A Custom Technology Adoption Profile Commissioned by Cisco Systems

Virtual Security In The Data Center

January 2012

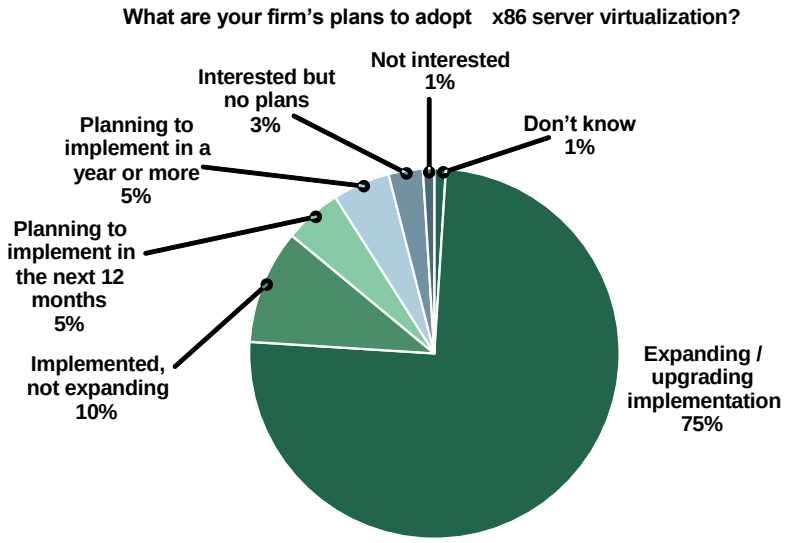
Introduction

The benefits of server virtualization are widely accepted and the majority of organizations have deployed virtualization technologies. Organizations are virtualizing mission-critical workloads but must now consider virtualization's security and compliance implications. Virtualization and security professionals now understand that there are significant security challenges that must be addressed in the new virtualized reality. Companies now acknowledge the potential real-world threats against virtualized environments. As security awareness increases among virtualization experts, enterprises will struggle to find the most effective and efficient ways to proactively protect virtualized environments. Our research indicates that while many organizations are leveraging existing data center security appliances to address new virtual security and compliance issues, there is an increasing adoption of virtualization-aware and virtualization-specific security solutions for mission-critical applications and scalable cloud-ready deployments.

Most Data Centers Use Virtualization, But Less Than Half Of Servers Are Virtualized

Most organizations have deployed virtual workloads and are comfortable with the technology from an operations perspective. According to Forrester Research's Forrsights Hardware Survey, Q3 2011, 85% of North American enterprises have already adopted x86 server virtualization or are planning to expand their implementation in the next 12 months. In fact, only 4% of respondents are not planning to implement x86 server virtualization in the future (see Figure 1). Of course, this type of technology adoption shift will affect the way that security in the data center is accomplished.

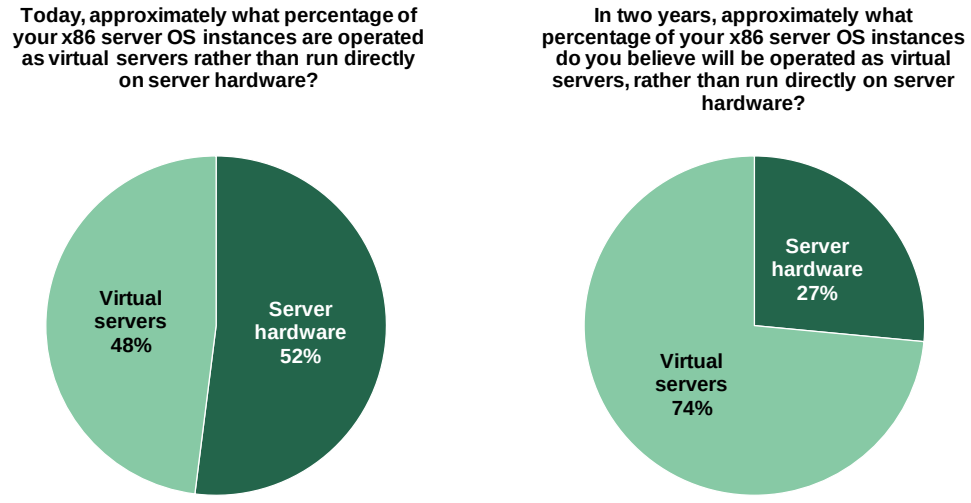
Figure 1
x86 Server Virtualization Adoption



Base: 300 IT decision-makers at North American organizations with 5,000 or more employees
Source: Forrsights Hardware Survey, Q3 2011

Despite the fact that the majority of survey respondents have deployed virtualization technologies, only 48% of the servers in the data center are virtualized today. IT leaders hope to grow their virtualization to 74% over the next two years (see Figure 2).

Figure 2
Percentage Of x86 Server OS Instances



Base: 244 IT decision-makers at North American organizations with 5,000 or more employees
(percentages may not total 100 because of rounding)
Source: Forrsights Hardware Survey, Q3 2011

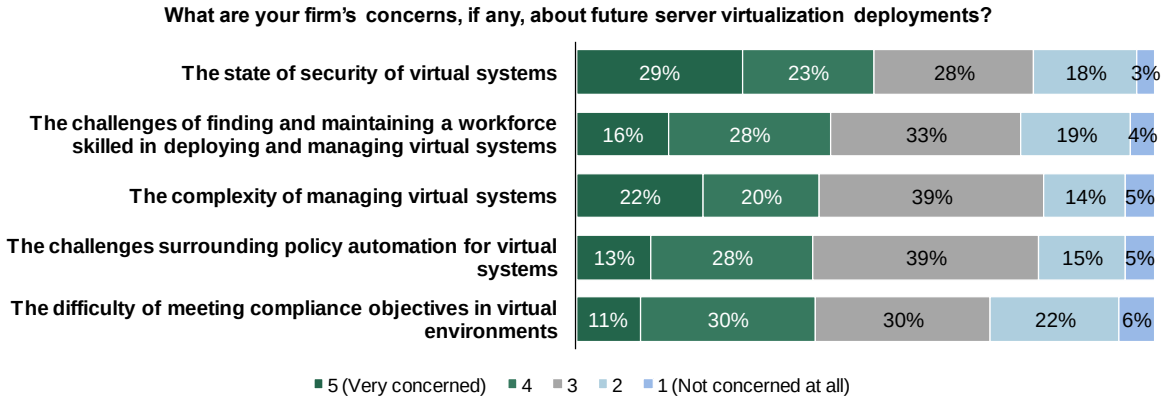
Clearly, these trends represent a significant change in the ways servers are deployed and managed. The technology intersection between virtualization and cloud offerings adds additional variables to the operational and security challenges that enterprises now face. To provide more insight into virtualization security trends, in November 2011 Cisco commissioned Forrester Consulting to take a closer look at the security implications of virtualization technologies among enterprises that already have a significant amount of virtualization and uncover how these organizations enforce security within their virtualized environments. The resulting survey of 79 North American enterprise security professionals demonstrates a demand for more specialized virtualization security controls.

For the purposes of this survey, a virtual machine is defined as any virtualized instance of a server that sits directly on a hypervisor. Sometimes called a guest or a workload, this survey uses the term "virtual machine" generically to describe a virtualized server instance.

Virtual System Security Trumps All Concerns

As organizations move toward 75% virtualization, they are looking beyond the initial use cases of virtualization. Organizations are now virtualizing mission-critical workloads in order to make their largest and most important applications more efficient reduce the costs associated with those applications. Virtualization is no longer reserved for commodity applications and servers; as a result, virtual system security is now a significant issue for IT decision-makers. In fact, 29% of the North American organizations surveyed by Forrester Consulting identified the overall state of security of virtual systems (as well as the compliance issues associated with those systems) as a major concern about future server virtualization deployments (see Figure 3). The complexities of the virtual systems themselves also rank high on this list, as do the potential ramifications of virtualization policies.

Figure 3
Virtualization Security Concerns Reign



Base: 79 IT decision-makers responsible for data center security at North American organizations
(percentages may not total 100 because of rounding)
Source: A commissioned survey conducted by Forrester Consulting on behalf of Cisco Systems, December 2011

Data center virtualization is multifaceted and requires a unique skill set to administer. The lines that delineated server, storage, network, and security roles are no longer clear and administrators need diverse

experience and expertise to properly manage virtual deployments. The market for staff with solid virtualization experience is competitive, and capable resources are in short supply: 44% of respondents indicated that maintaining a skilled workforce was a challenge.

Compliance objectives must also be factored into the virtualization story. More than 40% of survey respondents are concerned or very concerned with how virtualization will affect their compliance initiatives. For example, the PCI Security Standards Council has recently released compliance guidelines for virtualized systems. Because so many companies are affected by the PCI Data Security Standard, these guidelines could have a profound impact on the way in which companies choose to do virtualization security.

Consider this common scenario: a company takes credit cards. Because of this, they must abide with the PCI Data Security Standards. In an effort to reduce costs and streamline operational expenses they virtualized many of their servers. This virtualization was done quickly, with little thought given to the type of server being virtualized. As one European Senior Network Engineer noted, "We virtualized as soon as possible without thinking about the applications or if the software vendor agreed or certified the solution for the virtualization environment". This ad hoc virtualization process can be problematic. If a credit card database gets put on the same hypervisor as an externally facing web server, for example, then the web server, as well as every VM on the hypervisor, falls within scope of PCI compliance. [1]

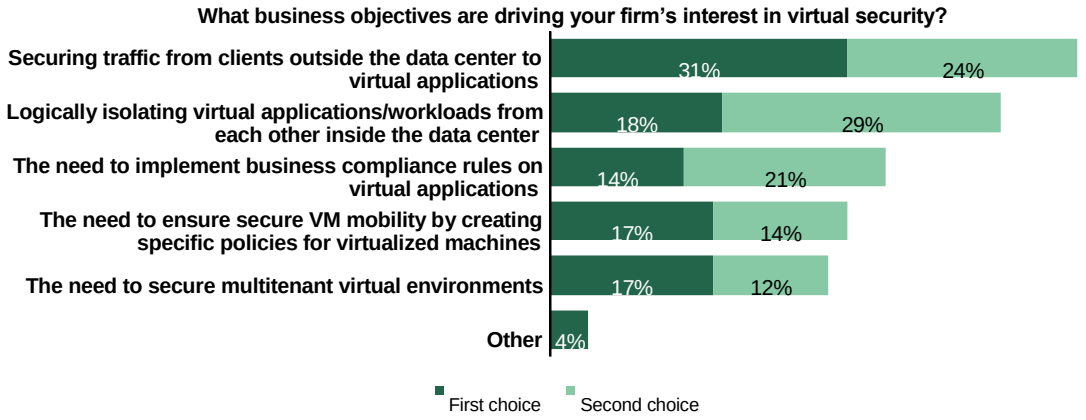
This means that all the hosts on the hypervisor must be secured within the confines of PCI. Section 3.5 of the PCI DSS Virtualization Guidelines states that "due to the increased risks and configuration challenges, the trust and risk level associated with each VM function should be taken into account when considering a virtualized design. Similarly, databases and other systems that store cardholder data require a higher security level than non-sensitive data stores. The risk of mixing sensitive data with data of lower trust must be carefully assessed." [2]

Therefore, the isolation and overall security of VMs on a hypervisor will become critical. The use of live migration tools could bring an entire network out of compliance if used improperly. Additionally, the need for on-demand virtualized capacity means that the security must scale with capacity changes. This requires an immediate scaling of virtualized security solutions.

Organizations Want To Secure External Access And Isolate Virtual Machines

The primary business objective driving interest in virtual security is the need to secure traffic to virtual applications from outside the data center (see Figure 4). Organizations must ensure that remote users can securely authenticate to and access virtual applications within the data center. But there is much more to virtualization security than just secure access.

Figure 4
Virtualization Security Business Objectives



Base: 79 IT decision-makers responsible for data center security at North American organizations (multiple responses accepted)
Source: A commissioned survey conducted by Forrester Consulting on behalf of Cisco Systems, December 2011

Compliance is a growing driver in the area of virtualization security. Companies are becoming aware of the intersection of virtualization and security and 35% of respondents now view business compliance as a virtual security objective.

Organizations are also very concerned with isolating workloads from each other within the data center, especially workloads that share the same underlying physical server. Forty-seven percent of respondents indicated that logical isolation of virtual applications was an important business objective. There is a direct relationship between compliance drivers and VM or workload isolation. Because virtualization enables organizations to significantly reduce their hardware costs by consolidating physical servers, the drive to maximize server density is huge. This desire to increase virtual server density is often at odds with security as the physical separation between application servers has been removed, and the ability to enforce security policies with traditional security appliances on mobile workloads is practically impossible. For example, there are concerns that an externally facing website VM sitting on the same hypervisor as a sensitive database VM could increase the risk of database compromise via the external web server. Therefore, expect the desire to logically isolate VMs with security policies based upon application types or VM attributes to increase.

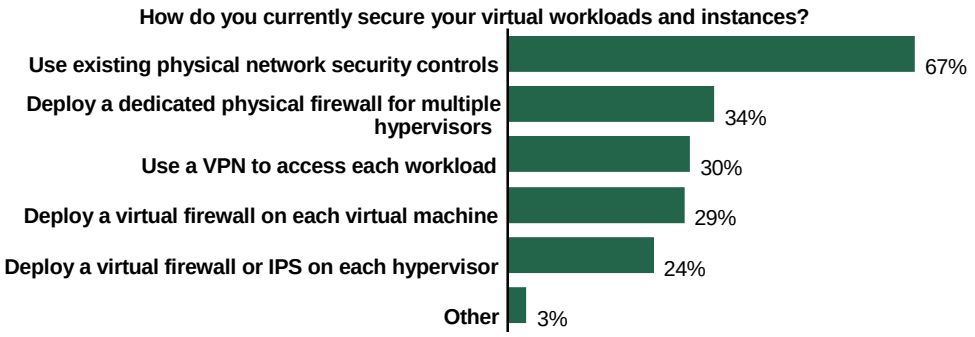
Traditional Network Security Controls Protect The Virtual Environment

The transition to virtual environments has been slow and methodical. When virtualization technologies were first introduced, those deployments were limited and often experimental. The only security controls available at that time were designed to secure physical server environments. It's no shock, therefore, to find that 67% of organizations are today using existing network security controls to protect virtual environments (see Figure 5).

"We secure the network architecture today using a hardware firewall that we have already implemented. But we see that this kind of solution needs to be changed and migrated." (Senior Network Engineer at a European telecoms operator)

Despite the wide deployment, existing network security solutions don't provide adequate security for virtual environments. They lack visibility, aren't virtualization-aware, and are unable to apply granular security controls to the virtual machines (VMs) operating within the dynamic virtual environment. Demonstrating compliance within virtual environments is also a challenge using traditional technologies. Organizations must finder a better way to secure mission-critical workloads.

Figure 5
Traditional Network Security Solutions Secure Today's Virtual Environment



Base: 79 IT decision-makers responsible for data center security at North American organizations (multiple responses accepted)
Source: A commissioned survey conducted by Forrester Consulting on behalf of Cisco Systems, December 2011

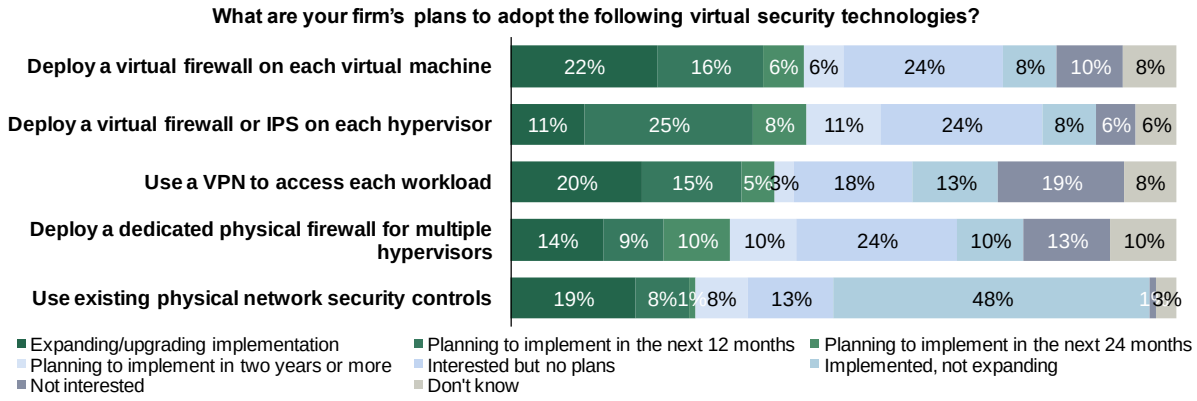
New virtual security technologies have been developed recently and there has been some noteworthy uptake of these controls as well. For example, 29% of organizations have deployed a virtual firewall on each virtual machine, while 24% have deployed a virtual firewall or IPS on each hypervisor instance. These results indicate that organizations are already realizing that there are better solutions for securing their virtual environments than the status quo.

Organizations Will Deploy Virtualization-Aware Security Solutions

Although organizations are predominantly leveraging existing security appliances to secure virtual servers for the sake of cost efficiency, the market seems to recognize there are limitations to this approach. The limitations can compromise VM mobility and further server consolidation and increase the complexity of compliance policies when implementing virtual applications on shared infrastructures. Forrester research indicates that the vast majority of new security investment will be in virtual security solutions that can overcome these challenges and accelerate the virtualization and cloud-readiness of key applications. Over the next two years, look for growth in areas that apply security policies specific to the VM itself. For example, 44% of organizations surveyed expect to deploy or expand deployments of virtual firewalls on each VM in the next 24 months (see Figure 6). Deploying these controls on each hypervisor, across multiple VMs, will have a slightly smaller uptake according to our survey, with 36% of companies looking to protect the

hypervisor itself. Because a hypervisor can host numerous VMs, success in this area could drive further adoption, as shared security controls across several VMs could prove to be more scalable and therefore more cost-effective.

Figure 6
Virtual Firewall Deployments Will Increase



Base: 79 IT decision-makers responsible for data center security at North American organizations
(percentages may not total 100 because of rounding)
Source: A commissioned survey conducted by Forrester Consulting on behalf of Cisco Systems, December 2011

The network will remain a widely used enforcement point, however. Respondents will continue to use existing network security controls to protect virtualized data centers, but future investment will be in the direction of virtualization-aware security solutions that overcome the challenges of scale, application mobility, and cloud-readiness. Look for VM- and hypervisor-hosted security controls to augment, not replace, existing network security devices as more sophisticated policy controls are required.

Methodology

This Technology Adoption Profile was commissioned by Cisco Systems. Forrester leveraged its Forrsights Hardware Survey, Q3 2011, and isolated responses of IT decision-makers at large North American enterprises with 5,000 or more employees. Forrester Consulting supplemented this analysis with custom survey questions asked of 79 IT decision-makers. The respondents were asked about their virtual security priorities and challenges and what they plan to look for in a virtualization security solution. This supplementary survey was conducted in December 2011. For more information on Forrester's data panel and Tech Industry Consulting services, go to www.forrester.com.

[1] According to the PCI DSS Virtualization Guidelines (https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf), "If any virtual component connected to (or hosted on) the hypervisor is in scope for PCI DSS, the hypervisor itself will always be in scope." (2.2.1 Hypervisor)

[2] See Section 3.5 of the PCI DSS Virtualization Guidelines: Mixing VMs of Different Trust Levels (https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf)