

McAfee®, Inc.

McAfee Total Protection for Virtualization Evaluation in VMware ESX and Microsoft Hyper-V Environments



Test Summary

Premise: In a dramatically short time, IT system architects have recognized the benefits of virtualized server environments and have deployed countless virtual servers. As with physical systems, these virtual servers need to be protected - when online or offline. McAfee addresses that challenge with a security solution that manages security for both physical and virtual environments.

McAfee, Inc. commissioned The Tolly Group to evaluate the effectiveness of McAfee Total Protection (ToPS) for Virtualization, managed by ePolicy Orchestrator (ePO) 4.0, in providing a comprehensive suite of security services to virtualized Microsoft Windows Server 2003 and Windows Server 2008 environments — online and offline — under both VMware and Microsoft’s Hyper-V server virtualization platforms.

Tolly engineers built virtual server environments using both VMware ESX Server version 3.5 and Microsoft Hyper-V. In these environments they deployed virtual instances of Microsoft’s Windows Server 2003 and Windows Server 2008. Engineers then exercised an extensive set of functions to illustrate that McAfee could provide extensive management and protection of virtual server environments in both online and offline states.

Tests were conducted in November and December 2008.

Test Highlights

- ▶ Delivers operational efficiencies with a single management platform for both physical and virtual environments via ePolicy Orchestrator
- ▶ Increases server reliability by automatically and transparently scanning and cleaning malware and updating the security profiles of offline images
- ▶ Provides virtualization-specific protection through anti-virus, anti-spyware, stateful firewall and host intrusion prevention
- ▶ Delivers cost-effective licensing model “per physical server”

Summary of Security Features Certified

Feature	Component	Certified
Manage security for physical and virtual servers	ePolicy Orchestrator	<input checked="" type="checkbox"/>
Automatically detect and remove malware and update virus signatures for online servers	VirusScan Enterprise/ Anti-spyware Enterprise	<input checked="" type="checkbox"/>
Automatically detect and remove malware and update security profiles for offline VMware, Microsoft and ISO images	VirusScan Enterprise for Offline Virtual Images	<input checked="" type="checkbox"/>
Protect virtual servers from corruption at the hypervisor level	Host IPS for server	<input checked="" type="checkbox"/>

Source: The Tolly Group, December 2008

Figure 1

Executive Summary

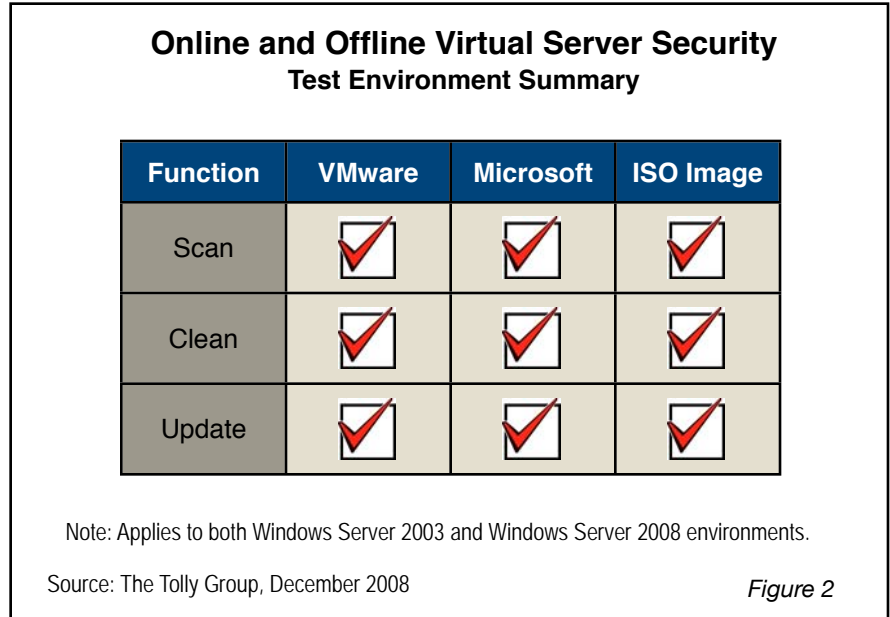
McAfee Total Protection for Virtualization extends the suite's extensive security coverage to online and offline virtual servers running in both VMware and Microsoft Hyper-V virtual server environments.

With the rapid rollout of virtualized server solutions, security professionals must contend with providing the same security for virtual servers as they do for physical servers. Furthermore, they must now concern themselves with attacks directed against the underlying hypervisor virtual infrastructure, as well as within a virtual machine and between virtual machines.

McAfee Total Protection for Virtualization is the first offering to provide a comprehensive solution for both traditional physical and next-generation virtual environments. This security suite protects online and offline virtual machines. Its security technologies include anti-virus, anti-spyware, stateful firewall, host intrusion prevention, and integrated, centralized management. A key element of the solution is the McAfee VirusScan Enterprise for Offline Virtual Images.

PROTECTING ONLINE AND OFFLINE VIRTUAL MACHINES

Tolly engineers verified that McAfee can successfully scan and clean malware and update security profiles of both Windows Server 2003 and Windows Server 2008 virtual



servers when running and also when offline without bringing these systems online. These automatic processes enable businesses to ensure up-to-date protection without the extra time and costs of manually updating offline and online systems. Tests were run with both servers implemented as virtual images in popular virtual image formats: 1) VMware, 2) Microsoft and, 3) ISO. (See Figure 2.)

FIREWALL & IPS

Physical servers are protected by physical separation, as well as by firewall appliances and network IPS systems. Virtual machines, on the other hand, have additional exposure, as many virtual servers reside on the same physical server host. Inter-virtual machine communication on a physical server host is invisible to the physical firewalls and IPS systems that reside outside of the server host. Thus, virtual machines can be susceptible to attacks from other machines on the virtual network and require additional protections.

Engineers validated that the firewall component of the McAfee suite could be used to block unwanted inbound and outbound traffic.

Engineers also validated the capability of McAfee Host IPS for server to protect virtual machines, key files, processes and registry entries from malicious access. (See Figure 3.)

MANAGEMENT & LICENSING

Engineers verified that both physical and virtual endpoints could be managed from a single instance of ePolicy Orchestrator. By using a single agent and single console management platform, businesses can save time and money by training and assigning fewer administrators to manage the many security technologies for both physical and virtual servers. Also from a reporting point of view, IT benefits from viewing its security all from a "single pane of glass."

From an economic perspective, it is important to note that McAfee prices the solution per physical server rather than per virtual server managed.

Thus, even if a user has 8, 12, 20 or more virtual servers running on a particular physical server, no additional McAfee licenses are required. This approach allows businesses to easily determine their licensing needs and to maximize the economic benefits of virtualization.

TEST ENVIRONMENT & METHODOLOGY

VIRTUAL SERVER SECURITY

For this test, engineers built both VMware ESX and Microsoft Windows 2008 Server Hyper-V virtual server environments. In each system, engineers created Microsoft Windows Server 2003 SP2 and Microsoft Windows Server 2008 virtual servers using the native virtual hard drive format of each respective virtualization platform. In addition, to provide an ISO image to test, engineers created both Windows server guest images on the VMware platform choosing ISO as the virtual disk image format.

McAfee Total Protection for Virtualization components were installed on each physical and virtual system. (See Figure 4 for component names and version levels.)

Each image was booted and loaded with an outdated security profile. The eicar.com test virus file was then loaded on to the root of the system (<http://www.eicar.org>) and the system was taken offline.

Using the administration console, engineers scheduled the offline image to be scanned.

After the scan, engineers booted the image and verified that: 1) the security software was up-to-date, 2) the eicar virus had been detected, and 3) the eicar virus had been removed from the system. This was done with each system implemented on each virtual disk image. This set of tests was also run with online virtual machines.

McAfee also provides non-Windows support for operating systems such as Linux and Solaris for components including Host IPS for server and VirusScan Enterprise for Linux, although these operating systems were not the focus of this evaluation.

VMWARE VIRTUAL INFRASTRUCTURE PROTECTION

Using the VMware server system, engineers attempted to make unauthorized changes similar to those that might be made by malware that could be present on the system. (See Figure 3.)

For the termination protection test, engineers attempted to terminate core VMware processes from within a virtual machine. These included: vmwareuser.exe, vmwaretray.exe, vmwareservice.exe

For the files and setting protection test, engineers attempted to delete files and modify key registry settings. Files and directories included:

C:\Windows\system32\driver\VMUS B.sys,

McAfee, Inc.

Total Protection for Virtualization

Virtualization Evaluation



C:\Windows\system32\driver\VMnetadpater.sys,

C:\Windows\system32\driver\VMnetbridge.sys,

Registry keys included:

\registry\machine\system\controlset001\services\vmusb*

\registry\machine\software\VMware,Inc.\VMnetlib,

\registry\user\5-1-5-21-2367631773\VMware,Inc.\RunningVMList*

For the VMware virtual machine files protection test, engineers attempted to delete files with the following file types: **/*.vmdk, **/*.nvram, **/*.vmsd, **/*.vmx, **/*.vmxf

In each case, engineers attempted to modify and/or delete the resource and verified that the McAfee solution detected this attempt and, based on the setting of the protection, either warn the user before allowing the action to proceed, or prohibiting the action completely.

This attack set covers represents a range of essential VMware resources.

For firewall tests, engineers first verified network connectivity between two systems by running Ping (UDP Echo) to illustrate that the two virtual machines could communicate. They then created a policy to block this application and verified that communication was prohibited.

For the resource test, engineers first validated that a virtual machine was able to access a USB-connected drive. Then the policy was changed to prohibit access and engineers verified that the device was not accessible by the virtual machine.

Virtual Infrastructure Protection

Threat	Protected
Prevent termination of virtual machine processes	<input checked="" type="checkbox"/>
Prevent modification of files and registry settings	<input checked="" type="checkbox"/>
Prevent modification of virtual machine files	<input checked="" type="checkbox"/>

Source: The Tolly Group, December 2008

Figure 3

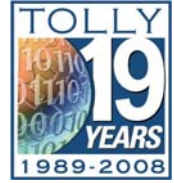
Security Components Evaluated

Vendor	Name	Version
McAfee	ePolicy Orchestrator	4.0
McAfee	VirusScan Enterprise	8.7.0.570
McAfee	VirusScan Enterprise for Offline Virtual Images	1.0.0
McAfee	Host IPS for server	7.0.0.688
McAfee	Anti-spyware Enterprise	8.7i
McAfee	ePolicy Agent	4.0.0.1180

Source: The Tolly Group, December 2008

Figure 4

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.



The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at:
 Web: <http://www.tolly.com>,
 E-mail: sales@tolly.com

EPOLICY ORCHESTRATOR

Engineers installed the management console on a Windows server system, and verified that the management system could communicate with and manage both the virtual servers, as well as physical servers.

TEST BED

The test bed consisted of three physical PCs - one for the management server and one for each of the virtualization platforms.

VMware ESX 3.5 Updated 3 and Microsoft Hyper-V Server 2008 provided the virtualization environments. (Hyper-V contains only the Windows Hypervisor, Windows Server driver model and virtualization components.)

The VMware system also was run on a PC with an Intel Core 2 Duo 3.2GHz processor and 4.0GB of RAM. The Microsoft system was run on a PC with an Intel Core 2 Extreme 3.0GHz processor and 4.0GB of RAM.

The ePolicy Orchestrator management system was run on a PC with an Intel Core 2 Duo 2.34-GHz processor and running Windows 2003 Server SP 2.

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

All trademarks are the property of their respective owners.

208344-Npabsu3-cb-VerL- 28JAN09