A comprehensive framework for securing virtualized data centers

Business white paper

Contents

Experiencing the virtualization wave

As data center virtualization reaches an adoption inflection point, HP recognizes the growing need for security solutions that can address this new reality of expanding virtualization and the security challenges that it presents. According to a report by Garter Group (Gartner EXP, January 2010), the top two priorities for the CIOs surveyed were: (1) virtualization and (2) cloud computing. This highlights the trend toward the use of these technologies to do more with less in the data center. The examples of organizations being asked to deploy more applications, to handle more users, and to do so on a smaller budget than they were given last year spans vertical industries.

It is estimated that today more than 16% of workloads are already running on virtual machines and that this number is expected to grow to 50% by 2012 (Gartner, Oct. 2009).

It is estimated that today, more than 16 percent of workloads are already running on virtual machines (VMs) and that this number is expected to grow to 50 percent by 2012 (Gartner, October 2009). Clearly, virtualization is moving to the mainstream and may soon be overtaking non-virtualized environments as a method for deploying applications across most vertical industries and in many geographies.

Organizations realize the benefits of moving to virtualization. According to a Phenom Institute report (Ave Total Cost of a Data Breach, Jan. 2010), the top reasons for customers to move to virtual servers for their applications are:

- To cut costs via server consolidation (81 percent)
- To improve disaster recovery (DR) and backup plans (63 percent)
- To provision computing resources to end users more quickly (55 percent)
- To offer more flexibility to the business (53 percent)
- To provide competitive advantage (13 percent)

Addressing virtualization security challenges

Recognizing these trends for the broad adoption of virtualization raises the question: will moving to virtualization make security for the network easier or more difficult to achieve? In a recent report conducted by Applied research ("2010 State of Enterprise Security Survey – Global Data"), some 2,100 of the top IT and security managers in 27 countries were surveyed about their opinions regarding this question. The results reflected a definite lack of consensus. The report showed that one-third of the group think virtualization and cloud computing make security "harder," while one-third said it was "more or less the same," and the remainder said it was "easier." The results seem to indicate that many are either in the process of defining policy for virtual environments, or have chosen to postpone that effort until a later date.

Perhaps, as a result of this failure to tackle the security question when deploying virtualized servers, there are experts who believe that the majority of virtual deployments may be less secure than physical deployments. Neal MacDonald of Gartner Group has estimated that "60 percent of virtualized servers will be less secure than the physical servers they replace." Neal also identifies some of the most common security risks for data center virtualization projects (Addressing the Most Common Security Risks in Data Center Virtualization Projects, Gartner, Inc. January 25, 2010):

- Information security isn't initially involved in the virtualization projects
- A compromise of the virtualization layer could result in the compromise of all hosted workloads
- Workloads of different trust levels are consolidated onto a single physical server without sufficient separation

- Adequate controls on administrative access to the hypervisor (Virtual Machine Monitor) layer and to administrative tools are lacking
- There is a potential loss of Separation of Duties (SOD) for network and security controls

Understanding security hype

While there are real challenges to deploying applications securely in a virtual environment, there is also a fair amount of hype surrounding the topic. While some of the areas of vulnerability and possible attack scenarios that have been identified are realistic possibilities, they are not a practical reality. Many of these potential attacks are not being encountered with any frequency, or at all. Those being discussed include:

- **Hyper-jacking**: Attacks targeted at subverting or layering a rogue hypervisor on a virtual server
- **VM Escape**: An exploit that enables a hacker to move from within a VM to the hypervisor
- **VM Hopping**: An instance in which one VM is able to gain access to another VM
- **VM Theft**: Unauthorized acquisition of a file containing VM
- **VM Sprawl**: The proliferation of virtualized server workloads

Evaluating virtualization security

The virtualization environment is not inherently insecure. However, most virtualized workloads today are being deployed in an insecure manner. This is a result of the immaturity of virtualization security tools and processes, and limited security training of staff, resellers, and consultants associated with virtualization. As virtualization platforms become the most important x86-based IT platforms in the next-generation enterprise data center, the combination of more workloads being virtualized and workloads becoming more mobile creates a complex and dynamic environment that may be even more difficult to secure as it grows.

A key factor to consider when approaching virtualization security is that the hypervisor becomes a high-value target of attack because of its control over the entire virtual environment. As a result, it can present the following risks:

- A hypervisor attack could allow authorized access to all hosted workloads
- A hypervisor Denial of Service (DoS) attack could cascade to all hosted workloads
- Increasing third-party integrations can expand the attack surface
- Incorrect or unauthorized configurations may magnify risk exposure
- Organizations may have to immediately implement untested vulnerability patches or leave at risk a system with an exposed critical vulnerability

Hypervisors must be considered mission critical and secured appropriately, much like operating systems, and require security because of the risks to the system and applications.

Another factor to consider is that deploying virtual servers is akin to adding another access layer to the network. It breaks traditional network design assumptions of one-to-one mapping of access port to server (OS+App). It also allows local communication between Virtual Machines that do not "hit the wire," and therefore, are not seen by traditional network-based security devices such as firewalls and IPSs. The virtual switches built into a virtual environment generally lack the monitoring capabilities that are common among their physical switch counterparts (for example, mirroring). Unfortunately, these unmanaged vSwitches provide poor overall visibility, making security more challenging.

Separating duties

Provisioning and management of virtual switches may also present some unique security challenges. In most cases, these functions are performed by those who manage the applications within an organization—the operations and server teams. Since much of this activity is out of the control and view of the networking and security teams, it often results in a situation where there is little or no integration with standard security controls or security tools. This contributes to an overall lack of visibility, added difficulty in detecting topology and making configuration changes, and the absence of configuration auditing that would be common practice in the physical network.

The virtual switches built into a virtual environment generally lack the monitoring capabilities that are common among their physical switch counterparts (for example, mirroring).

Implementing trust zones

For the physical network, organizations are used to setting up segmented areas or trust zones, to keep applications and associated data with different levels of sensitivity and user permissions from one another. In the virtual environment, workloads of different trust levels may operate on the same physical server or vSwitch, so they do not follow the physical standards for zone separation. The virtual machines need their own efficient zone definitions and policies to be adequately protected, but the distributed vSwitch increases the risk of incorrect or unauthorized virtual machine configurations. Therefore, the ability to maintain trust zone definition through the workload lifecycle, as well as the auditing of zones to make sure that they have workload compliance, is very important.

The common practice of moving VMs, via vMotion for instance, for disaster recovery or other purposes, also presents a set of security control challenges. Maintaining security policies for workloads at rest, while they are operating, and when they are being moved to a different set of resources is important to the overall security of the data center. The situation is often further complicated by the need to migrate or translate appropriate security as applications are moved to the internal or external cloud services.

Tackling the security challenge

Protecting high value targets

HP TippingPoint secure virtualization framework delivers the following capabilities to help organizations protect their high value virtual assets:

- Inspection of ingress and egress traffic with a purpose-built physical intrusion prevention system (IPS) platform
- Deployment of in-line inspection and automated threat blocking for protection from targeted hypervisor attacks
- Utilization of vulnerability shielding for zero-day protection of hypervisor and hosted workloads
- Implementation of options for virtual and physical IPS solutions to enable consistent polices, segmentation, and trust zones across both physical and virtual data center environments
- Industry-leading security research team, Digital Vaccine Labs (DV Labs) which is focused on conducting vulnerability research for data center virtualization tools and applications

Controlling the "New Access Layer"

The TippingPoint secure virtualization framework allows organizations to gain control of the virtual environment by introducing in-line security policy enforcement. The TippingPoint Virtual Controller (vController) and Virtual IPS (vIPS) solutions are purpose-built to secure the virtual infrastructure, and enable organizations to gain visibility and control of virtual network traffic flows. They allow for the enforcement of trust zones and network segmentation with IPS and virtual firewall. TippingPoint solutions perform in-line inspection and

automated threat blocking within the virtual servers and between trust zones. They provide the same policies and filters across both physical and virtual servers to simplify overall security management for the data center.

Inspection offload with vController

The TippingPoint vController takes advantage of the performance characteristics of the purpose-built TippingPoint N-Platform, an IPS that delivers excellent performance and accuracy in its class for detecting and stopping threats up to the application layer. The vController provides a direct path to the TippingPoint IPS appliance to inspect and control VM-to-VM communications. Using the VMsafe API, the vController efficiently directs appropriate traffic to the IPS and its leading threat suppression engine (TSE) facilitates peak performance and control required in the virtual data center. This greatly reduces the consumption of host resources in places where they may be limited. The vController and IPS platform also operate in unison to support high-availability (HA) capabilities, including failover of the vController when HA requirements and configured policy dictate. Using the vController is among the best options for high-density virtual server environments.

Virtual IPS

The TippingPoint vIPS compliments the vController by providing a purpose-built IPS virtual appliance for deployments where a physical IPS device is not practical. This option leverages host resources for inspection and control, and is an excellent solution for low-density virtualization areas such as remote offices or branch offices (ROBO). Some implementations where a virtual IPS appliance may be practical include:

- Office-in-a-box ROBO deployments where all workloads are virtualized within a single, redundant box
- Disaster recovery environments
- Public cloud environments where security is offloaded to the cloud along with production workloads
- Peak demand capacity due to seasonality where cost constraints dictate a lower cost solution

Security management

One of the most critical aspects of securing virtualization is the ability to manage the environment. In particular, policies must be assigned by VM, zone, or both, rather than by the traditional location or network connection. The TippingPoint solution leverages proven management through a visual console that enables visibility and control of this dynamic environment. It automates trust zone assignments for new or un-trusted workloads, it confirms that policies follow a VM regardless of its current state (in motion, powered on, or powered off), and enables cloned VMs to inherit the policies of the VM from which they were cloned (the parent VM).

Figure 1: Secure virtualization framework components

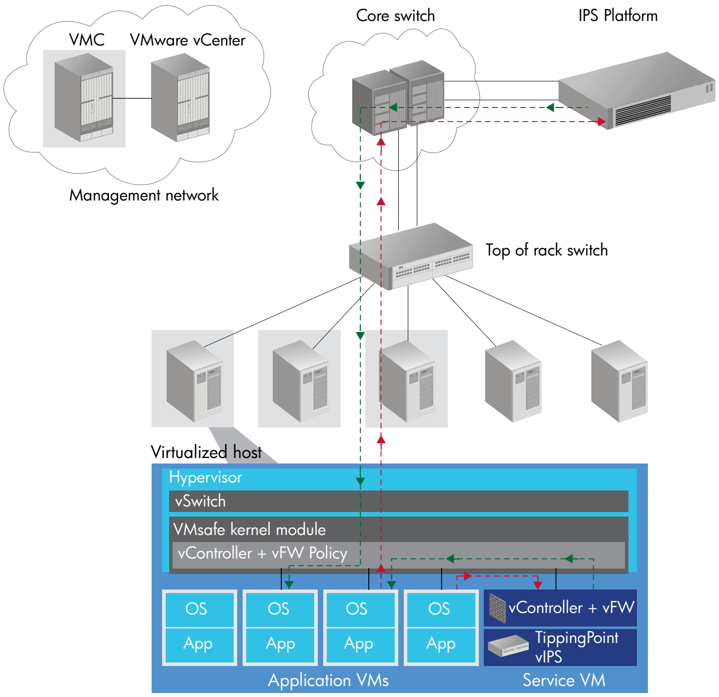
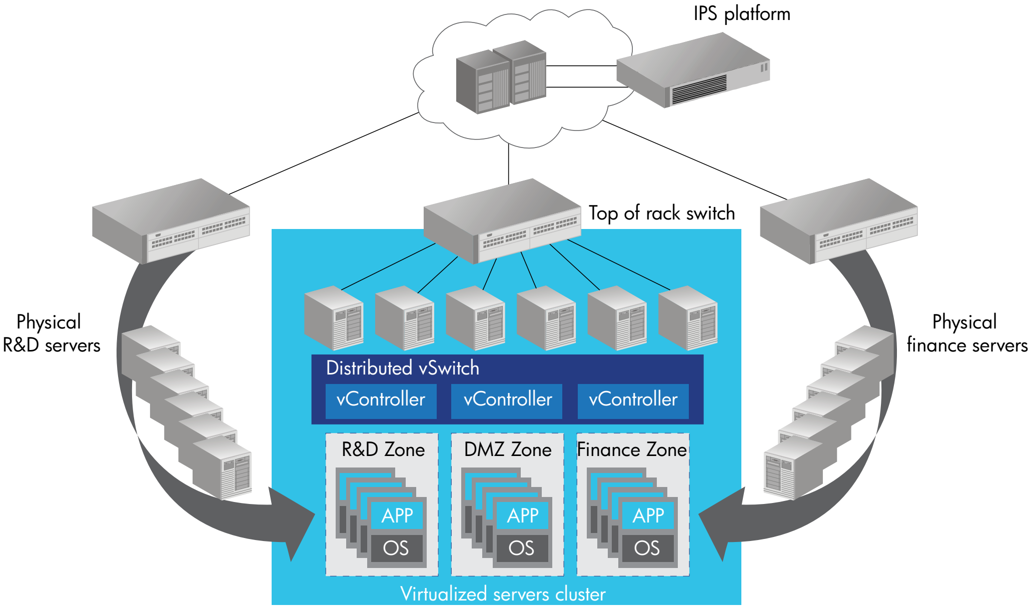


Figure 2: Security model for unified physical and virtual data center security



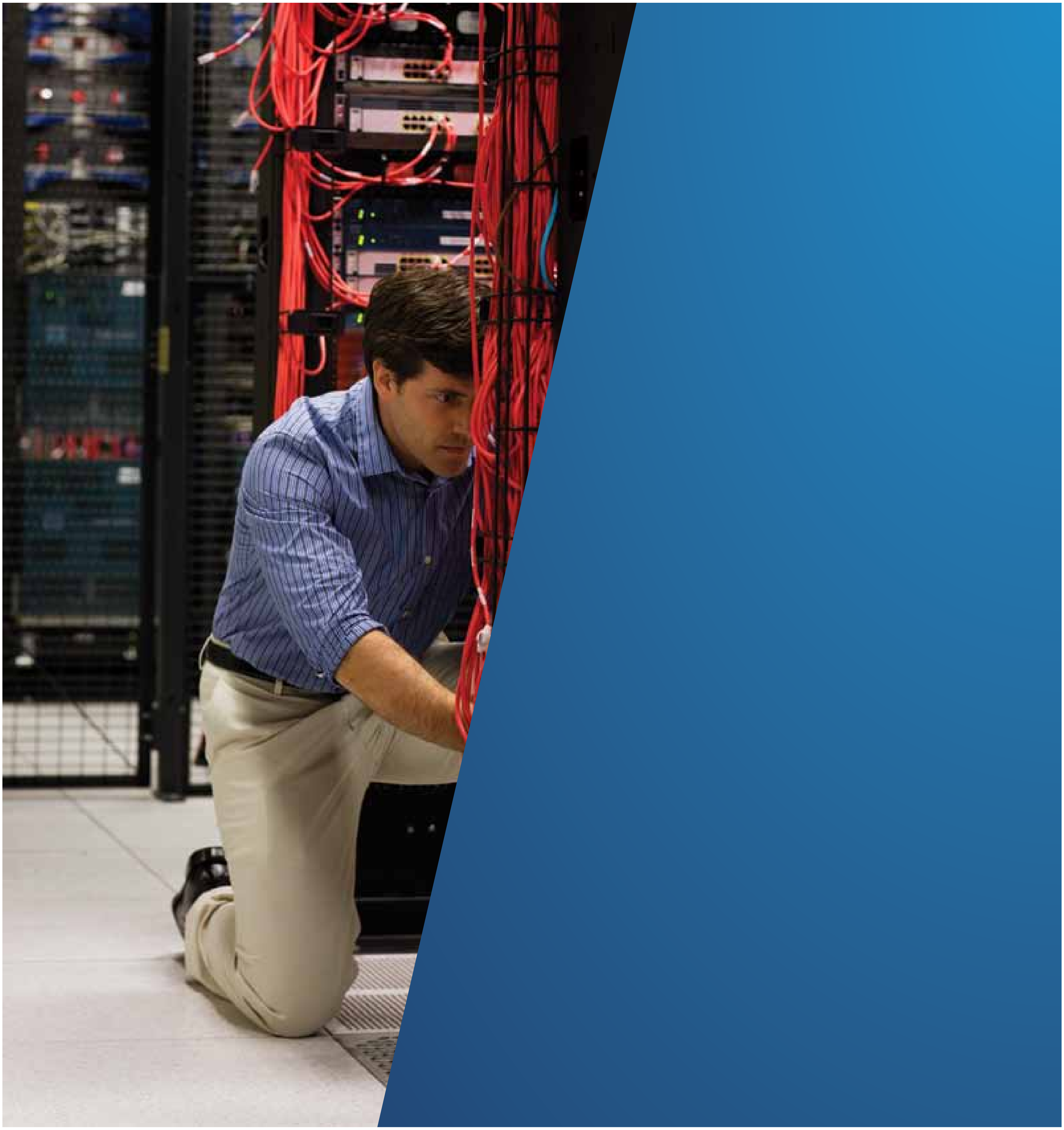
Providing proven and timely threat coverage
TippingPoint DV Labs is the premier security research organization for vulnerability analysis and discovery. Its team consists of industry-recognized security researchers that apply their cutting-edge engineering, reverse engineering, and analysis talents to their security research that has resulted in undisputed industry leadership in vulnerability discovery. The by-product of these efforts fuels the creation of vulnerability filters that are automatically delivered to customers' IPS platforms through the Digital Vaccine service. This service enables evergreen (up-to-date) protection against emerging threats. Digital vaccines are delivered to customers at least twice a week, or immediately when critical vulnerabilities emerge, and can be deployed automatically without IT interaction. Digital Vaccine filters are created to address specific exploits as well as potential attack permutations, protecting customers from zero-day threats to operating systems, services, applications, and virtual infrastructure.

Summary

The effectiveness of HP TippingPoint security solutions has been proven by deployments in thousands of organizations worldwide, including many Fortune 1000 and Global 1000 companies. These solutions are particularly valued as enterprises accelerate migration of their production workloads and mission-critical assets to the virtualized infrastructure. The TippingPoint secure virtualization framework—with its combination of purpose-built IPS platforms, enterprise-class management solutions, and industry-leading threat research and security filter development—addresses the unique requirements of the most demanding and virtualized data center environments.

Your next step

To learn more about how HP can enhance security in a virtualized data center environment, visit **www.tippingpoint.com**



Share with colleagues

Get connected

www.hp.com/go/getconnected

Get the insider view on tech trends, alerts, and HP solutions for better business outcomes

© Copyright 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA1-9777ENW, Created July 2010