

A background image showing a person's hand pointing at a laptop screen. Overlaid on the image are several semi-transparent circular gauges with numerical markings, suggesting a technical or data-related environment.

Meeting the Challenges of Virtualization Security

Coordinate Security. 

 Server Defense for
Virtual Machines

A Trend Micro White Paper | August 2009

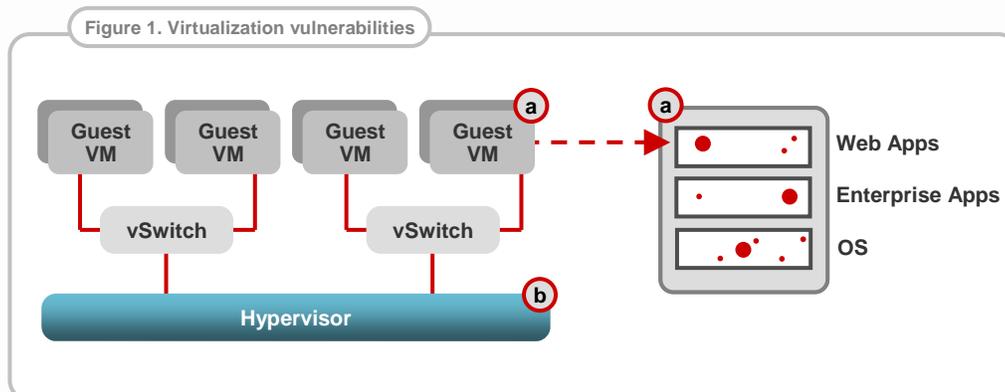
I. INTRODUCTION

Virtualization enables your organization to attain significant gains in efficiency and cost-effectiveness, along with the additional benefits of a greener consolidated datacenter, increased scalability and improved time to resource fulfillment. Unfortunately, the advantages of virtualization are balanced by increased risk exposure as virtual systems in your datacenter face many of the same security challenges as your physical servers, in addition to a number of unique challenges in protecting these IT resources. Your organization needs to consider which security mechanisms can best protect both physical and virtual servers, particularly as a virtualized architecture fundamentally affects how mission-critical applications are designed, deployed, and managed.

Trend Micro offers real solutions to these challenges. Leveraging innovative technologies brought to Trend Micro with the acquisition of Third Brigade, and our long-standing security experience, we have developed a coordinated approach for both server defense—including intrusion detection and prevention, firewall, integrity monitoring and log inspection—and malware protection that can be deployed today. It is architected to take advantage of the additional capabilities that virtualization vendors are adding to their platforms, such as those introduced through the recently released VMware vSphere™ 4 which includes access to VMware VMsafe™ APIs. We provide the necessary level of protection to improve the security of mission-critical applications in virtualized environments. This paper discusses the Trend Micro coordinated approach to server defense for virtual machines.

II. CHALLENGES OF VIRTUALIZATION SECURITY

A virtualized system uses the same operating system—and enterprise and Web applications—as a physical system. The primary threat to these virtualized systems is the capacity of malware to remotely exploit vulnerabilities in these systems and applications [see Figure 1a], although there are also vulnerabilities that can be exploited in the system's hypervisor [see Figure 1b].



Virtualization vendors continue to work to simplify the service console, as seen with VMware ESXi, and as such reduce its potential attack surface. Most hypervisor vulnerabilities will not be remotely exploitable, since the hypervisor does not have services which terminate remote protocols. Hypervisor vulnerabilities will typically be exploited from malware which compromises a virtual machine (VM). One of the best methods to protect against attacks to hypervisor vulnerabilities is to prevent malware from getting installed in the virtual environment in the first place.

The dynamic nature of virtualized environments presents new challenges for intrusion detection/prevention systems (IDS/IPS). Because virtual machines can quickly be reverted to previous instances, and easily moved between physical servers, it is difficult to achieve and maintain consistent security.

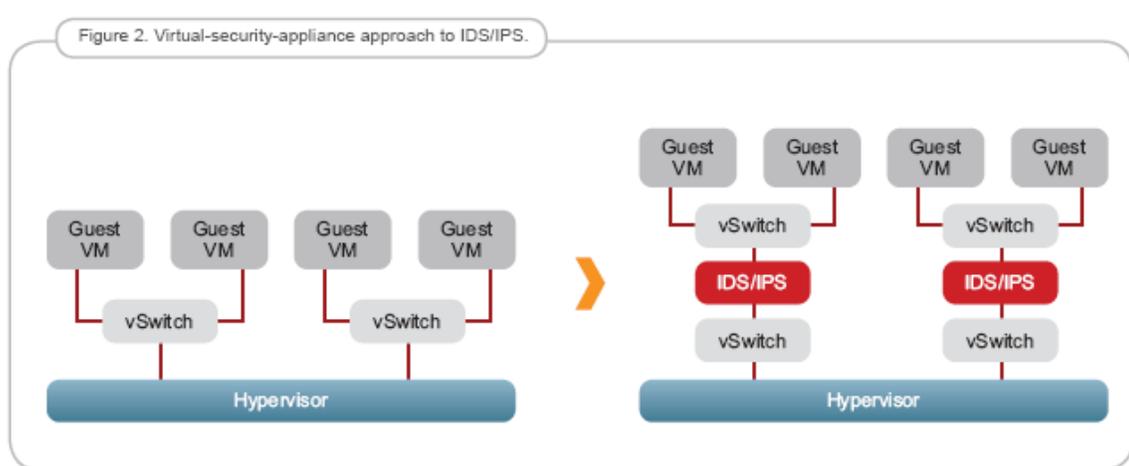
To create an effective approach to virtualization security, you should be guided by the same security principles that have evolved to protect your physical IT resources. One of these principles is “defense in depth,” which is a fundamental security requirement for organizations that recognize the “de-perimeterization” that has emerged in their IT infrastructure. This principle is supported by industry best practices, and organizations such as the Jericho Forum include it as part of their security recommendations. Virtualization has made the challenge of de-perimeterization even more apparent, and the need for leading-edge security even greater, because of the inability of appliance-based security to deal with attacks between VMs on the same physical system. Best practices for security are crucial. Among the forum's other guiding principles are these rules:

- The scope and level of protection should be specific and appropriate to the asset at risk
- Business demands that security enable business agility and be cost effective
- Whereas boundary firewalls might continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves
- In general, the closer to an asset that protection is provided, the easier it is to protect that asset

Applying these and other principles to the virtualized datacenter, we see a clear need for mechanisms to be deployed directly on the physical server to protect these virtualized systems—an approach to virtualization security that enables protection to occur as close as possible to the asset itself.

III. CURRENT APPROACHES IN VIRTUALIZATION SECURITY

Prior to widespread availability of security solutions purpose built for VMware VMsafe APIs, two initial approaches are usually taken with security software to protect virtual machines—one is to apply a virtual security appliance within the virtualized computing environment, to monitor the traffic flow between a virtual switch (vSwitch) and one or more guest VMs [see Figure 2].

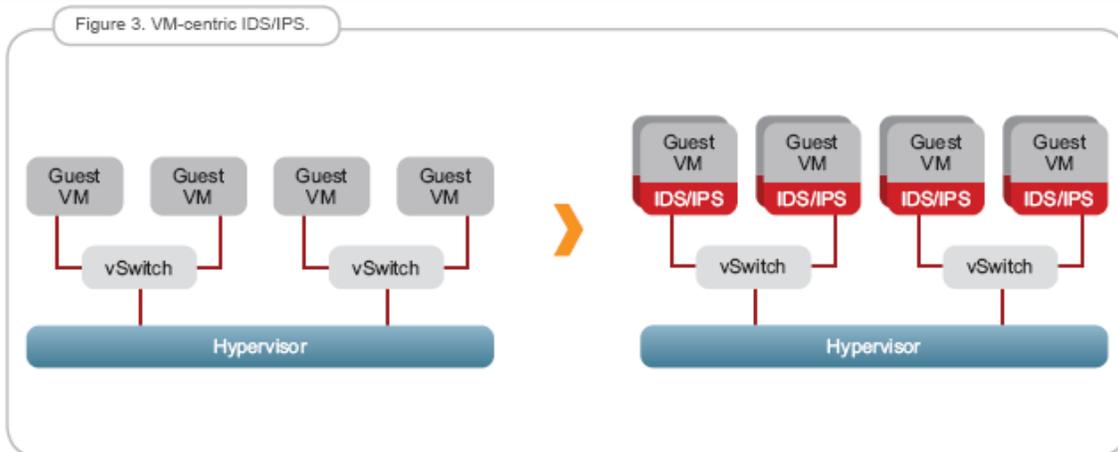


Although a virtual-security-appliance solution provides IDS/IPS protection from attacks originating on the network, there are significant limitations to this option:

- **Inter-VM traffic**—Virtual security appliances must be placed in front of a vSwitch, and they cannot prevent attacks between VMs on the same vSwitch
- **Mobility**—If controls such as VMware VMotion™ are used to transfer a VM from one physical server to another, the security context is lost. It is necessary to configure the clustering of virtual security appliances for every potential destination to which a VM could be relocated, resulting in a corresponding negative impact on performance
- **Non-transparency**—Because the virtual network architecture must be altered to deploy virtual security appliances, this will have adverse administrative and performance impacts on the existing system
- **Performance bottlenecks**—The virtual security appliance must process all traffic between VMs and the network, which can result in a performance bottleneck

TREND MICRO VIRTUALIZATION SECURITY

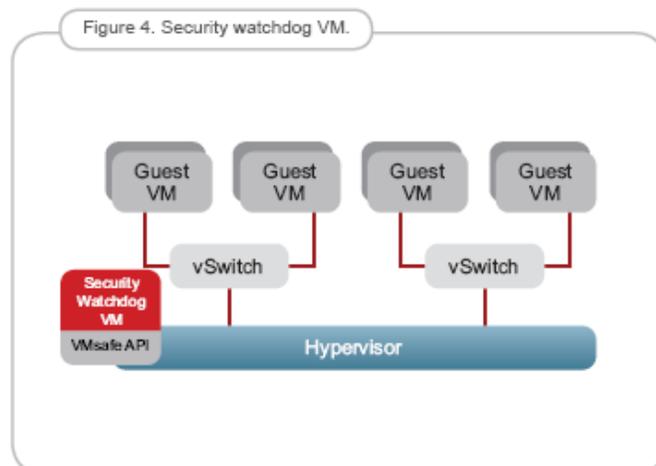
With the other approach, the same IDS/IPS functionality can be deployed on each virtual machine [see Figure 3].



Unlike the virtual-security-appliance method, the VM-centric approach avoids the limitations of inter-VM traffic, mobility, and a lack of visibility. Although the VM-centric option also has a performance impact on the system, it is distributed across the VMs in the IT infrastructure. However, a VM-centric architecture still faces the challenge of deploying an IDS/IPS security agent on each VM. This is reduced by the use of mechanisms such as templates—as noted by VMware in their online tutorial, “Working with Templates”—to deploy a common security agent across each virtual machine. However, the dynamic nature of virtualized environments can still result in virtual machines being introduced to the production environment without a security agent in place.

IV. SECURITY WATCHDOG VIRTUAL MACHINE (VM)

The VMware VMsafe program enables you to deploy dedicated security VMs with privileged access to hypervisor APIs. This makes it possible to create a unique security control, a security watchdog VM, as noted in Gartner’s report, Radically Transforming Security and Management in a Virtualized World: Concepts. This security watchdog VM is a new means of implementing security controls within a virtual environment [see Figure 4].



Security watchdog functions utilize introspection APIs to access privileged state information about each virtual machine, including their memory, state, and network traffic. This removes the inter-VM and non-transparency limitations of the virtual-security-appliance approach for IDS/IPS filtering, because all network traffic within the server is visible without changing the virtual network configuration. However, mobility and performance impacts must still be considered when performing IDS/IPS filtering in security watchdog VMs.

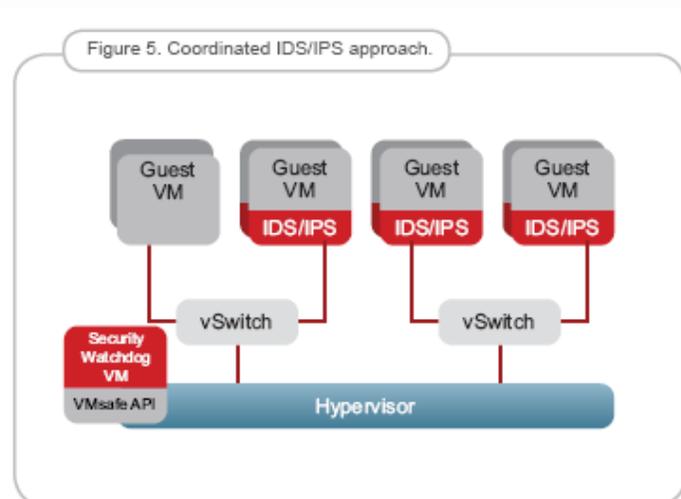
A wide range of security functions—including antivirus, encryption, firewall, IDS/IPS, and system integrity—all potentially can be applied in security watchdog VMs. Virtual security appliances are being repurposed to use these APIs, and VM-centric agent technologies also will be redesigned to execute in security watchdog VMs. However, flexibility still will be required to deploy some functionality within a security watchdog VM and within some VMs using VM-centric agents, because:

- Certain security functionality only can be achieved by VM-centric agents—for example, dealing with encrypted traffic or accessing certain real-time state information
- Performance tradeoffs exist between implementing a solution via security watchdog VM versus deploying a VM-centric agent
- Necessary introspection APIs are being developed and released in stages, you need mechanisms to deliver security during the transition as security watchdog VM functionality emerges

As a result, a coordinated approach is needed—one providing both the benefits of a VM-centric approach and the advantages offered by introspection APIs, to provide intelligent options that minimize performance bottlenecks and redundant controls while cost-effectively reducing security risks. Trend Micro offers you a solution to meet this need.

V. A COORDINATED SECURITY APPROACH

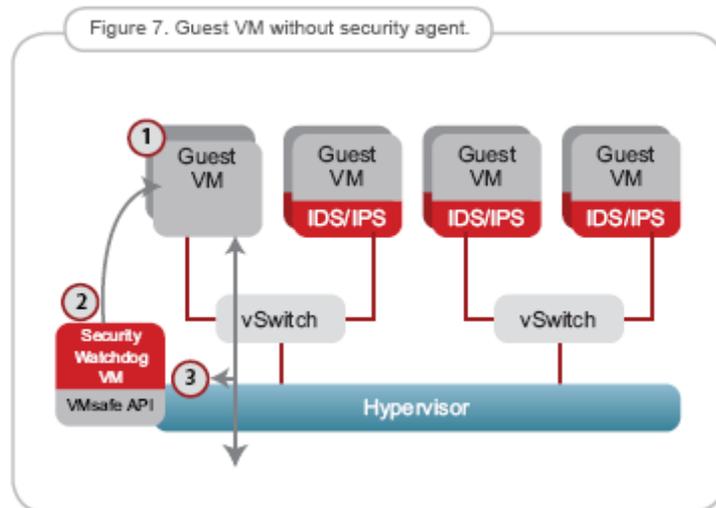
Our coordinated approach to protecting virtualized environments consists of a VM-centric agent that can be deployed on individual virtual machines, as well as a security watchdog VM deployed to protect multiple virtual machines. This architecture ensures that critical IT assets—VMs—can be protected by deploying software on the assets themselves, while noncritical assets are protected by the security watchdog VM [see Figure 5].



TREND MICRO VIRTUALIZATION SECURITY

As previously noted, not every VM necessarily will have a security agent installed. Figure 7 outlines coordination when a guest VM is deployed without requiring an agent:

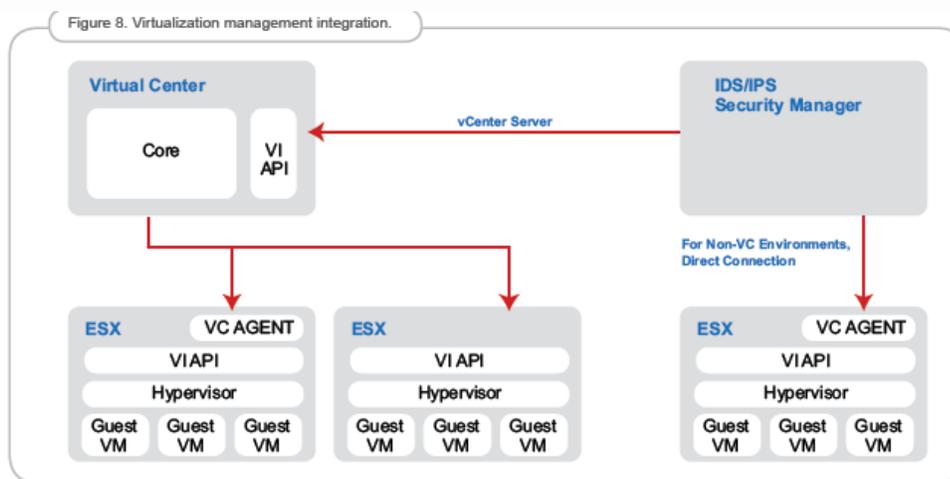
- When a guest VM is started, the security watchdog VM is notified
- If the guest VM does not require an agent, the security watchdog VM scans the guest configuration and applies appropriate IDS/IPS filtering within the security watchdog VM
- Data flows through the security watchdog VM via VMsafe APIs, with IDS/IPS filtering applied.



This architecture's advantage is that traffic intended for VMs with an IDS/IPS security agent deployed incurs no significant delay, since traffic is routed directly from hypervisor to guest VM. Traffic for the remaining agentless virtual machines can be processed centrally by the security watchdog VM, with minimal impact.

VIRTUALIZATION MANAGEMENT INTEGRATION

Virtualization platforms typically include a centralized management system for managing the deployment of physical hosts and VMs, such as VMware vCenter Server. The IDS/IPS system's security management function connects with this virtualization management system to obtain the configuration of hosts and virtual machines [see Figure 8].



TREND MICRO VIRTUALIZATION SECURITY

The layout of systems then can be displayed in a similar structure within the IDS/IPS security manager, to enable easy and effective management of physical host and virtual machines [see Figure 9].

ENTERPRISE MANAGEMENT

Enterprise-class IDS/IPS systems provide centralized security management that is integrated with virtualization management. This function defines and distributes policy to the IDS/IPS enforcement components and collects events for actions the enforcement component takes, such as attacks detected or prevented. Other key elements of centralized security management in a distributed IDS/IPS system include:

- Management scalability—The management component itself should be capable of virtualization into multiple VMs to enable scalable deployment and high availability
- Integration points—Such as syslog and Web services—so that IDS/IPS can be integrated into other enterprise security elements, including security information and event management (SIEM) systems
- Supporting security capabilities—Including role-based access control and an audit history of administrator actions
- Third-party evaluations—These evaluations, such as the Common Criteria for Information Technology Security Evaluation, assist in ensuring that a specific set of security parameters has been achieved

COMPLETE IDS/IPS FUNCTIONALITY

Although network traffic analysis is common to both virtual security appliances and VM-centric agents, the NIST Guide to Intrusion Detection and Prevention Systems defines host-based intrusion detection and prevention as including:

- Code analysis
- Network traffic analysis—deep packet inspection and application protocol inspection
- Network traffic filtering—firewall
- File system monitoring
- Log analysis
- Network configuration monitoring

Figure 9. Hosts and virtual machines.



Each of these areas of functionality also requires coordination between VM-centric agents and security watchdog VMs to ensure consistent security.

MULTIPLE VIRTUALIZATION PLATFORMS

Although VMware is the virtualization market leader, many other vendors are developing virtualization platforms—including Microsoft Windows Server Virtualization and Citrix XenServer. Although a security watchdog VM's depth of functionality will vary on each platform, Trend Micro's coordinated approach for virtualization security will be applicable to all.

SOFTWARE LICENSING MODELS

The transition to virtualized environments has drawn increasing attention to software licensing, as virtualization has had a significant impact on software just as it has revolutionized hardware utilization. Organizations expect licensing to increase software utilization by offering appropriate choices without inflating software costs. As organizations adopt the coordinated approach to IDS/IPS, flexible, "future-proof" licensing options are required that fit well in both physical and virtual environments. These include the ability to license IDS/IPS agents per VM, as well as the ability to license IDS/IPS functionality for an unlimited number of VMs on a physical server. License management mechanisms should ensure that organizations can track license use in a dynamic virtualized environment without adding complexity.

VI. CONCLUSION

While a virtualized IT infrastructure shares many of the same security challenges faced by physical server environments, you can leverage your investment in multiprocessor, multi-core architectures and virtualization software to provide the security mechanisms required to protect them. Additionally, virtualized IT resources can be protected both today and in the future, with security enhancements made as introspection capabilities, such as the VMsafe APIs continue to evolve in virtualization platforms. Adopting the coordinated approach with security software offered by Trend Micro enables optimized protection, immediate solution deployment and ensures a baseline of security for all virtual machines without introducing bottlenecks or redundant controls. Trend Micro enables you to expand your virtualization deployment to cover all of your mission-critical systems.

VII. WHY TREND MICRO

Trend Micro has been singularly focused on content security since its founding 20 years ago. With over one billion U.S. dollars in annual revenue, over 1,000 threat researchers—and over 4,000 employees—around the world, Trend Micro has the size, the speed, and the unique in-the-cloud core technology infrastructure required to handle today's enterprise content security. No other security vendor can match the strengths Trend Micro offers enterprises. That is why thousands of enterprises around the globe continue to put their trust in Trend Micro.

As the speed of threats increases, so do risks and costs. Enterprises are looking for security that is scalable, manageable, and capable of reliably staying ahead of new threats. Only Trend Micro offers the unique combination of immediate protection with less complexity. Powered by the innovative Smart Protection Network, Trend Micro Enterprise Security delivers immediate protection that improves automatically, closing the window of vulnerability before damage is done. Trend Micro also dramatically reduces the time to acquire, deploy, and manage security. With Trend Micro Enterprise Security, enterprises minimize their time to protection, reducing business risks and costs.

For more information please call or visit us at.
www.trendmicro.com/virtualization
+1-877-21-TREND

VIII. REFERENCES

- Gartner, Radically Transforming Security and Management in a Virtualized World: Concepts, Neil MacDonald, March 14, 2008
- Common Criteria for Information Technology Security Evaluation, www.commoncriteriaportal.org
- Jericho Forum, www.jerichoforum.org/
- NIST Guide to Intrusion Detection and Prevention Systems, <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>
- VMware, www.vmware.com/overview/security/vmsafe.html
- VMware tutorial: "Working with Templates," www.vmware.com/support/vc13/doc/c13templateintro.html
- VM World News, www.vmware.com/vmworldnews/esx.html

© 2009 Trend Micro, Incorporated. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. (WP01_VirtSec_080911US)