of respondents report that network security is an upfront consideration when implementing new network technology. Network security is important because it's the backbone of the larger security ecosystem. In the past, security measures were largely reactive. But IT organizations are becoming more proactive. They want to have a strategy in place as they implement initiatives around virtualization, cloud services, consolidation and modernization. And the strategy must be balanced with convenience and speed. Applications and Infrastructure-as-a-Service can be provisioned in minutes. Organizations need the ability to scale and flex the network and security to assure it serves the interest of the application. It is unacceptable for security to take a couple of months to catch up with the virtualized resources. Security should be constantly scaled and flexed in tandem with the physical network or SDN network or both.

**A MAJORITY OF RESPONDENTS REPORT THAT NETWORK SECURITY IS AN UPFRONT CONSIDERATION WHEN IMPLEMENTING NEW NETWORK TECHNOLOGY.**

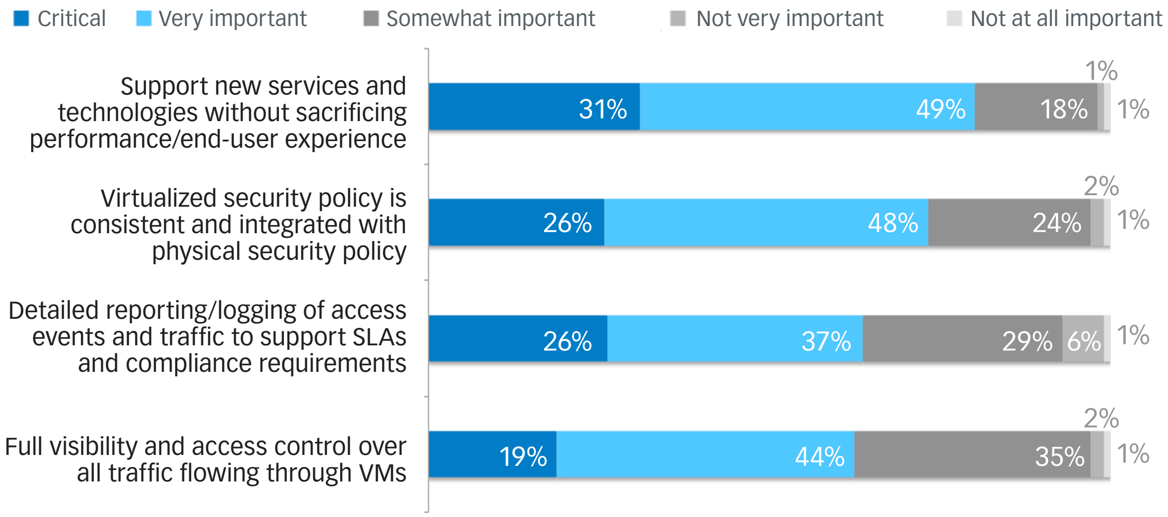
Consideration of Network Security When Implementing New Network Technology



Performance is also a concern when evaluating network security solutions to support a virtualized environment. In fact, 80 percent of respondents to the *Network World* survey consider it highly important to be able to support new services and technologies without sacrificing performance. This tends to be a problem when perimeter security solutions are retrofitted for the virtual environment rather than purpose-built for VMs. It can be compared to putting a heavy coat of armor on a little machine that wants to move around. The armor weighs—and slows—the VM down. Furthermore, because VMs are in a multitenant environment, it is important to secure them north to south with other physical perimeter security measures, but also east to west to protect them from other VMs that might be sitting on the same server. Security must double-down—making sure no one is coming in from the outside or the VM sitting next door—but without slowing performance.

## WHEN EVALUATING NETWORK SECURITY SOLUTIONS TO SUPPORT A VIRTUALIZED ENVIRONMENT, 80% CONSIDER IT HIGHLY IMPORTANT TO BE ABLE TO SUPPORT NEW SERVICES AND TECHNOLOGIES WITHOUT SACRIFICING PERFORMANCE.

Level of Importance When Evaluating Network Security Solutions to Support a Virtualized Environment



**56%** of respondents say securing web traffic is their biggest security concern.

However, **61%** of respondents say emerging network security technologies only address part of the cyber security threats facing their organization.

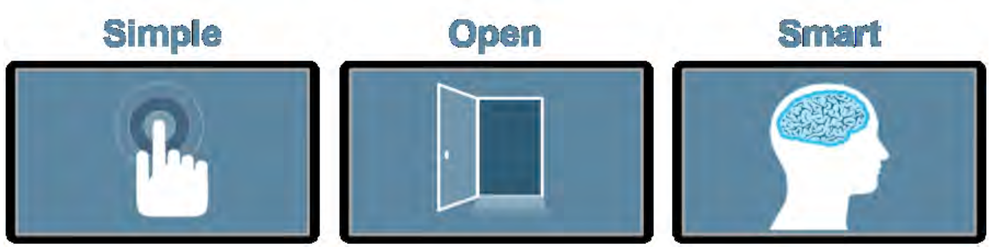
SOURCE: Ponemon Institute© Research Report

Workloads must also be secured in a consistent manner, and the policies that apply to physical workloads must apply to virtual workloads regardless of where they reside. Organizations must be able to manage them with a consistent policy in mind so that zones defined for the physical network can also be articulated in the VM. If the policy says this workload is associated with financial information and the data moves to another cloud provider, the policy should travel with that workload and adhere to the zone policy established for the physical network. Managing policies once for both the physical and virtual environments reduces operational overhead. It also ensures there will be no mistakes that can leave the organization vulnerable to attack or falling out of compliance with regulatory requirements.

Organizations should also consider the firewall technology they deploy in the data center. Some providers insist that their next-generation firewall solution can help protect the virtualized data center. However, this technology has a specific use case in an office or campus environment. The application visibility and control capabilities are aimed at keeping people from inadvertently contracting a virus. These capabilities are not needed in the data center, nor are they effective at protecting the infrastructure. The majority of security professionals who responded to a 2013 Ponemon Institute report commissioned by Juniper Networks indicated that current next-generation firewalls and IP reputation feeds address only part of the cybersecurity threat, leaving significant exposure to the most concerning attacks. Applications and infrastructure reside in the data center, which is why it requires a high-performance, highly scalable firewall-based gateway.

# CONCLUSION

In an effort to achieve the level of agility that business demands, many IT organizations have virtualized their data center resources. With applications, servers and storage virtualized, IT is able to react more quickly to business needs. However, these virtualization efforts go only so far before network complexity brings efficiencies to a halt. To achieve greater levels of agility, IT must address the network.



That means simplifying the infrastructure and operations with virtualization. Juniper Networks MetaFabric™ Architecture—a simple, open and smart approach to data center design—accelerates the deployment and delivery of applications within and across multiple virtualized data centers. It provides location-independent coordination and management of devices across multiple sites, maximizing data center resources and ROI to allow you to establish a solid physical network foundation and address the security and BC/DR requirements needed for network virtualization success.

MetaFabric™
ARCHITECTURE

FOR MORE INFORMATION, VISIT
www.juniper.net/datacenter

NETWORKWORLD
Custom Solutions Group

JUNIPer®
NETWORKS