

# Symantec Endpoint Protection 12.1 vs. Trend Micro Deep Security 8

## 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. Trend Micro Deep Security (DS) 8. 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...*

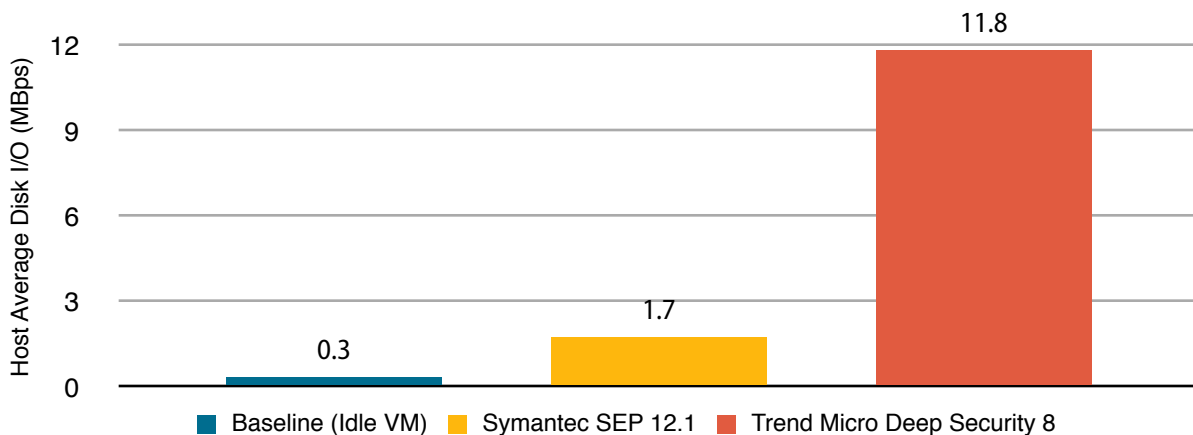
### TEST HIGHLIGHTS

Symantec Endpoint Protection 12.1:

- 1 Uses 86% less disk bandwidth and 37% less CPU when performing on-demand scanning compared to Trend Micro Deep Security 8
- 2 Uses 21% less disk bandwidth and 36% less CPU during on-access scanning when compared to Trend Micro Deep Security 8

### On-Demand Anti-Malware Scan Resource Utilization VMware ESXi 5.0u1 Host Disk I/O

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



Notes: 1. ESXi 5u1 host results reported, includes all virtual desktops and the DSV. 2. Windows 7 Professional, 64-bit VMs. Solutions instructed to scan 50 VMs. 163.2MB of unique data introduced to each VM between each test. See the test methodology section for full details. 3. SEP Shared Insight Cache configured to optimize scanning. The initial post-deployment SEP scan averaged 2.9 MBps of I/O per VM, subsequent on-demand scans averaged 1.7MBps, as reported above. 4. DS8 took 17-18 min to finish scanning each VM. For SEP, the first two VMs in each test iteration required 16-21 min, and 6-8 min for subsequent VMs. Amount of data scanned across solutions varied due to dynamic data and caching. See report text for details. No A/V storms observed during any test. 5. Test duration (14h16m) determined by maximum time needed for DS8 to serially scan 50 VMs. SEP set to randomize scans over 14 hours.

Source: Tolly, April 2012

Figure 1



### Executive Summary (con't)

SEP 12.1 is deployed as an agent running on each virtual desktop system. Trend Micro's Deep Security 8 is implemented as a VMware virtual appliance (DSVA) that serves as a central point of processing for security activities, connecting to the clients using VMware's vShield Endpoint Agent.


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

**Symantec, Corp.**

**Symantec Endpoint Protection 12.1**

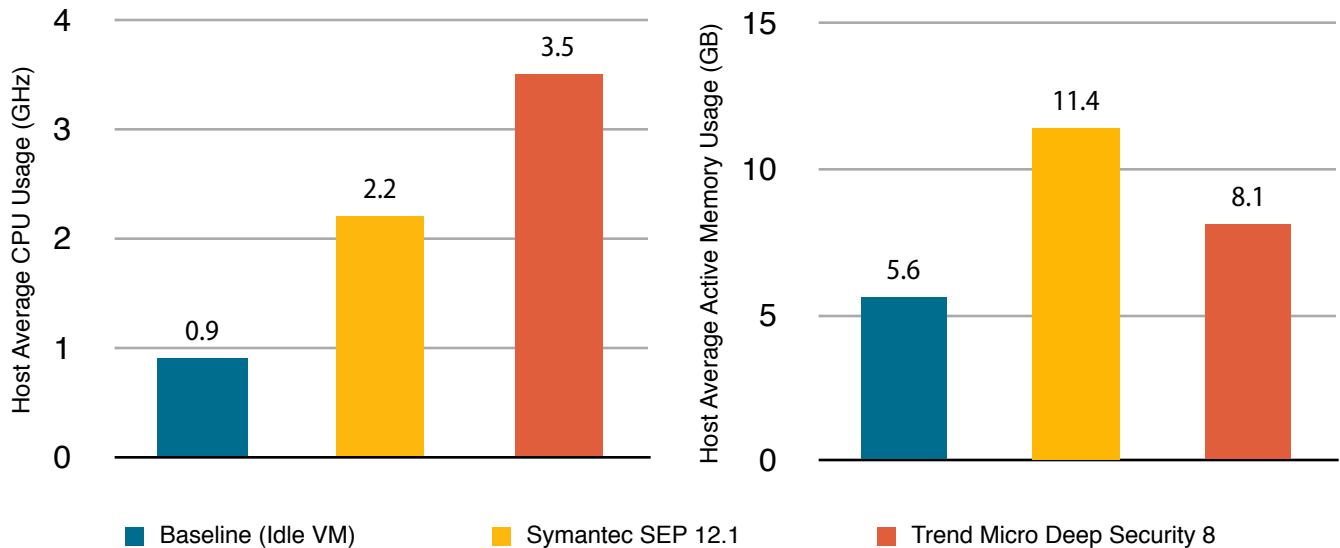


**Endpoint Security for Virtualization Performance**

*Tested April 2012*

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

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



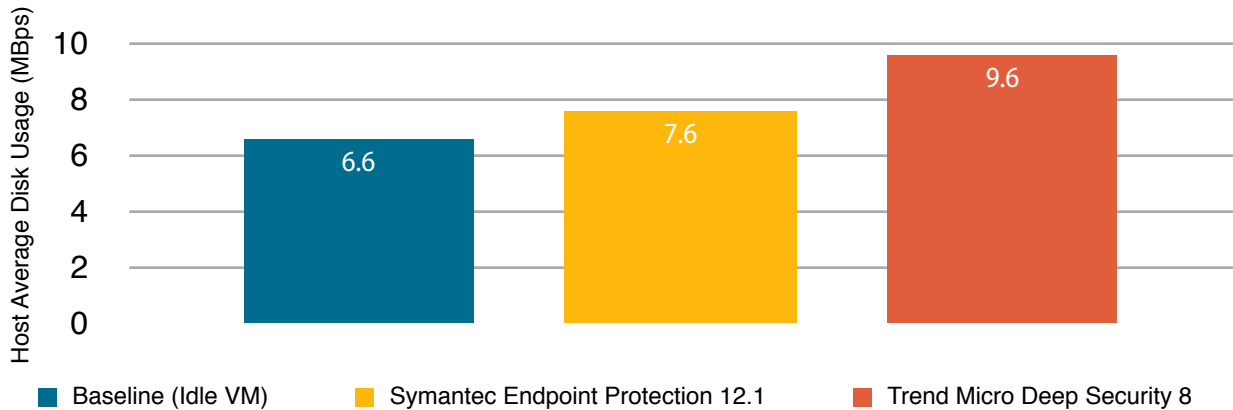
Notes: 1. ESXi 5u1 host results reported, includes all virtual desktops and the DSVA. 2. Windows 7 Professional, 64-bit VMs. Solutions instructed to scan 50 VMs. 163.2MB of unique data introduced to each VM between each test. See the test methodology section for full details. 3. SEP Shared Insight Cache configured to optimize scanning. 4. DS8 took 17-18 min to finish scanning each VM, for SEP, the first two VMs in each test iteration required 16-21 min, and 6-8 min for subsequent VMs. Amount of data scanned across solutions varied due to dynamic data and caching. See report text for details. No A/V storms observed during any test. 5. Test duration (14h16m) determined by maximum time needed for DS8 to serially scan 50 VMs. SEP set to randomize scans over 14 hours.

Source: Tolly, April 2012

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: Results reported here are for the ESXi host hosting all virtual desktops and the Deep Security Virtual Appliance. Windows 7, 64-bit installations. 50 VMs were running the same workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Adobe Reader and network file transfers.

Source: Tolly, April 2012

Figure 3

## 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.

For this test, each system was instructed to run on-demand scans of all 50 VMs. The Trend Micro Deep Security solution automatically serializes the scans to avoid excessive resource consumption. Deep Security finished the full scan for 50 VMs in 13 hours 49 minutes, 14 hours 16 minutes and 14 hours 5 minutes in three tests. Tolly engineers used the maximum run, 14 hours 16 minutes as the test duration.

The Symantec solution was configured to randomize all 50 scans within an 14-hour period in order to avoid excessive resource consumption.

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

The average host disk I/O for the first post-deployment SEP on-demand scan test was 2.9 MBps. As Symantec offers caching, it throttles back its demand on disk I/O to approximately 1.7 MBps for subsequent tests. The Trend Micro solution places demands on disk I/O that are over 6 times that of Symantec. See Figure 1.

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.

Tolly engineers found that Trend Micro Deep Security uses 59% more CPU for an on-demand scan than Symantec SEP 12.1.

The processing power and memory usage of both solutions are shown in Figure 2.

It should be noted that the two 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 Endpoint Protection 12.1 uses Shared Insight Cache to reduce the amount of scanned data. It also offers a feature to bypass scanning all files on the base image, which is not enabled by default and Tolly engineers did not enable it for any test. This feature would have further reduced the scanning activities for SEP.

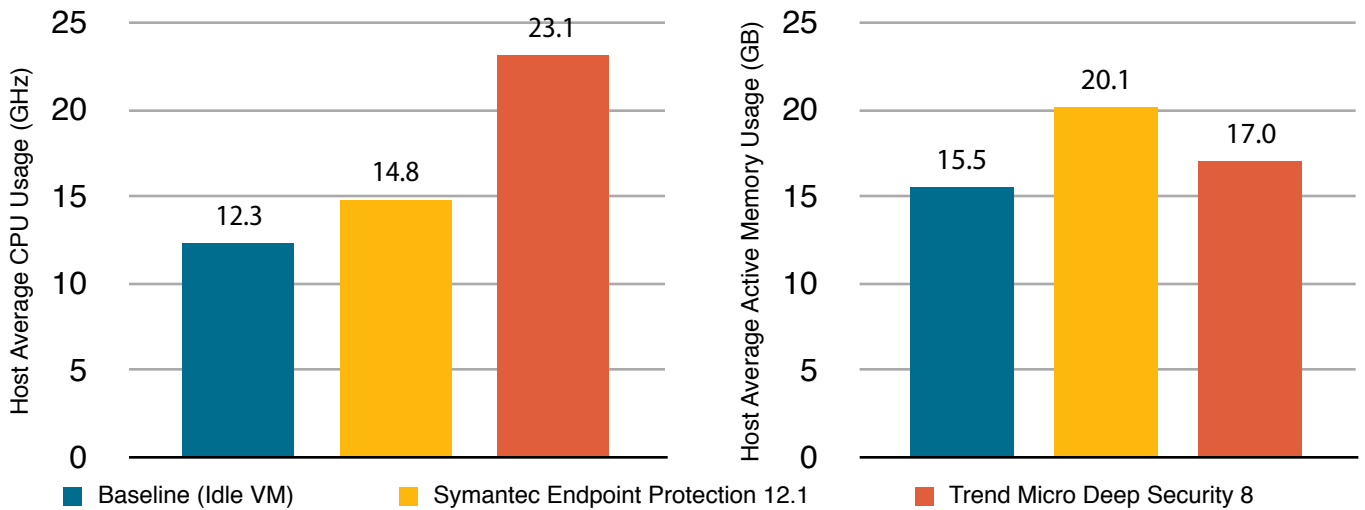
To ensure no VM would be completely cached, Tolly engineers changed 163.2 MB of dynamic files on each VM before each on-demand test iteration. Please see the test methodology section for details.

### 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.

### 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: Results reported here are for the ESXi host hosting all virtual desktops and the Deep Security Virtual Appliance. Windows 7, 64-bit installations. 50 VMs were running the same workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Adobe Reader and network file transfers.

Source: Tolly, April 2012

Figure 4

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

At 7.6MBps for host average disk usage, Tolly engineers found SEP 12.1 only added 1MBps to the baseline measurement, compared to an added 3MBps for Trend Micro. See Figure 3.

Because files need to be queued for the Deep Security Virtual Appliance to scan, the file transfer time was longer compared to SEP 12.1.

Symantec SEP 12.1 also used less CPU (GHz) than Trend Micro Deep Security 8. At 14.8GHz, Symantec used ~35% less CPU than Trend Micro, on average. In order to keep the CPU usage for the Deep Security Virtual Appliance lower than 75% on average, 6 vCPUs were assigned to it. See Figure 4.

### 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.

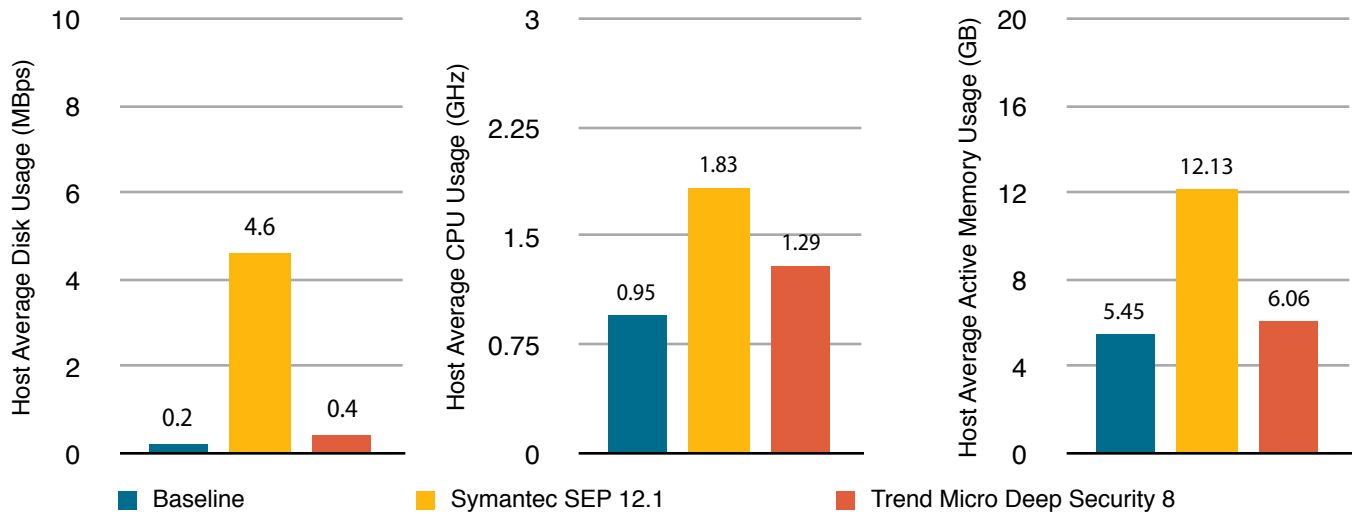
Trend Micro Deep Security implements an architecture where a single copy of the file is downloaded to the virtual appliance. While Symantec endpoint agents each individually downloaded and performed the signature update, Symantec Endpoint Protection, by default, ran an active scan on each VM as part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

Trend Micro Deep Security finished the signature update in 5 minutes with minor impact on the host. See Figure 5.

Tolly engineers verified that Symantec’s randomization algorithm effectively distributed the download tasks for the 50 clients across the designated 4-hour and 15-minute window for start time. Tolly engineers measured resource consumption over that period and reported that Symantec’s average disk I/O was 4.6 MBps, CPU consumption was 1.83 GHz and memory consumption was 12.23 GB. No “storms” or VMware system degradation was observed. See Figure 5 for details.

### Virus Definition Update: VMware ESXi 5.0u1 Host Resource Utilization

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



Notes: 1. Results reported here are for the ESXi host hosting all virtual desktops and the Deep Security Virtual Appliance. 2. Symantec Endpoint Protection ran an active scan on each VM as part of the definition update process by default 3. Different vendors completed the definition updates in different times with different mechanisms. Results shown are average ESXi host resource consumption over 4 hours and 15 minutes. Please see report text for details.

Source: Tolly, April 2012

Figure 5

## 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 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 environment.

In the Deep Security test, as suggested by Trend Micro, the Anti-Malware profile was used for all 50 VMs and the CPU usage for manual scan and scheduled scan was set to high in the Deep Security policy. The default configuration for the Deep Security Virtual Appliance uses 2 vCPUs. However, the CPU usage was at 100% for nearly the entire on access test duration. Tolly engineers increased this to 6 vCPUs to make sure the average DSWA CPU usage was below 75%, as recommended by Trend Micro.

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 the Symantec Virtual Image Exception tool was used with the command "vietool.exe c: --hash" to hash the files on the disk to prepare the system for the first scan. Then "SMC -stop" was run from the run line, delete all copies of the Hardware Key config XML file sephwid.xml, remove 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 bypass scanning of base image files feature was not enabled for SEP by default.

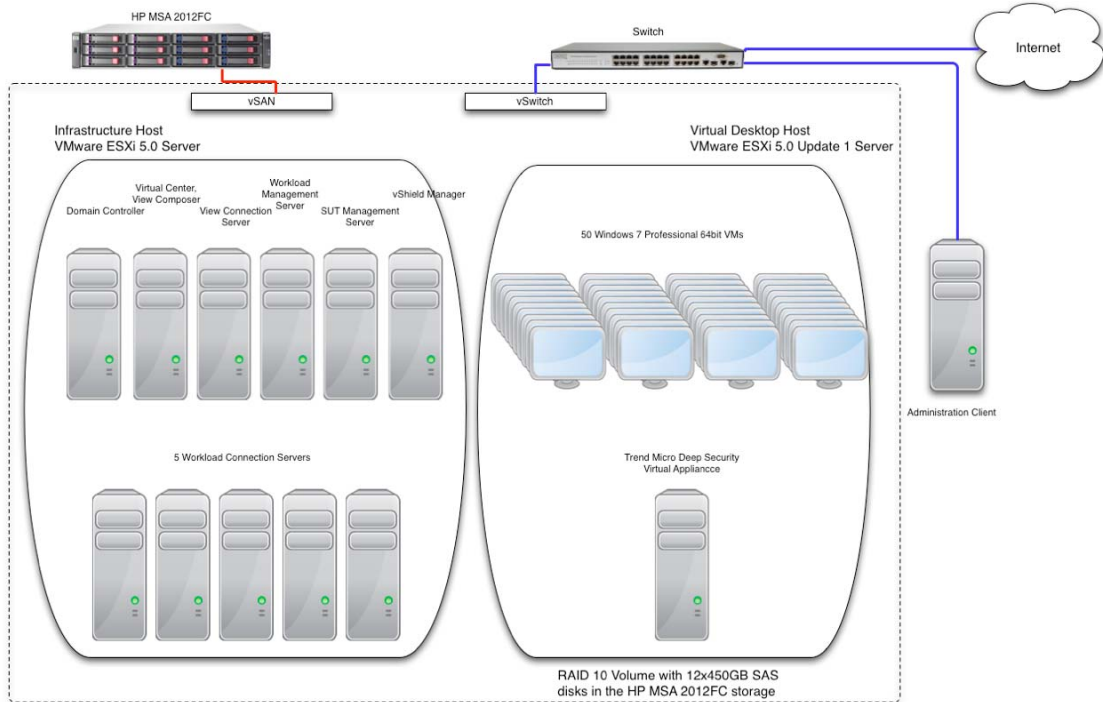
## On-Demand Anti-Malware Scan

All VMs were in an idle state. The test duration (14 hours and 16 mins) was determined by the maximum time that Deep Security used to finish scanning all 50 VMs.

Before the first on-demand test, 489.6MB of files were pre-populated to each client. 244.8MB of those files were the same on each client and the other 244.8MB 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.

Symantec Endpoint Protection was scheduled to scan all 50 VMs with random start times inside a 14 hour window, based on the test duration determined by Deep Security.

### Test Environment: Virtual Desktops and the Deep Security Virtual Appliance



Source: Tolly, April 2012

Figure 6

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 10MB of files from a file server to the VM --> ping 127.0.0.1 for 20 seconds --> transfers 10MB of files from the VM to the file server --> repeat.

The script ran for 25 iterations. The files transferred included a 1MB docx file, a 1MB pdf file, a 1MB pptx file, a 1MB xls file, a 1MB zip file, another 3 pdf files, another ppt file,

another doc file and one VMware-vShield-Endpoint-Driver-1.0. msi file.

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 state. Symantec Endpoint Protection was scheduled to update all 50 clients with random start times within a 4-hour period. Trend Micro Deep Security only required updating the Deep Security Virtual Appliance, which took less than 5 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.

The whole test duration was 4 hours and 15 minutes. 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 a 16-port 4Gb SAN switch.

All virtual desktops were stored in a RAID 10 volume with 12 drives. The Trend Micro Deep Security Virtual Appliance was stored in the same volume as all virtual desktops. Please see Figure 6 for the test bed diagram.

### Systems Under Test

Vendor	Product	Components	Implementation
Symantec, Corp.	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 8	Trend Micro Deep Security Manager version 8.0.1448; Deep Security Virtual Appliance 8.0.0,1199; ESX Filter Driver 8.0.0,1189; Assigned the pre-configured Windows Anti-Malware security profile	Single virtual appliance. Agentless client communicates via VMware vShield API

Source: Tolly, April 2012

Table 1



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

### 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, April 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](mailto: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 vendor, inviting them to review test methodology and their results prior to publication. Trend Micro responded to our request with the following suggestions: To use the Windows Anti-Malware profiles for the virtual desktops, to change the CPU settings for the manual and scheduled scan policies to HIGH, to increase the number of vCPUs for the DSWA to keep the CPU usage under 75%. Tolly followed all suggestions for testing.

Tolly provided results to Trend Micro and VMware and received no further comments or response prior to publication.

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.