TEST REPORT

Tolly.

#211123
August 2011
Commissioned by Symantec, Corp.

Symantec Endpoint Protection 12.1 vs. McAfee and Trend Micro

Anti-virus Performance in VMware ESX Virtual Environments

Executive Summary

As IT architects scale deployments of virtual desktop infrastructure (VDI) solutions, they must be aware of the resource requirements of "always on" and high-use components such as endpoint security systems. In virtual environments, vendors can implement their solution as a client-based agent where all security processing takes place on the client, a virtual appliance that handles the anti-virus (A/V) workload or, possibly, some hybrid of the two approaches.

Symantec Corp. commissioned Tolly to benchmark the performance of its new Symantec Endpoint Protection 12.1 within virtual environments vs. comparable solutions from McAfee and Trend Micro. Specifically, this testing focused on the system resource requirements of each solution when performing on-demand and on-access scanning,and during distributed virus definition updates.

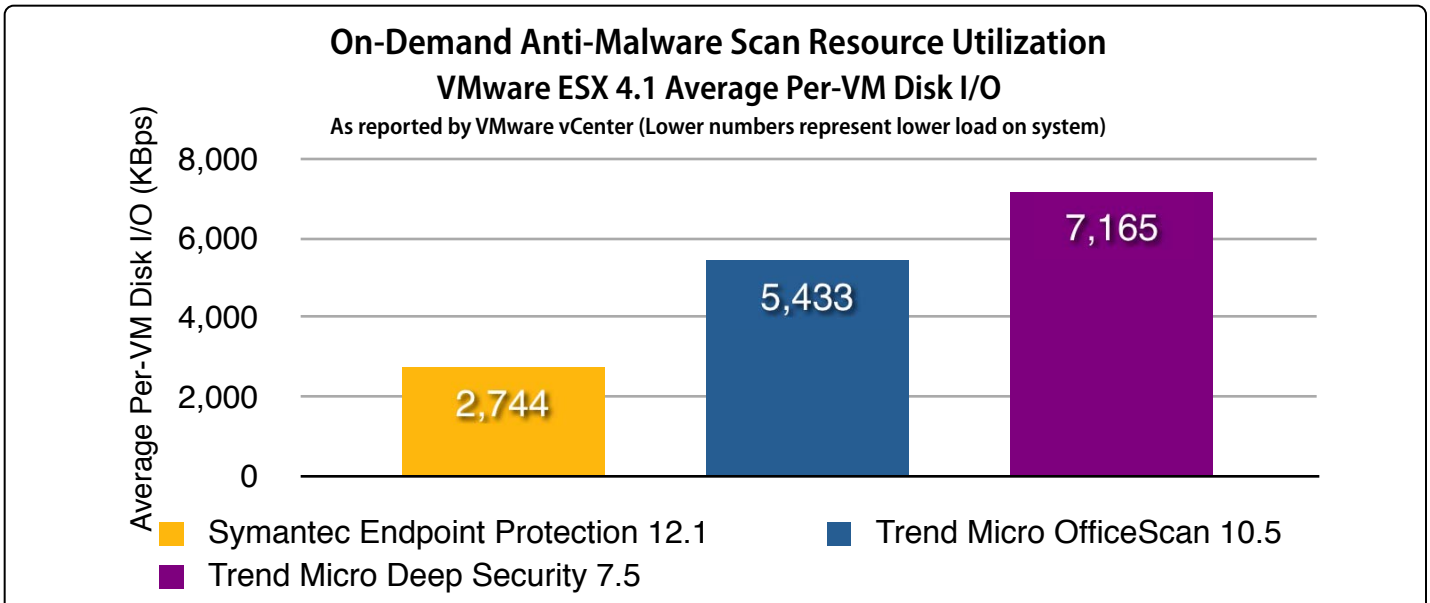
continued on next page...

TEST HIGHLIGHTS

Symantec Endpoint Protection 12.1:

1. Was able to perform an on-demand scan on each VM in about half the time while consuming 49% less disk bandwidth than comparable solutions

2. Used 20% less disk bandwidth when performing on-access scanning compared to Trend Micro's Deep Security



Note: Windows 7 Enterprise, 64-bit installations. Solutions instructed to scan 50 VMs. Reported results are average of 10 VMs. SEP configured to use shared insight cache to optimize scanning. Trend Office Scan pre-scan templates not used as all 50 VMs were identical and no scanning would take place. SEP completed each scan in12 - 13 minutes; the Trend Micro products required 23 - 24 minutes to complete each scan. The amount of data scanned varied across products. See report text for details. No A/V storms observed during the test. McAfee MOVE for VDI does not offer on-demand scanning.

Source: Tolly, June 2011

Figure 1

Executive Summary (con't)

The Symantec Endpoint Protection 12.1 solution was compared to two implementations each from McAfee and Trend Micro.

Like Symantec, the Trend Micro Office Scan 10.5 provides for a full agent on each client, and all processing is conducted on a client-by-client basis. Trend Micro's Deep Security 7.5 is implemented as a VMware virtual appliance that serves as a central point of processing for security activities, connecting to the clients using VMware's vShield Endpoint Agent

Both McAfee solutions were based on the vendor's Management for Optimized Virtual Environments, referred to by the acronym "MOVE" for virtual desktop infrastructure (VDI) environments 1.6. For the second McAfee solution tested, the vendor's host intrusion prevention system (HIPS) and SiteAdvisor products were layered on to the system. This allows the testing to provide relevant information both for customers that use MOVE by itself as well as those that layer on the other products for added security.

Testing encompassed various scanning and system update functions and was performed using 50 Microsoft Windows 7 Enterprise (64-bit) virtual machines. Tolly engineers measured critical system resources, disk input/output (I/O), CPU consumption and memory usage at both the virtual machine and VMware host levels.

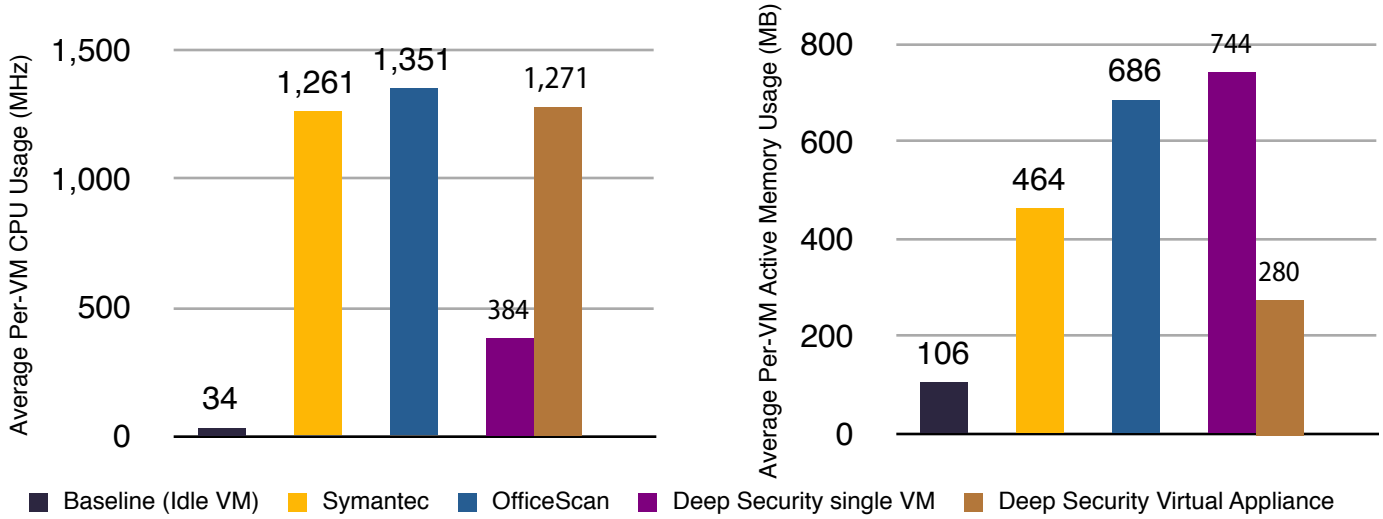
Symantec Endpoint Protection 12.1 demonstrated that, through use of its randomization algorithm for system task initiation, resource-intensive tasks such as on-demand scans and signature updates could be automatically distributed over a period of many hours, thus avoiding excessive resource consumption and so-called anti-virus "storms". (Analysts use the term "storm" to describe a situation where

Symantec Corp.
Symantec Endpoint Protection 12.1
VMware Anti-virus System Performance

Tolly. Certified

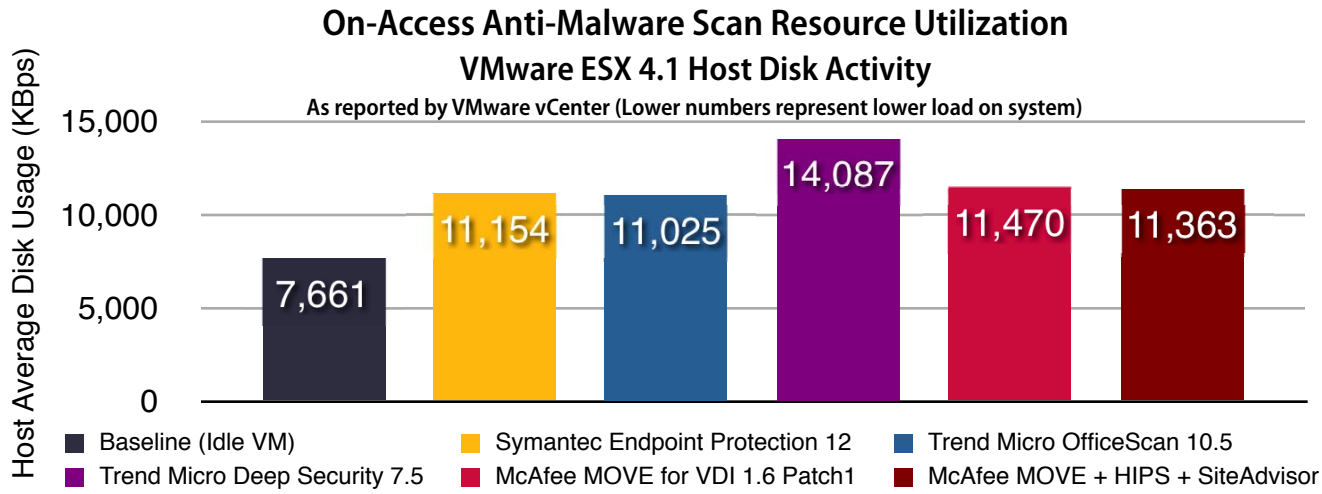
Tested June 2011

On-Demand Anti-Malware Scan Resource Utilization
VMware ESX 4.1 Per-VM CPU and Memory Activity
As reported by VMware vCenter (Lower numbers represent lower load on system)



Note: 1. Windows 7 Enterprise, 64-bit installations. Solutions instructed to scan 50 VMs. Reported results are average of 10 VMs. SEP configured to use shared insight cache to optimize scanning. Trend Office Scan pre-scan templates not used as all 50 VMs were identical and no scanning would take place. Symantec SEP completed the scan in12 - 13 minutes; Trend Micro products required 23 - 24 minutes to complete the scan. McAfee MOVE for VDI does not offer on-demand scanning.
2. Trend Micro Deep Security requires the Deep Security Virtual Appliance (DSVA) to be on the same ESX host as all virtual desktops. The virtual appliance's load is shown adjacent the Deep Security single VM for reference.
Source: Tolly, June 2011

Figure 2



Note: Windows 7, 64-bit installations. Test workload run on 50 VMs. Reported results are average of all VMs. Test engineers noted that, in the McAfee MOVE solution test, the longer the VMs were active prior to commencing the test, the higher the host resource utilization was. This chart represents best McAfee results from 3 tests.

Source: Tolly, June 2011 Figure 3

many virtual machines initiate resource-intensive tasks simultaneously, detracting significantly from the resources available to other virtual machines on the same host.)

Test Results

On-Demand Anti-Malware Scan

For any number of reasons, an IT security administrator may decide to initiate full scans on dozens of clients "on demand". Such tasks can be resource-intensive and, if run simultaneously, place an unacceptable load on the VMware host system and degrade the overall virtualization system performance.

For this test, each system was instructed to run on-demand scans of all 50 VMs. The Trend Micro Deep Security solution and OfficeScan solution automatically serialize the scans to avoid excessive resource consumption. The Symantec solution was configured to initiate all 50 scans within an 8-hour period to avoid excessive resource consumption.

Figures 1 and 2 summarize the results for the Symantec and Trend offerings.[1]

The Symantec system throttles back its demands on disk I/O to approximately 2,700 KBps per second. The two Trend Micro solutions place demands on disk I/O that are 2 and 3 times that of Symantec. Figure 2 illustrates that the processing and memory demands of the Symantec offering are both lower than the comparable Trend Micro solutions.

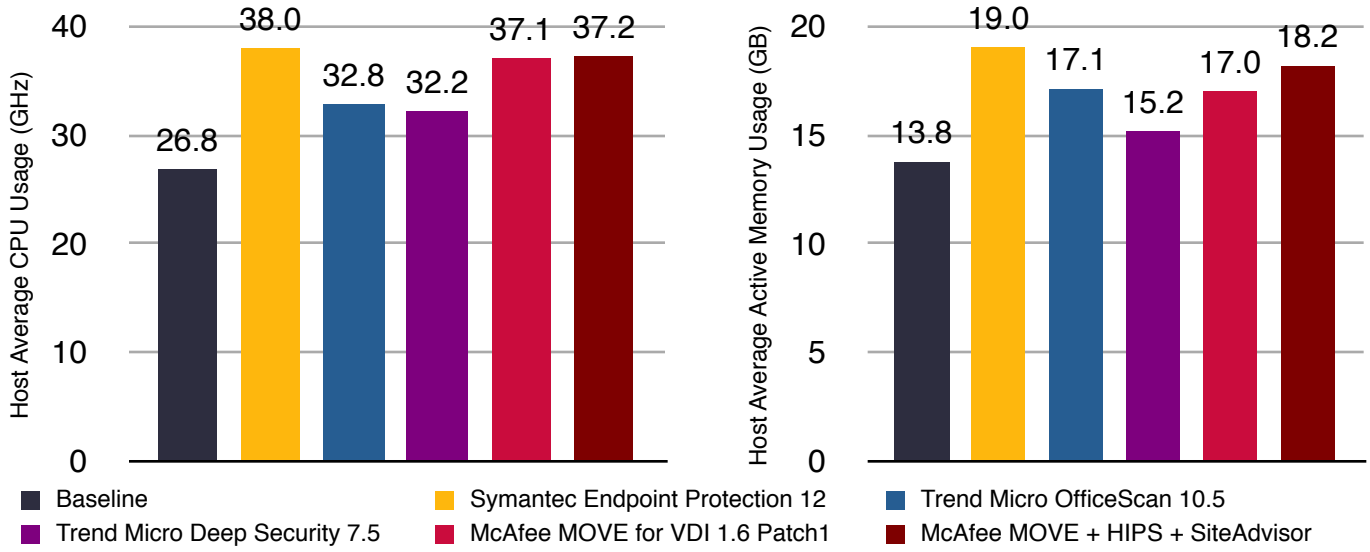
The Trend Micro Deep Security solution consists of two components - the client virtual machine and the Trend Micro Deep Security Virtual Appliance (DSVA) - both of which place demands on system resources.

The processing power and memory usage o f both components are both shown in Figure 2. As the disk I/O activity of the Trend Micro client VM was negligible, it is not included in Figure 1.

It should be noted that the three products tested use different schemes to determine which files will be scanned and, thus, each required differing amounts of time and total disk I/O to complete the scan.

Symantec uses a caching method to avoid re-scanning identical content across virtual machines. Both Symantec Endpoint Protection and Trend Micro OfficeScan provide for a pre-scan template to optimize the scanning. These features were not used due to the use of identical machines to be deployed within the VDI environment, and use of the template would have significantly reduced scanning activities. As the focus of the test is to understand resource consumption on a "per second" basis during the test, the amount of data actually scanned is not of critical concern.

[1] McAfee MOVE for VDI 1.6 does not offer an option for on-demand scanning.



Note: Windows 7, 64-bit installations. Test workload run on 50 VMs. Reported results are average of all VMs. Test engineers noted that, in the McAfee MOVE solution test, the longer the VMs were active prior to commencing the test, the higher the host resource utilization was. This chart represents best McAfee results from 3 tests.

Source: Tolly, June 2011

Figure 4

On-Access Anti-Malware Scan

Throughout the work day, the endpoint security solution is invoked to scan files and other registry/RAM contents as they are accessed.

For this test, a script exercising various Microsoft Office functions was run on all 50 VMs and resources were measured at a VMware host level.

Figures 3 and 4 summarize the results for these tests which included the two McAfee solutions. Engineers noted that the results were quite similar for all of the systems tested.

Where test results for the Symantec and Trend Micro solutions remained consistent when tests were re-run, this was not the case with the McAfee solutions. When the McAfee tests were re-run a day later without a reboot, the resource consumption increased significantly. Only after all virtual desktops running the McAfee solution were rebooted and benchmarked again, did the McAfee solutions deliver the lower resource consumption illustrated in the report figures.

Signature Update

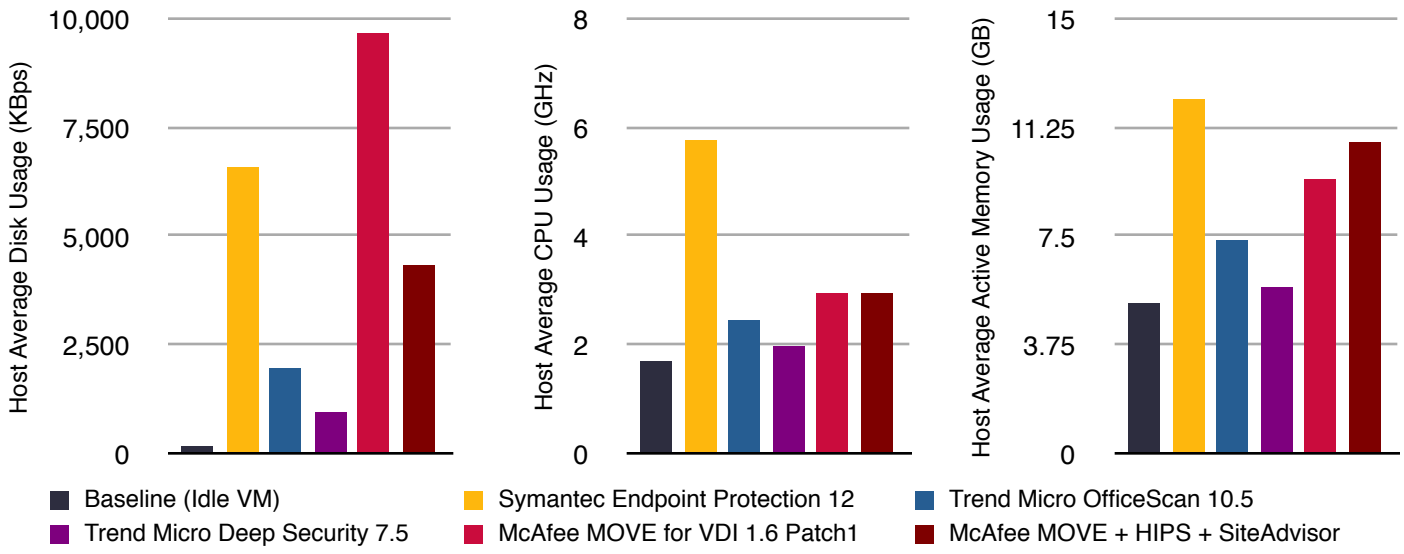
Endpoint security systems periodically retrieve updated information, referred to as "signatures", that assist in effectively identifying and eliminating new threats.

While less resource-intensive than an on-demand scan, IT administrators are rightly concerned with the performance impact on VMware host servers if multiple signature updates are run simultaneously.

McAfee MOVE and Trend Micro Deep Security implement an architecture where a single copy of the file is downloaded to the virtual server. While Symantec and Trend Micro OfficeScan endpoint agents each individually downloaded and performed the signature update, Symantec Endpoint Protection, by default ran an active scan on each VM as part of the definition update process, ensuring that no recently-discovered threats have manifested in the systems.

Tolly engineers verified that Symantec's randomization algorithm effectively distributed the download tasks for the 50 clients across the designated 4-hour window for start time. Tolly engineers measure resource consumption over that period and reported that Symantec's average disk I/O was 6,565 KBps, CPU consumption was 5,750 MHz and memory consumption was 12.2 GB. No "storms" or VMware system degradation was observed. See figure 5 for details.

Virus Definition Update: VMware ESX 4.1 Host Resource Utilization
As reported by vCenter (Lower numbers represent lower load on system)



Note: 1. Symantec Endpoint Protection ran an active scan on each VM as part of the definition update process by default.
2. Different vendors completed the definition updates in different times with different mechanisms. Results shown are average ESX host resource consumption over 4 hours and 15 minutes. Please see report text for details.
3. McAfee MOVE's performance was highly unstable. There were idle time disk usage spikes on each VM which inflated the final results. Test engineers noted that, in the McAfee MOVE solution test, the longer the VMs were powered on prior to commencing the test, the higher the host resource utilization was. This chart represents the best-case McAfee results from 3 test iterations.

Source: Tolly, June 2011 Figure 5

Test Methodology

All tests were conducted using the same hardware infrastructure. All 50 Windows 7 Enterprise (64-bit) virtual machines were deployed using VMware View 4.6 as linked clones. The persistent pool was composed from a template with 1 vCPU, 1GB RAM, and a 30GB thick-provisioned disk.

See Table 1 for a list of all systems under test and see Table 2 for details of the VMware virtual server environment.

On-Demand Anti-Malware Scan

All VMs were in idle status. Symantec Endpoint Protection was scheduled to scan all 50 VMs with random start time within an 8 hours period. Engineers isolated each VM run and averaged that data to generate the Symantec results.

Trend Micro OfficeScan and Deep Security scanned VMs serially and were only able to finish fewer than 25 VMs during the 8 hour and 30 minute test period. So single VM performance was used as the basis for comparison. Trend Micro OfficeScan's "generate Pre-Scan Template" feature was not used nor was the similar Symantec Endpoint Protection feature Virtual Image Exception used. The Trend Micro Virtual Desktop Infrastructure Support plugin was used for Trend Micro OfficeScan to optimize its performance in virtual environment..

McAfee MOVE for VDI only supports on-access scan but not on-demand scan. Thus, results do not include MOVE.

Performance results with 1 minute intervals were exported from VMware Virtual Center.

On-Access Anti-Malware Scan

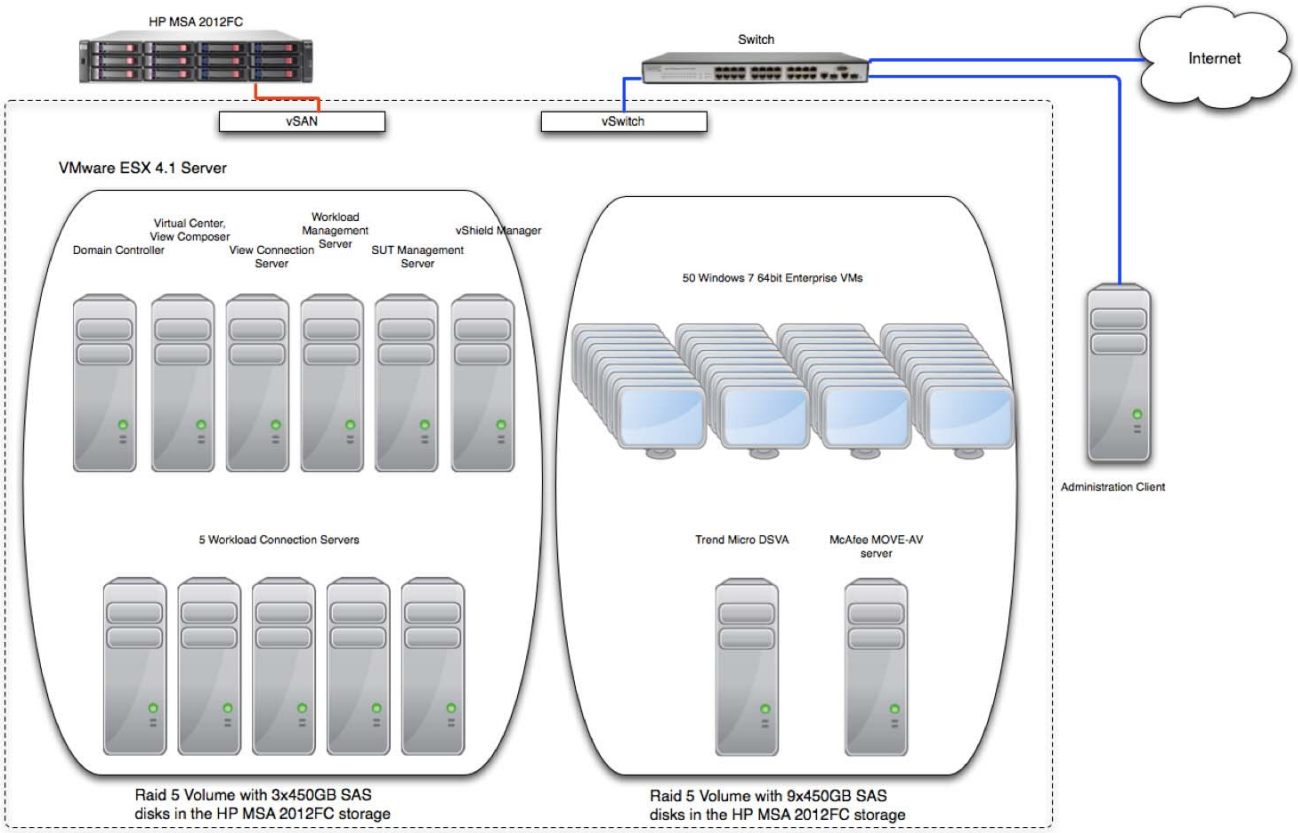
Each VM was running the same workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Adobe Reader and network file transfers. The test duration was 40 minutes.

Real-time performance results with 20 seconds intervals were exported from VMware Virtual Center.

Signature Update

All VMs were in idle status. Symantec Endpoint Protection and Trend Micro OfficeScan were scheduled to update all 50 clients with random start times within a 4

Virtualized Anti-virus Test Environment



Source: Tolly, June 2011

Figure 6

hours period. Trend Micro Deep Security only required updating the Deep Security Virtual Appliance which took 1 to 2 minutes. McAfee MOVE only required updating the MOVE A/V server which took 4 to 5 minutes. The whole test duration was 4 hours and 15 minutes.

Symantec Endpoint Protection ran one active scan on each VM as part of the definition update process by default. The active scan option can be unchecked.

Performance results with 1 minute intervals were exported from VMware Virtual Center.

Test Environment

One HP DL580 server with 4x Intel® Xeon® X7460 processors (6-core, 2.67GHz, 16MB L3 cache) and 128GB RAM was used to host the test environment. One HP MSA2012FC storage with 12x HP MSA2 450GB 3G 15K 3.5 inch SAS HDDs was used to store all VMs. The host and the storage were connected by 4G FC with a 16-port 4Gb SAN switch.

All infrastructure VMs were stored in a RAID 5 volume with three drives. All virtual desktops were stored in another RAID 5 volume with nine drives. The Trend Micro Deep Security Virtual Appliance and McAfee MOVE-AV server were stored in the same volume as all virtual desktops. Please see figure 6 for the test bed diagram.

Some analysts consider the best practice for virtual anti-virus environments is to run infrastructure VMs and virtual desktops on different hosts. Trend Micro Deep Security virtual appliance is required to be on the same VMware host as all virtual desktops.

McAfee MOVE-AV server should be placed on the same host as all virtual desktops according to McAfee's best practices so all test results represented as Host Total in this report are the sum of all 50 virtual desktops' performance plus the Deep Security Virtual Appliance for Deep Security and the MOVE-AV server for McAfee MOVE).

Systems Under Test

Vendor	Product	Components	Implementation
Symantec	Endpoint Protection 12.1	Symantec Endpoint Protection Manager 12.1.601.4699; Symantec Shared Insight Cache 1.0.0.409	Endpoint client with Shared Insight Cache for on-demand scan optimization
Trend Micro, Inc.	Deep Security 7.5	Trend Micro Deep Security Manager version 7.5.6323; Deep Security Virtual Appliance 7.5.0.5534; ESX Filter Driver 7.5.0.5435; Assigned the pre-configured Windows 7 Desktop security profile.	Single virtual appliance. Agentless client communicates via VMware vShield API
Trend Micro, Inc.	OfficeScan 10.5 + IDF	Trend Micro OfficeScan Server 10.5 Build 1093; Trend Micro Virtual Desktop Support 1.0.1023; OfficeScan Intrusion Defense Firewall Client 6.1.69	Endpoint client. VDI plugin on the management server communicates with VMware vCenter
McAfee	MOVE for VDI 1.6 patch 1	McAfee ePolicy Orchestrator 4.6.0 Build 1029; MOVE-AV Extension 1.6.0.153; McAfee Agent for Windows 4.5.0.1852; MOVE AV Agent 1.6.0.1213; MOVE AV Server 1.6.0-1110; VirusScan Enterprise 8.7.0i	Thin agents on client. On access scan is routed to MOVE AV server for all clients. No on-demand scan support
McAfee	MOVE for VDI + HIPS + SiteAdvisor	Components Above; McAfee Host Intrusion Prevention 8.0.0.1741; McAfee SiteAdvisor Enterprise Plus 3.0.0.638	Same as above

Source: Tolly, June 2011 Table 1

VMware Performance Host Testbed Components

Component	Version/Build
VMware ESX	4.1.0 build 348481
VMware vCenter Server	4.1.0 build 258902
VMware View Composer Server	2.6
VMware View Connection Server	4.6.0 build 366101
VMware vShield Manager	4.1 build 310451
Server Hardware	4x Xeon x7460 (Hexacore) running at 2.67GHz with 128 GB of DDR 2 RAM
Storage Area Network	HP StorageWorks MSA connected via 4GB FibreChannel
Guest VM Resources	1GB RAM and 1 vCPU
Guest Operating System	Microsoft Windows 7 Enterprise 64-bit

Source: Tolly, June 2011 Table 2

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
You can reach the company by email at *sales@tolly.com*, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Interaction with Competitors

In accordance with our process for conducting comparative tests, The Tolly Group contacted the competing vendors inviting them to review test methodology and their results prior to publication. McAfee did not respond. Trend Micro declined active participation but provided the following comment when provided results for review: "Trend Micro believes that activating OfficeScan's Base Image Whitelisting feature would have created the same benefits of the SEP12 caching feature(s) in a real world test and deployment."

For more information on the Tolly Fair Testing Charter, visit:
http://www.tolly.com/FTC.aspx

Terms of Usage

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 a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. 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.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. 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. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

211123-tb-9-kt-jt-yy - 17Aug11-VerX