

Symantec Endpoint Protection 12.1

Competitive Anti-virus Performance in VMware vSphere 5 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 (SEP) 12.1 within VMware vSphere 5 virtual environments vs. agentless and agent-based solutions from competing vendors. Specifically, this testing focused on the system resource requirements of each solution when performing on-demand and on-access scanning functions, and during distributed virus definition updates.

continued on next page...

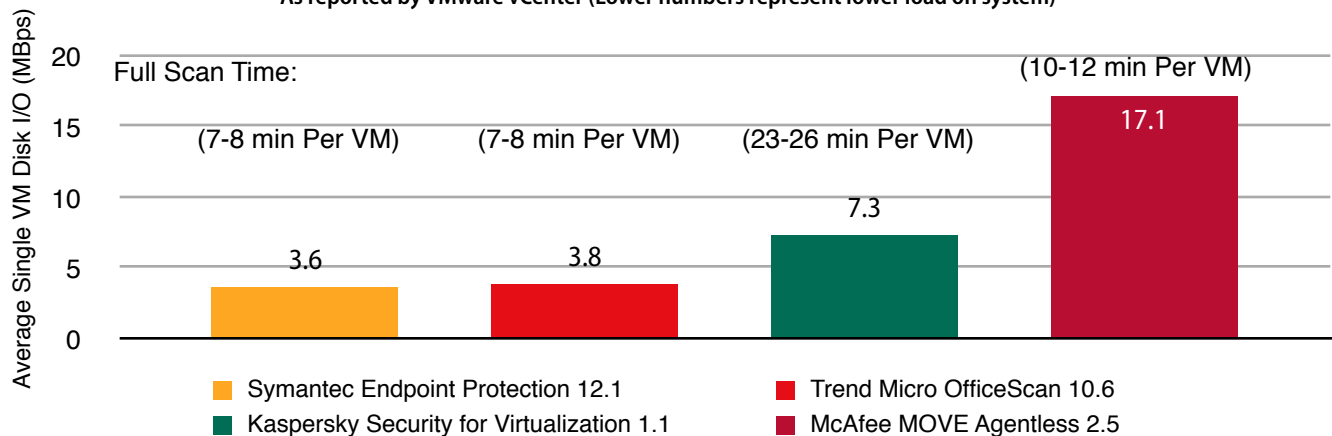
TEST HIGHLIGHTS

Symantec Endpoint Protection 12.1:

- 1 Lowest single-VM disk I/O and memory demand for on-demand scan with fast per-machine run time
- 2 Demonstrates avoidance of anti-virus “storms” through implementation of randomization algorithm for resource-intensive functions

On-Demand Anti-Malware Scan Resource Utilization Average Single Virtual Machine Disk I/O

As reported by VMware vCenter (Lower numbers represent lower load on system)



Notes: 1. Windows 7 Professional, 64-bit. Solutions were scheduled to scan all 50 VMs. Results reported are the time and performance for scanning each VM. 2. SEP network Shared Insight Cache was enabled to optimize scanning. OfficeScan used SmartScan method. OfficeScan's pre-scan template feature and SEP's Virtual Image Exception were not enabled. These two features may further reduce the resource usage for these two solutions. 3. Amount of data scanned across solutions varied due to dynamic data and caching. See report text for details. 4. No A/V storms observed during any test. 5. McAfee MOVE Multi-platform 2.5 does not offer on-demand scan capability.

Source: Tolly, August 2012

Figure 1



Executive Summary (con't)

SEP 12.1 is deployed as an agent running on each virtual desktop system, as is Trend Micro's OfficeScan. Kaspersky Lab's Kaspersky Security for Virtualization and McAfee MOVE Agentless products are implemented as VMware virtual appliances that serve as a central point of processing for security activities and connect to the clients using VMware's vShield Endpoint Agent. McAfee MOVE Multi-platform uses agents on each VM to offload files to an offload scanner for real-time protection.


Testing encompassed various scanning and system update functions and was performed using 50 Microsoft Windows 7

Professional (64-bit) virtual machines. Tolly engineers measured critical system resources such as disk input/output (I/O), CPU consumption and memory usage at both the virtual machine and VMware host level.

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".

Symantec Corp.

Symantec Endpoint Protection 12.1

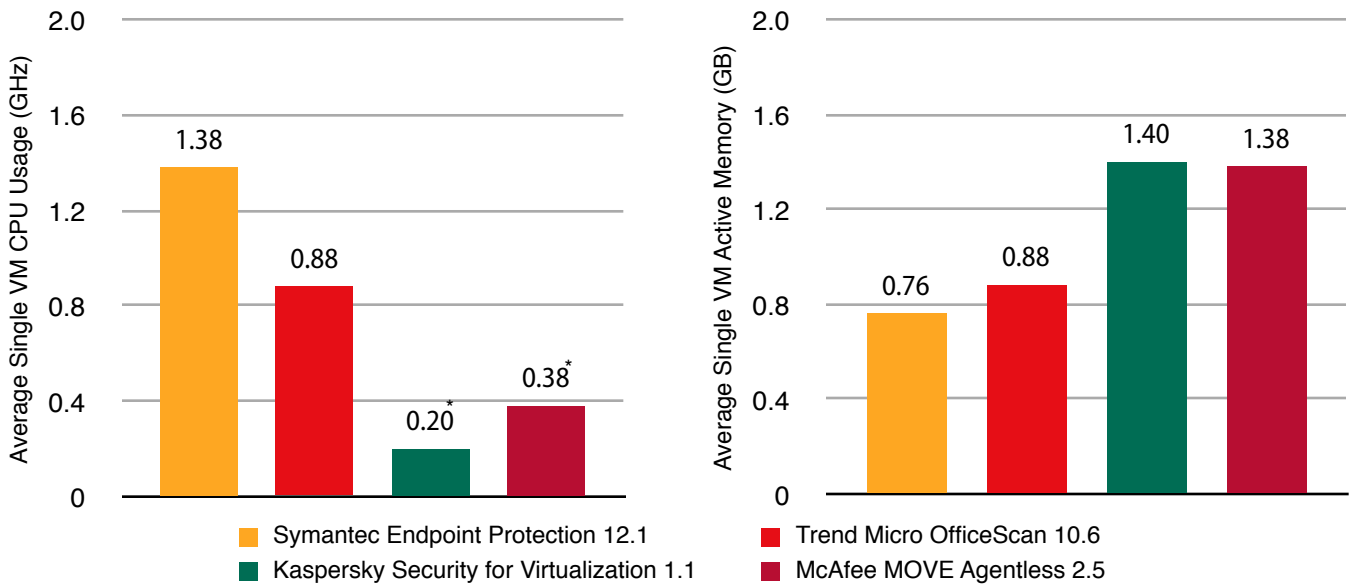


Endpoint Security for Virtualization Performance

Tested August 2012

On-Demand Anti-Malware Scan Resource Utilization Average Single VM CPU and Memory Activity

As reported by VMware vCenter (Lower numbers represent lower load on system)



Notes: *Additional load on the host: Kaspersky's security virtual appliance - 3.97GHz (by default, with 4 concurrent VMs under scan), McAfee MOVE Agentless security virtual appliance - 1.19GHz (by default, with 2 concurrent VMs under scan). SEP and OfficeScan do not require additional virtual appliance on the same host with the virtual desktops.

1. Windows 7 Professional, 64-bit installation. Solutions scheduled to scan all 50VMs. Results reported are the time and performance for scanning each VM. 2. SEP network Shared Insight Cache was enabled to optimize scanning. OfficeScan used SmartScan method. OfficeScan's pre-scan template feature and SEP's Virtual Image Exception were not enabled. These two features may further reduce the resource usage for these two solutions. 3. Amount of data scanned across solutions varied due to dynamic data and caching. See report text for details. 4. No A/V storms observed during any test. 5. McAfee MOVE Multi-platform 2.5 does not offer on-demand scan capability.

Source: Tolly, August 2012

Figure 2



Analysts use the term “storm” to describe a situation where 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 host system, degrading the overall virtualized system performance.

Only SEP allows administrators to configure the time window within which SEP needs to initiate scanning each of the 50 VMs. As other solutions did not provide this option, the run time for this test varied across products.

For SEP, Tolly engineers scheduled the full scan to run in an 8-hour window. All VMs ran the full scan starting at a random time within that window. SEP used Shared Insight Cache to reduce the number of files that needed to be scanned on each VM. The first VM required approximately 25 minutes to run the full scan. The subsequent VMs, leveraging the cache of previously-scanned files, needed only 7 to 8 minutes to complete.

Both vShield-based solutions - McAfee MOVE Agentless and Kaspersky Security for Virtualization - scan VMs serially on a host. By default, McAfee MOVE Agentless scanned 2 concurrent VMs while Kaspersky Security for Virtualization scanned 4 concurrently. Caching was enabled for McAfee MOVE Agentless for all tests. McAfee MOVE Agentless required 10 to 12 minutes to scan each VM while Kaspersky Security for Virtualization required 23 to 26 minutes.

OfficeScan also scans VMs serially with the help of Trend Micro’s VDI plug-in. With the

default scanning method (SmartScan), OfficeScan needed 7 to 8 minutes to complete each scan.

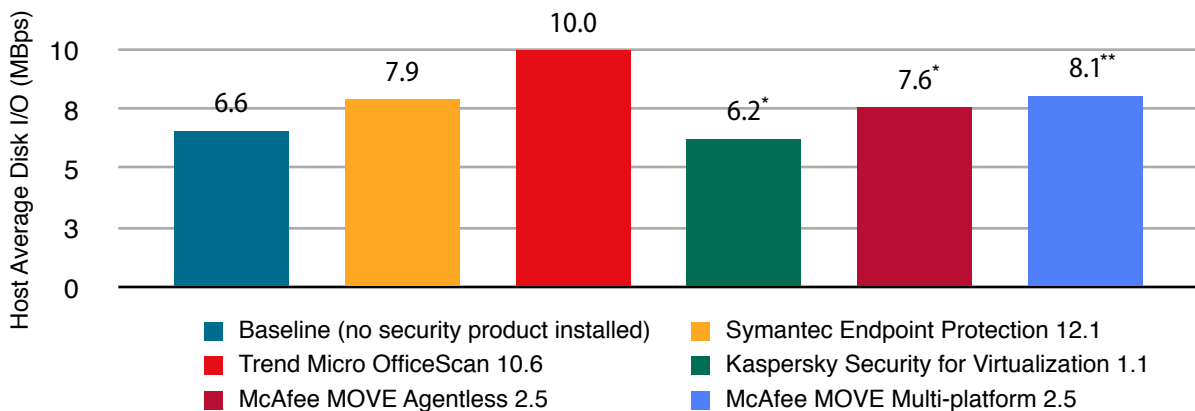
Figures 1 and 2 summarize the results for the competitive offerings supporting the full scan, “on-demand” functionality.

As Symantec leverages a centralized cache server for all clients, it throttles back its demand on disk I/O to approximately 1.7 MBps for repeated scans. The Trend Micro solution also offers comparable performance, whereas the vShield enabled products require an average of 1 to 3.75X more Disk I/O per VM for Kaspersky and McAfee, respectively. See Figure 1.

vShield-enabled solutions consist of two components - the client virtual machine and the Virtual Appliance (VA) - both of which place demands on system resources. This additional overhead was recorded but not factored into the “Per VM” utilization metrics, and is noted in Figure 2.

On-Access Anti-Malware Scan Resource Utilization VMware ESXi 5.0u1 Host Disk Activity

As reported by VMware vCenter (Lower numbers represent lower load on system)



Note: *File transfers took much longer in tests of Kaspersky Security for Virtualization and McAfee MOVE Agentless. So it is possible that not all files finished transferring during the test duration for these two products. See Figure 5 for detail. **For the VMware View environment, vmware\vdms needs to be excluded from scanning in McAfee MOVE Multi-platform solution. Otherwise, the resource usage is unstable.

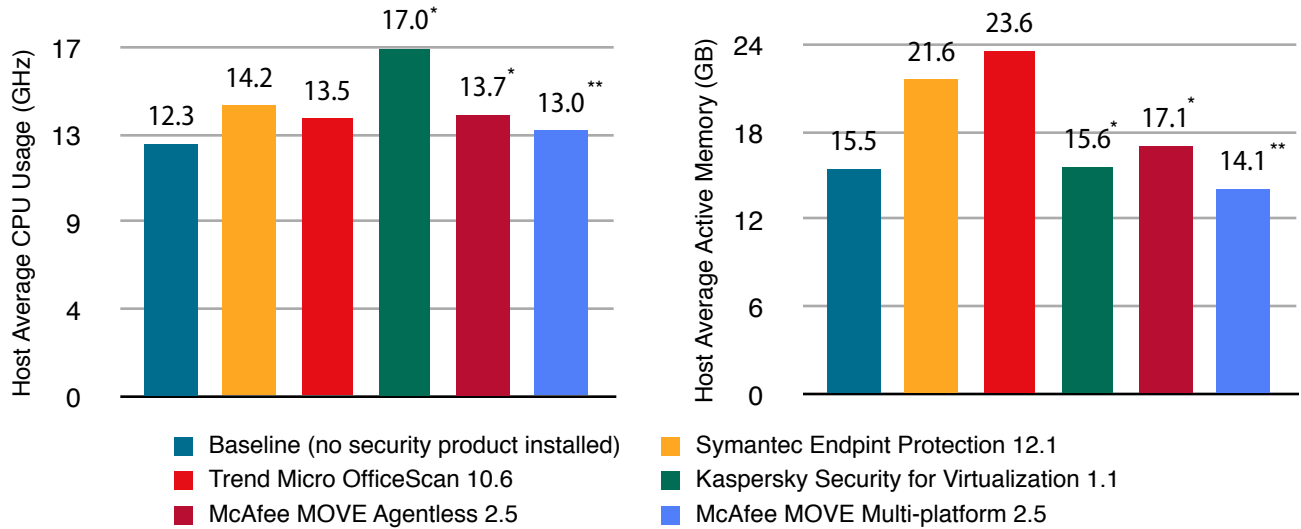
1. Results reported here are for the ESXi host hosting all virtual desktops and the security virtual appliance from Kaspersky Security for Virtualization and McAfee MOVE Agentless. 3. Windows 7, 64-bit installation. 50 VMs were running the same workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Adobe Reader and network file transfers.

Source: Tolly, August 2012

Figure 3

On-Access Anti-Malware Scan Resource Utilization VMware ESXi 5.0u1 Host CPU and Memory Activity

As reported by vCenter (Lower numbers represent lower load on system)



Note: *File transfers took much longer in tests of Kaspersky Security for Virtualization and McAfee MOVE Agentless. It is possible that not all files finished transferring during the test duration for these two products. See Figure 5 for detail. **For VMware View environment, vmware/vdm needs to be excluded from scanning in McAfee MOVE Multi-platform solution. Otherwise, the resource usage is unstable.

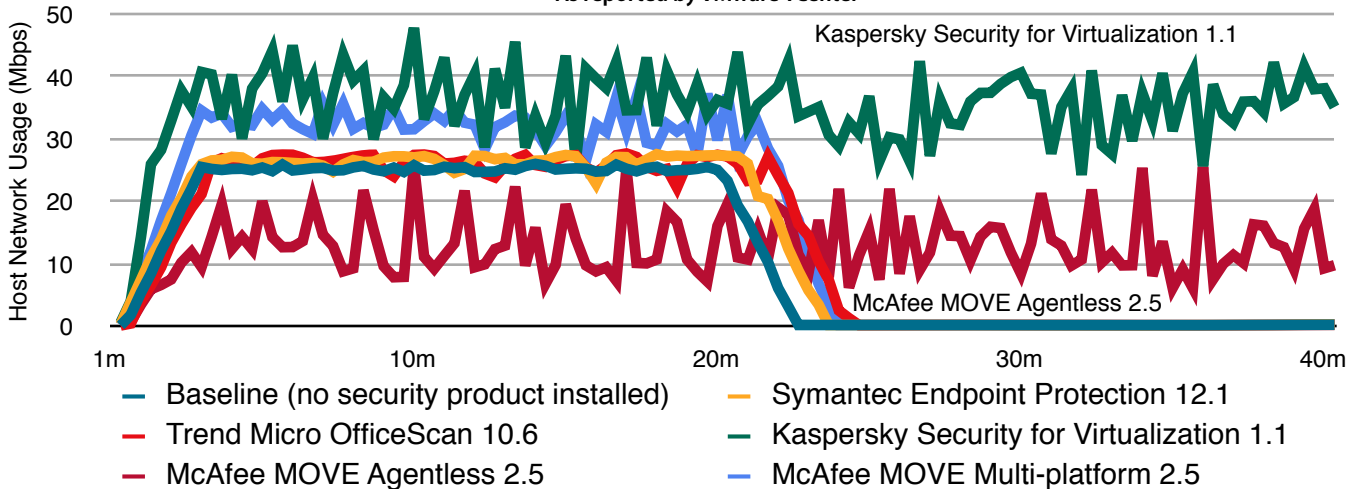
1. Results reported here are for the ESXi host hosting all virtual desktops and the security virtual appliance from Kaspersky Security for Virtualization and McAfee MOVE Agentless. 3. Windows 7, 64-bit installation. 50 VMs were running the same workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Adobe Reader and network file transfers.

Source: Tolly, August 2012

Figure 4

On-Access Anti-Malware Scan Resource Utilization VMware ESXi 5.0u1 Host Network Activity

As reported by VMware vCenter



Note: File transfers ran much longer in tests of Kaspersky Security for Virtualization and McAfee MOVE Agentless than in tests of agent-based solutions. The figure illustrates that agent-based solutions completed the transfer in approximately 20 min where Kaspersky and McAfee MOVE agentless show continued host network activity.

Source: Tolly, August 2012

Figure 5



On Access Anti-Malware Scan

Throughout a typical work day, an endpoint security solution is invoked to scan files and other registry/RAM contents as they are accessed. This test attempted to mirror that type of usage.

For this test, a script exercising various Microsoft Office functions and network file transfers was run on all 50 VMs. The user activities were constant over the entire test duration, whereas the file transfers were introduced for the first 20 minutes of the test. Resources were measured at the VMware host level.

At 7.9 MBps for host average disk usage, Tolly engineers found SEP 12.1 only added 1.3 MBps to the baseline measurement.

As shown in Figure 5, the file transfers for Kaspersky and McAfee Agentless solutions did not complete during the 40-minute test window and, instead, loaded the network for the entire test duration, leading to

slightly lower activity than other solutions. This behavior may have been related to the way that the virtual appliances process the files.

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.

Symantec Endpoint Protection and Trend Micro OfficeScan require updating endpoint agents on each VM. They were scheduled to update all 50 clients with random start times within a 4-hour period. Because of the centralized, agentless architecture of Kaspersky Security for Virtualization and

McAfee MOVE Agentless, these solutions only required updating the security virtual appliance, which took less than 5 minutes. McAfee MOVE Multi-platform only required updating the offload scan server which was not on the same physical host as all virtual desktops, and therefore no performance impact was measured on the host. See Figure 6.

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 had 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 measured resource consumption over that period and reported that Symantec's average disk I/O was 5.0 MBps, CPU consumption was 1.91 GHz and memory

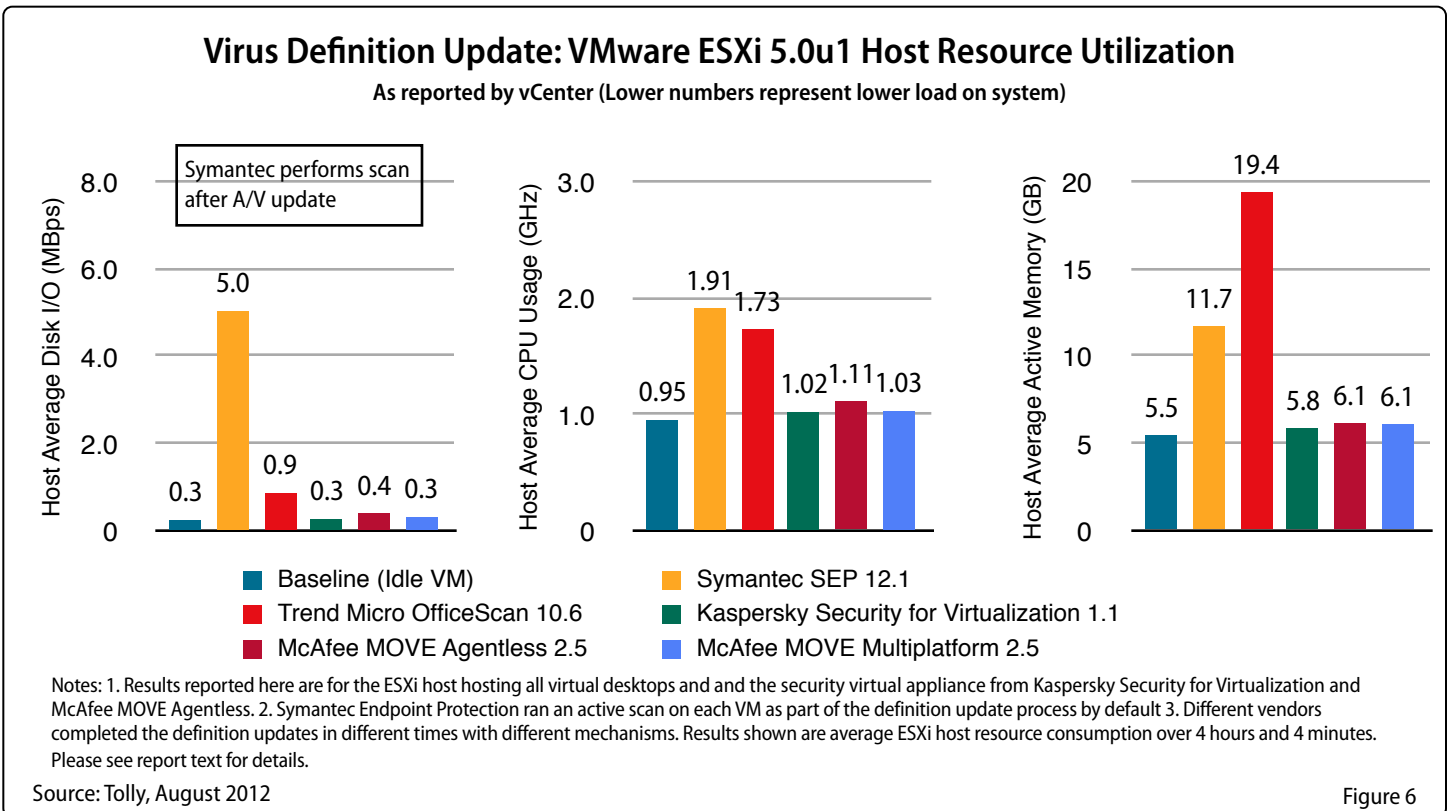
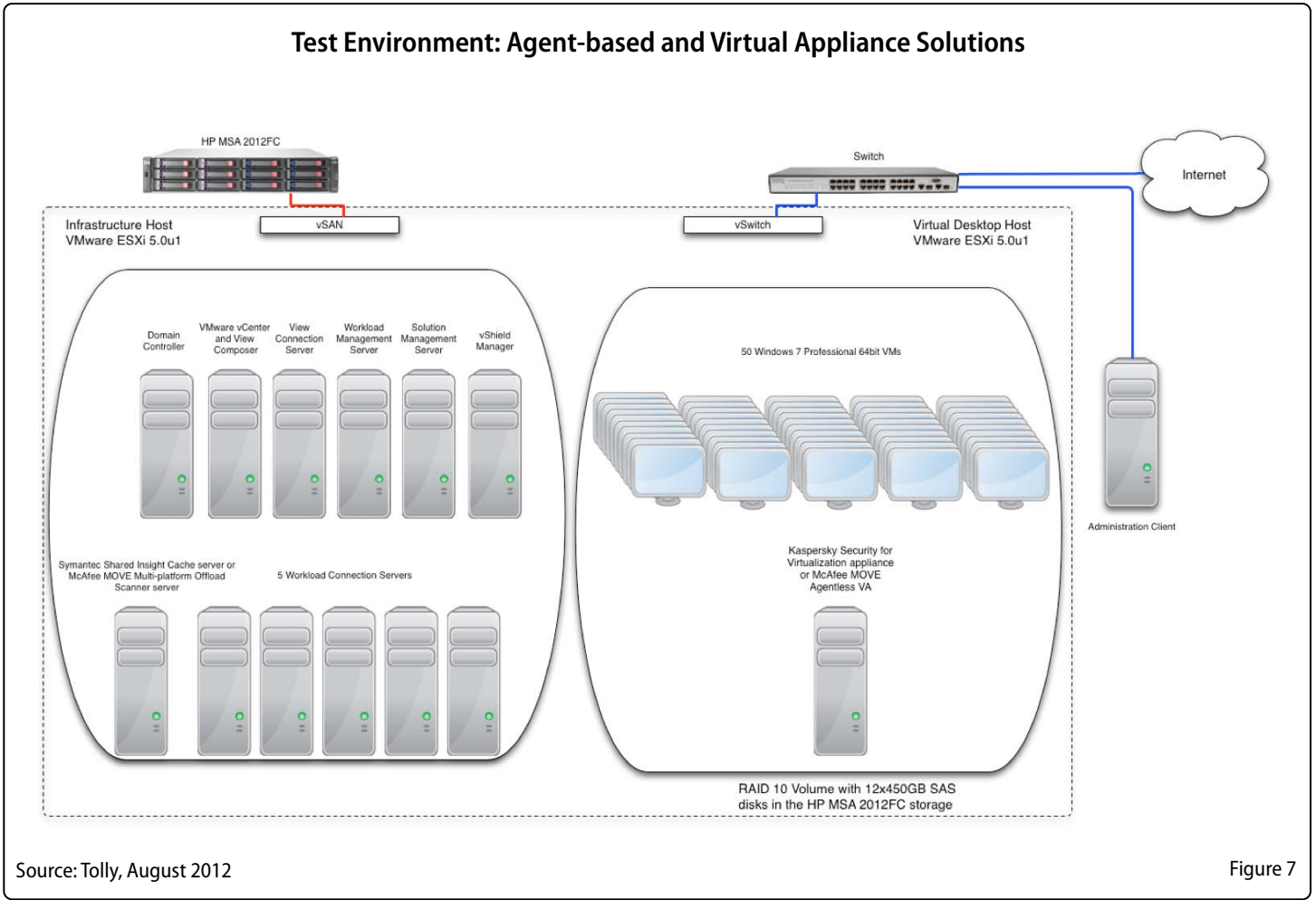


Figure 6



consumption was 11.65 GB. Despite consuming slightly more host resources, no “storms” or VMware system degradation were observed on the host. See Figure 6 for details.

Test Methodology

All 50 Windows 7 Professional (64-bit) virtual machines were deployed using VMware View 5.0 as linked clones. The persistent pool was composed from a golden image with 1 vCPU, 2GB RAM, and a 30 GB thick-provisioned disk.

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

In the Symantec Endpoint Protection test, the managed SEP client was installed on the golden image first. Then the image was left connected to the Internet for more than 3 hours to allow the reputation to seed.

Then “SMC -stop” was run from the run line, deleting all copies of the Hardware Key config XML file sephwid.xml, removing the HardwareID, ComputerID and HostGUID under “HKLM\Software\Symantec\Symantec Endpoint Protection\SMC\Sylink\Sylink\” to allow Symantec Endpoint Protection Manager to see each cloned image as a unique client when they reconnect. The Virtual Image Exception feature was not enabled for SEP which is the default configuration.

SEP supports network Shared Insight Cache (SIC) and vShield based virtual Shared Insight Cache. Tolly engineers used network SIC for testing.

For Trend Micro OfficeScan, the VDI plug-in was installed to optimize performance. The pre-scan template feature, which is similar to SEP’s Virtual Image Exception feature was not used. A Trend Micro provided tool was used to remove the UUID from the systems as to deploy and register properly in a VDI environment.

In the McAfee MOVE Multi-platform test, as suggested by McAfee, policy enforcement interval was set to 60 minutes. Additionally, per McAfee’s request, the directory “vmware\vdm” was added to exclusion for real time scanning due to unstable performance.



The default configuration was used for both Kaspersky Security for Virtualization and McAfee MOVE Agentless solutions.

On-Demand Anti-Malware Scan

All VMs were booted and idle for at least an hour prior to testing. Before the first on-demand test, 489.6 MB of files were pre-populated to each client. 244.8 MB of those files were the same on each client and the other 244.8 MB files were unique to each client. Between each run/iteration, Tolly engineers changed 163.2 MB files for each client. 81.6 MB of those files were the same for all clients and 81.6 MB files were unique to each client. There was an update test run before each on-demand scan test.


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, and Adobe Reader applications, with network file transfers in the background.

A batch file was used to transfer files in each VM. The script does the following task:
 ping 127.0.0.1 for 20 seconds --> transfer 10 MB of files from a file server to the VM --> ping 127.0.0.1 for 20 seconds --> transfers 10 MB of files from the VM to the file server --> repeat.

The script ran for 30 iterations. The files transferred included a 1 MB docx file, a 1 MB pdf file, a 1 MB pptx file, a 1 MB xls file, a 1 MB zip file, another 3 pdf files, another ppt file, another doc file and one VMware-vShield-Endpoint-Driver-1.0. msi file.



The test methodology used for this report relies upon test procedures, metrics and documentation practices as defined in Tolly Common Test Plan #1105: Anti-Virus Endpoint Performance in Virtual Environments. For more information, please go to:
<http://CommonTestPlan.org>

Systems Under Test

Vendor	Product	Components	Implementation
Symantec Corp.	Endpoint Protection 12.1	Symantec Endpoint Protection Manager 12.1.1959.1959; Symantec Shared Insight Cache 12.1.1959.1959	Endpoint client with Shared Insight Cache for on-demand scan optimization
Trend Micro, Inc	OfficeScan 10.6	OfficeScan 10.6.1062 VDI plug-in	Endpoint client with VDI plug-in for on-demand scan optimization
Kaspersky Lab	Kaspersky Security for Virtualization 1.1	Kaspersky Security Center 9.2.69 Kaspersky Security for Virtualization (ksv appliance) 1.1.0.54	Single virtual appliance. Agentless client communicates via VMware vShield API
McAfee, Inc	MOVE Agentless 2.5	McAfee ePolicy Orchestrator 4.6.2 (Build: 234) [McAfee move-sva: McAfee MOVE AV Agentless 2.5.0.228 McAfee VirusScan Enterprise for Linux 1.7.0 McAfee Agent for Linux 4.6.0.2156]	Single virtual appliance. Agentless client communicates via VMware vShield API
McAfee, Inc	MOVE Multi-platform 2.5	McAfee ePolicy Orchestrator 4.6.2 (Build: 234) McAfee Agent 4.5 McAfee MOVE AntiVirus [Multi-Platform] 2.5.0.164 McAfee VirusScan Enterprise 8.8.8.0.777	McAfee agent and MOVE agent on each VM. Files are offloaded to the Offload Scanner server for real-time scan.

Source: Tolly, August 2012

Table 1

To emulate a real-world environment, 5 MB of files were unique to each user for each iteration, 4 MB were unique to a iteration, but common across all users, and 1 MB was common across all test iterations and all users.

The test duration was 40 minutes. Real-time performance results with 20 second granularity were exported from VMware Virtual Center over the test duration.

Signature Update

All VMs were in idle state prior to testing. The entire test duration was 4 hours and 4 minutes. Solutions were configured to schedule updates as per their respective best practices. Performance results with 1

minute intervals were exported from VMware Virtual Center.

Test Environment

One HP DL380G7 server with 2x Intel® Xeon® X5680 processors (6-core, 3.33GHz) and 128GB RAM was used to host the VDI 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 an 16-port 4Gb SAN switch.

All virtual desktops were stored in a RAID 10 volume with 12 drives. The vShield virtual appliances were stored in the same volume as all virtual desktops. Please see Figure 7 for the test bed diagram.

Symantec SEP12.1

To learn more about SEP 12.1, go to the Symantec website by scanning the code below.



VMware Performance Host Testbed Components

Component	Version/Build
VMware ESXi	5.0.0, 623869
VMware vCenter Server	5.0.0, 455964
VMware View Composer Server	2.7.0, 481620
VMware View Connection Server	5.0., 481677
VMware vShield Manager	5.0, 473791
Server Hardware	2x Xeon x5680 (Hex-core) running at 3.33GHz with 128 GB of DDR3 RAM
Storage Area Network	HP StorageWorks MSA connected via 4GB FibreChannel
Guest VM Resources	2GB RAM and 1 vCPU, 30 GB Thick Provisioned Disk
Guest Operating System	Microsoft Windows 7 Professional 64-bit

Source: Tolly, August 2012

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. Tolly followed all suggestions for testing. All vendors except Trend Micro responded and were provided with the test methodology as well as their individual results prior to publication. McAfee and Kaspersky reviewed the test plan and offered configuration recommendations. McAfee reviewed the results and asked questions which we answered. We did not hear back from Kaspersky after receiving their results.

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.