#213132
August 2013
Commissioned by
Kaspersky Lab

Kaspersky Security for Virtualization v2.0

Competitive Anti-virus Performance and Effectiveness in VMware vSphere 5.1 Virtual Environments

Executive Summary

In virtual environments, anti-virus (A/V) solutions can be implemented as a client-based agent, whereby all security processing takes place on the client, a virtual appliance that handles the A/V workload- or some hybrid of the two. As more users of virtual infrastructures begin to understand the advantages of virtualization-specific security solutions over traditional agent-based approaches, leading vendors have begun to take note, adding such virtualization-specific products to their portfolios. Efficient resource usage with minimal impact on the host and virtual infrastructure, specifically, are the primary benefits of using a solution optimized for a virtual environment.

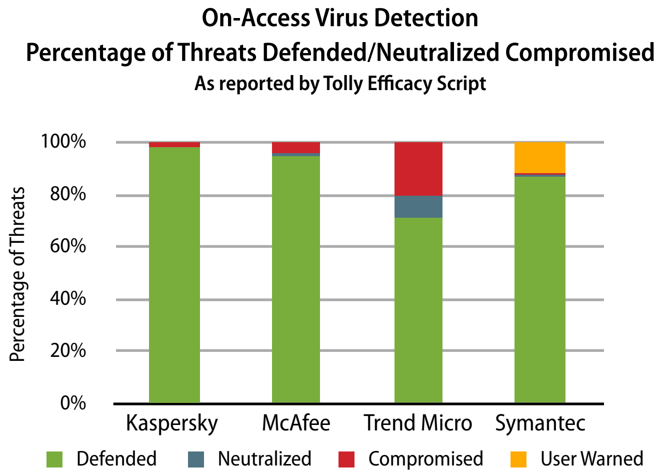
Kaspersky Lab commissioned Tolly to benchmark the performance and effectiveness of its new, agentless Security for Virtualization v2.0 offering in VMware vSphere 5 virtual environments vs. agentless Trend Micro Deep Security 8 SP2 and McAfee MOVE Agentless Security 2.6 and agent-based Symantec SEP 12.1.2.

Tolly found that Kaspersky Security for Virtualization 2.0 blends efficient hypervisor resource usage with solid protection abilities by delivering lower average response times and disk usage than the other products tested. Kaspersky also defended against threats better than the the other agentless offerings under test. See Figure 1 and Table 1.

TEST HIGHLIGHTS

Kaspersky Security for Virtualization v2.0 demonstrates:

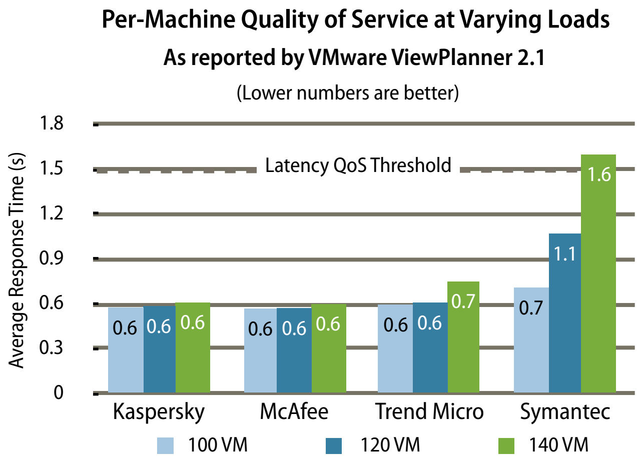
1. Significantly better Quality of Service when scaling than the Symantec agent-based solution
2. Lower disk consumption leading to improved consolidation ratios compared to the Symantec agent-based solution
3. Significantly lower scan times in repeated on-demand scans than other agentless solutions under test
4. Higher malware detection rate than other agentless solutions under test



Notes: Test samples gathered 5/16/2013. Verified malware list sourced from virussign.com. "User Warned" denotes a popup generated by Symantec warning about the file, the user is allowed to override and execute the file.

Source: Tolly, May 2013

Figure 1



Notes: VMware View Planner 2.1 standard workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Outlook, Media Player, Adobe Reader, Firefox and 7-zip applications. One definition update task was scheduled to run during the test.

Source: Tolly, May 2013

Figure 2

Executive Summary (Con't)

Agentless systems leverage VMware's vShield Endpoint to centralize endpoint security processing on a virtual appliance and eliminate the need for installing endpoint security software on each virtual client. The Symantec solution provides endpoint security using client-side processing and leverages the virtual environment through use of a cache shared among the virtual machines.

AV Scan Effectiveness and Performance

In an on-access test of 498 new malware samples, the Kaspersky solution had the highest virus detection rate of the agentless solutions and only 1.2% lower than Symantec.

Kaspersky implements caching to accelerate execution of on-demand scans across multiple virtual machines. A cache built during an initial on-demand scan of 10 test VMs reduces the run time from 101 minutes to scan all ten initially to a mere 7 minutes on a second scan of the same 10 VMs.

While McAfee completes its initial scan of the same machines in 60 minutes, the subsequent scan is reduced by only 10% and takes 54 minutes. Trend Micro requires 223 minutes - over 3.5 hours - to complete the scans the first and subsequent times[1] . See Figure 5.

Endpoint Security Scalability

The performance benefit of agentless security becomes more readily apparent when running many virtual machines simultaneously.

Where all of the solutions tested deliver a per-machine, average response time of less than a second running the test load on 100 VMs simultaneously, the response time of the agent-based Symantec solution is double that of Kaspersky at 120 VMs and triple that of Kaspersy at 140 VMs.

Greater resource efficiency of the Kaspersky agentless solution can help users scale to supporting a greater number of users before requiring additional VMware hosts. See Figure 2.

Test Results

Effectiveness

On-Access Virus Detection

To demonstrate the effectiveness of each solution, Tolly subjected each solution to a corpus of malware samples from VirusSign using Tolly's custom script. Upon accessing

Kaspersky Lab

Security for Virtualization v2.0

Endpoint Security for Virtualization Performance & Effectiveness

Tolly. Certified

Tested May 2013

On-Access Virus Detection

498 Threats as Identified by VirusSign
As reported by Tolly Efficacy Script

	Defended	Neutralized	Warned	Compromised	Defended / Neutralized Warned (%)
Kaspersky	489	0	N/A	9	98.2%
McAfee MOVE Agentless	471	6	N/A	21	95.6%
Symantec	432	4	59*	3	99.4%
Trend Micro	354	42	N/A	102	79.5%

Notes: Test samples gathered 2013-05-16. Verified malware list sourced from virussign.com.
*Symantec "Warned" suggested that users delete the file, but the user was allowed to override and execute.

Source: Tolly, May 2013

Table 1

[1] Symantec's implementation provides for random run time within a user specified execution window, thus it was not appropriate to include a run time for Symantec on this test.

the files, the endpoint security systems would either defend against the threat, neutralize the threat, simply warn the users or compromise the system with no notification.

Kasperksy defended against most threats, permitting only 1.8% of threats to compromise the system, compared to 4.2% for McAfee, 20% for Trend Micro and 0.6% of threats permitted for Symantec. See Figure 1 and Table 1.

On-Access False Positive

At times, blocking legitimate applications or files can be as disruptive as allowing corrupted Esxtop files to run, thus as part of the efficacy tests, engineers evaluated each solutions' ability to detect false positives.

All solutions under test detected 100% of the false positives.

Quality of Service

Quality of Service factors heavily into the overall experience of a product. Users find any application latency due to an endpoint security solution to be frustrating and annoying.

To simulate how each solution handles everyday demands, Tolly engineers used VMware View Planner 2.1 standard workload with common programs installed (Microsoft Word, Excel, PowerPoint, Internet Explorer, Outlook, Media Player, Adobe Reader, Firefox and 7-zip applications), and measured the time to execute different tasks, such as opening word files, browsing .pdf files, completing Excel sheets, etc. This test was repeated and scaled to simulate 100, 120 and 140 VMs.

Average Response Time

Tolly engineers measured the time needed to execute these tasks. A VM response time that climbs above one second can impact user productivity especially when compounded by other delay in the delivery path to the user.

Both Kaspersky and McAfee averaged 0.6 seconds to respond to basic workplace tasks and commands for 100, 120 and 140 VMs.

Trend Micro averaged similarly, at 0.6 for 100 and 120 VMs and .7 seconds for 140 VMs. Symantec's latency was comparable at 0.7 seconds for 100 VMs, but jumped to 1.1 seconds of latency for 120 VMs and 1.6 seconds for 140 VMs. See Figure 2.

Physical Disk Usage

Though the time to complete tasks is an indicator of how much disk is being utilized, Tolly wanted to demonstrate the actual impact on the system and its performance. While running the Quality of Service latency tests with the View Planner workload, Tolly engineers used esxtop batch mode to capture performance counters for the ESXi hypervisor.

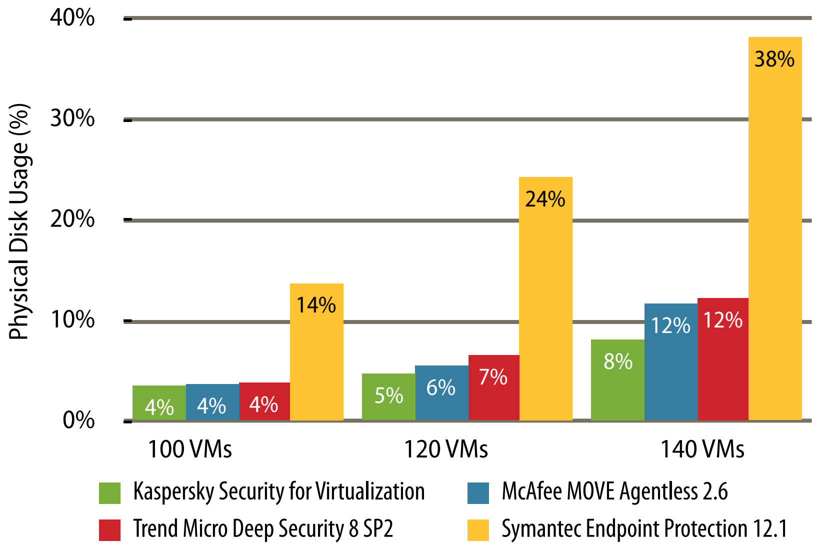
Kaspersky demonstrated consistently low physical disk usage at 4% for 100 VMs, 5% for 120 VMs and 8% for 140 VMs. Both McAfee and Trend Micro used 4% for 100 VMs, but disk usage increased to 6% and 7%, respectively for 120 VMs, and up to 12% for both McAfee and Trend at 140 VMs. See Figure 3.

Symantec used, comparatively, a very high percentage of physical disk compared to the other three products under test. Symantec used 14% for 100 VMs, 24% for 120 VMs and 38% for 140 VMs. See Figure 3.

Disk Usage in the Quality of Service Test

As reported by VMware Esxtop

(Lower numbers are better)



Notes: Esxtop was run with batch mode to capture the Physical Disk SCSI Device\% Used counter. VMware View Planner 2.1 standard workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Outlook, Media Player, Adobe Reader, Firefox and 7-zip applications. One definition update task was scheduled to run during the test.

Source: Tolly, May 2013

Figure 3

Performance

On-Demand Anti-Malware Scan Time

A key component of any endpoint security solution is to perform scheduled system scans. These scans often take up a great deal of system resource, so users are hesitant to run them, thus compromising the overall security of their system. Kaspersky implements caching technology which optimizes this process for virtual environments.

Tolly engineers ran this test twice, in order to demonstrate each solutions ability, or inability to shorten subsequent scan times via caching.

For the first run, Kaspersky took 101 minutes, McAfee took 60 minutes, and Trend Micro took 223 minutes. For the second scan, Kaspersky's time was reduced to 7 minutes, while McAfee remained comparable to its' first run scan time at 54 minutes. Trend Micro's time is the same for the second run as the first at 223 minutes. See Figure 4.

Tolly engineers scheduled a full scan task for each SUT to scan 10 VMs. All agentless solutions under test scanned VMs serially with default settings. Symantec's settings to run this test had to be manually overseen, so they were not deemed comparable to the other results gathered from automated scans. Tolly engineers recorded the total duration to finish scanning 10 VMs from each SUT's management console.

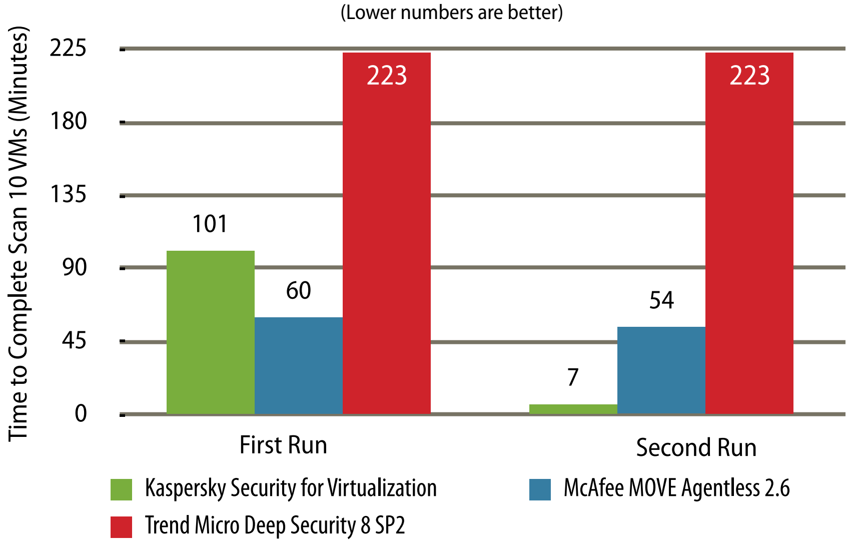
On-Demand Scan Physical Disk Usage

The same process was used to measure the physical disk usage during the scheduled full scan. Kaspersky demonstrated the lowest disk usage for both the first and second scans, at 0.555% and 0.007%, respectively. McAfee used 0.9% and 0.1%,, respectively, Trend Micro used 1.1% for both

On-Demand Scan Time for First and Subsequent Runs

As reported by Solution Consoles to Scan 10 VMs

(Lower numbers are better)



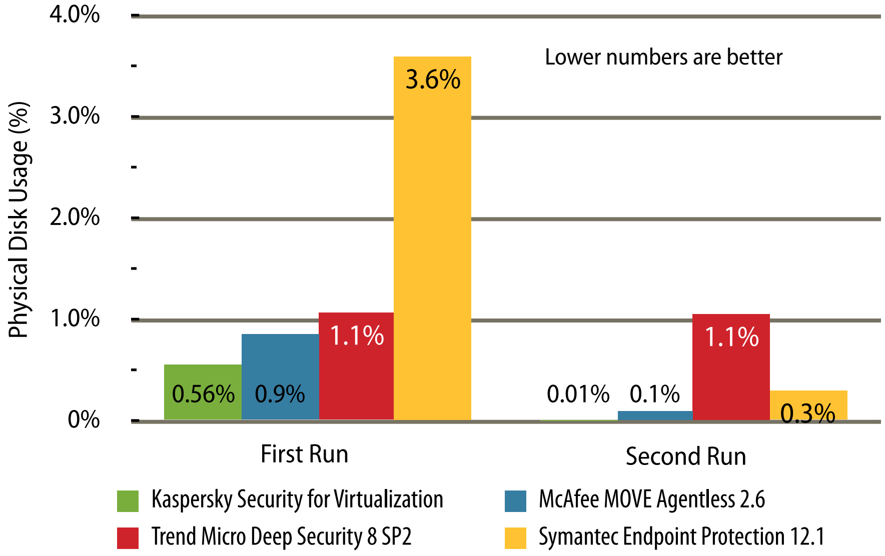
Notes: No background workload running during the test. SUTs were all scheduled to full scan 10 VMs with default settings. Symantec's total scan duration for 10VMs need to be manually specified. and is thus not included in this test.

Source: Tolly, May 2013

Figure 4

Average Physical Disk Usage for First and Subsequent On Demand Scans for 10 VMs

As reported by VMware Esxtop



Notes: No background workload running during the test. SUTs were all scheduled to full scan 10 VMs with default settings. SEP used 2 hour randomization window. Results were averaged for 4 hours based-on the longest scan duration (Trend Micro Deep Security 8 SP2). Esxtop was run with batch mode to capture the physical disk SCSI Device\% Used counter.

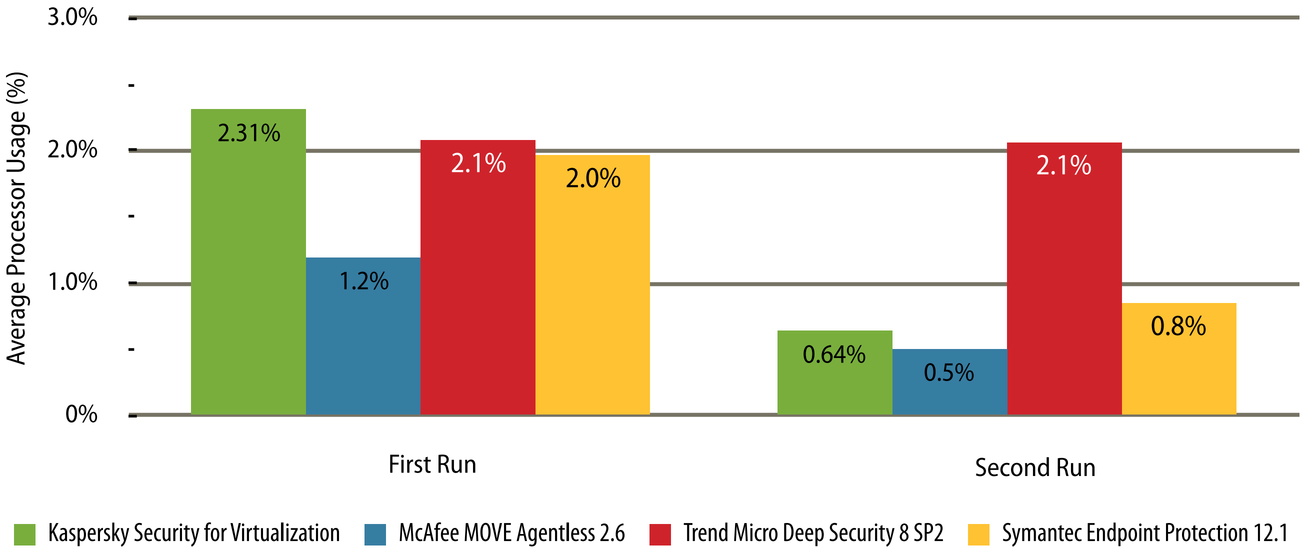
Source: Tolly, May 2013

Figure 5

Average Processor Usage for First and Subsequent On-Demand Scans for 10 VMS

As reported by VMware Esxtop

(Lower numbers are better)



Notes: No background workload running during the test. SUTs were all scheduled to full scan 10 VMs with default settings. SEP used 2 hour randomization window. Results were averaged for 4 hours based-on the longest scan duration (Trend Micro Deep Security 8 SP2). Esxtop was run with batch mode to capture the Physical CPU(_Total)\% Processor Time counter.

Source: Tolly, May 2013

Figure 6

runs, and Symantec used 3.6% for the first run and .3% for the second. See Figure 5.

While running the on-demand scan test, Tolly engineers used Esxtop batch mode to capture the performance of the ESXi hypervisor. As the longest scan duration is about 4 hours (with Trend Micro Deep Security 8 SP2), the average results for 4 hours were used for comparison.

On-Demand Scan Average Processor Usage

As a further benchmark for system usage, Tolly engineers measured the average processor usage for a first and second scan. Kaspersky used 2.31% for its first run, and 64% for the second. McAfee used 1.2% for the first run and 0.5% for the second run. Trend Micro used 2.1% for both runs, while Symantec used 2% for the first run and 0.8% for the second. See Figure 6.

Test Methodology

140 Windows 7 Enterprise (64-bit) virtual machines were deployed as linked clones with VMware ESXi 5.1.0-838463 hypervisor. The Windows 7 gold image was prepared according to VMware View Planner best practices. See Table 2 for a list of all systems under test and see Figure 7 for details of the VMware virtual environment.

Effectiveness

Test samples gathered 5/16/2013. Verified malware list sourced from virussign.com.

The script enabled each client VM to boot up from a fresh (clean) image, snapshot its file system and running processes, and proceed to download and execute a sample from the file server.

The director script kept track of which samples had already been downloaded for a particular iteration and test corpus. Each time a VM booted up, it checked in with this application and was assigned a file to download.

The workload script was created using AutoIT, leveraging the IE_Create functionality to download the samples. Using process and file system snapshots taken immediately after the download, the script determines whether or not the file has been successfully downloaded to the system. If the file exists, the VM is instructed to execute it, followed by another file and process snapshot to determine if the file was allowed to run. This, compared with registry/autorun snapshots and screenshots of the UI at different times provides the basis for the results.

Using this data, the script determines at what stage each of the samples was allowed and where it was detected and defended by the software, reporting this information to the director.

After a full run-through of the client workload, the client writes all its data back to a shared file server, and performs a logoff.

A separate controller is leveraged to perform the VM image refreshes. When one VM logs off and reports that it has finished executing, it writes to a separate networks share which is continually monitored. Each VM writes a unique tagged file to the share, which then prompts the session logoff and reboot. This deletes the VM state and clones out a fresh base disk from which to boot for the next iteration.

Each sample iteration required approximately ten minutes, with all VMs randomized to avoid excessive resource consumption. Each sample was run through at least three different VMs to ensure accuracy.

Quality-of-Service

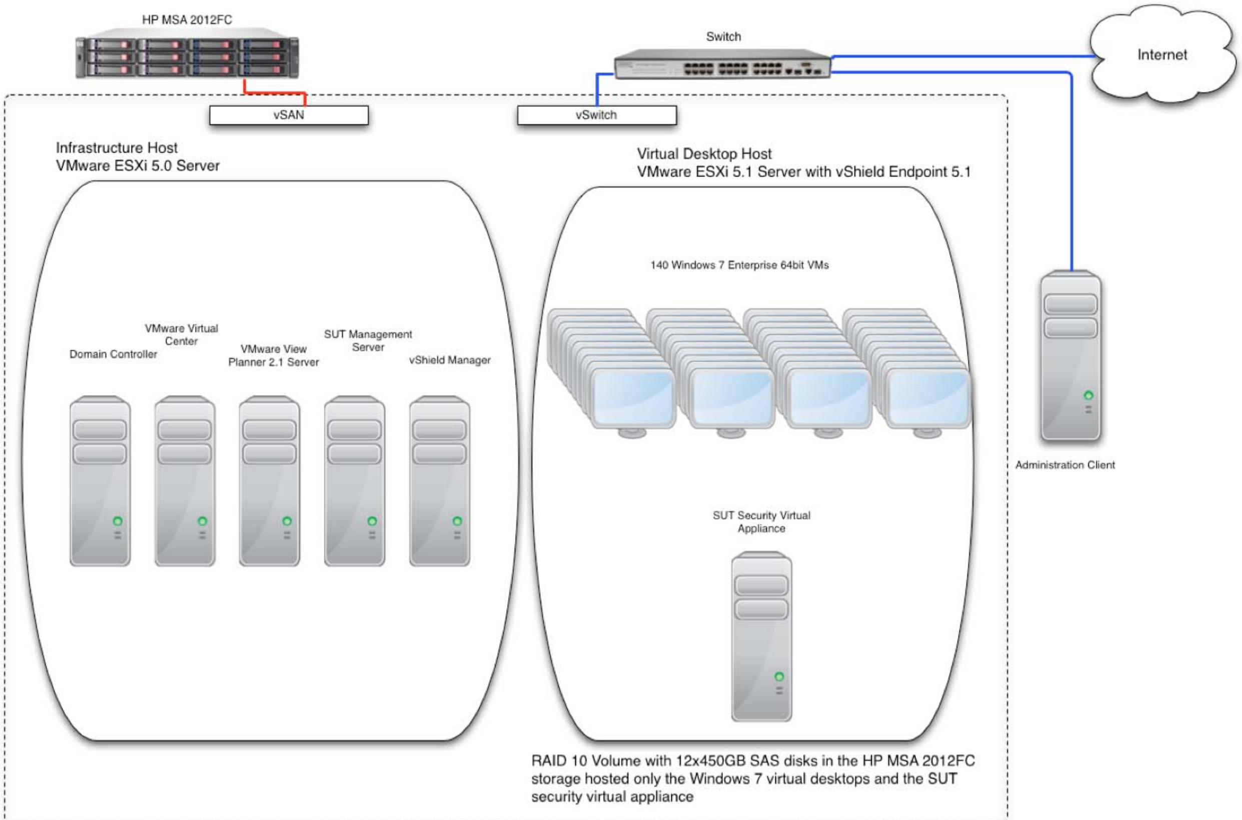
Tolly engineers used VMware View Planner 2.1 standard workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Outlook, Media Player, Adobe Reader, Firefox and 7-zip applications to test the user quality of service. View Planner reports the time to execute different tasks like opening word files, browsing pdf files, filling in Excel sheets, etc. Tolly engineers then used the results to compare the user experience with different security products installed.

On-Demand Anti-Malware Scan

10 Windows 7 VMs were powered on for the On-demand scan test to evaluate the time required to scan each VM with different solutions.

Kaspersky, Trend Micro and McAfee solutions are agentless solutions. By default, Kaspersky Security for Virtualization 2.0 and Trend Micro Deep Security 8 SP2 scan VMs serially. McAfee MOVE Agentless 2.6 also scan VMs in serial but with two VMs at a time by default. Symantec Endpoint Security 12.1.2 were configured to scan VMs randomly in a 2 hours period. Symantec Endpoint Protection supports additional features like Virtual Image Exception (VIE) which can avoid scanning files from the gold image. The purpose of this test is to evaluate

Test Environment - vShield-based Endpoint Protection Solutions


HP MSA 2012FC
Switch
Internet
vSAN
vSwitch
Infrastructure Host
VMware ESXi 5.0 Server
Virtual Desktop Host
VMware ESXi 5.1 Server with vShield Endpoint 5.1
140 Windows 7 Enterprise 64bit VMs
Domain Controller
VMware Virtual Center
VMware View Planner 2.1 Server
SUT Management Server
vShield Manager
Administration Client
SUT Security Virtual Appliance
RAID 10 Volume with 12x450GB SAS disks in the HP MSA 2012FC storage hosted only the Windows 7 virtual desktops and the SUT security virtual appliance

Source: Tolly, May 2013

Figure 7

Systems Under Test

Vendor	Product	Architecture	Components	Implementation
Kaspersky Lab	Kaspersky Security for Virtualization v2.0	Agentless	Kaspersky Security Center 10.0.3361 Kaspersky Security for Virtualization (ksv appliance) 2.0.0.34	Single virtual appliance. Agentless client communicates via VMware vShield API
McAfee, Inc	MOVE Agentless 2.6	Agentless	McAfee ePolicy Orchestrator 4.6.2 (Build: 234) and 5.0.0 (Build:1160) McAfee move-sva: McAfee MOVE AV Agentless 2.6.0.409	Single virtual appliance. Agentless client communicates via VMware vShield API
Symantec Corp.	Endpoint Protection 12.1.2	Agent-based	Symantec Endpoint Protection Manager 12.1.2015.2015; Symantec Security Virtual Appliance 12.1.1959.1959	Endpoint client with vShield-based Shared Insight Cache for on-demand scan optimization
Trend Micro, Inc	Deep Security 8 SP2	Agentless	Deep Security Manager 8.0.4100 Deep Security Virtual Appliance 8.0.0.2120	Single virtual appliance. Agentless client communicates via VMware vShield API

Source: Tolly, May 2013

Table 2

the scan for all new files and then the caching function for the 2nd and 3rd scan. So the Virtual Image Exception feature was not used for SEP. The vShield-based Shared Insight Cache feature was enabled for SEP.

The time duration to scan each VM was recorded from all SUT's logs. Esxtop recorded the performance of the ESXi hypervisor for 4 hours. The average results in 4 hours were reported in this report.

View Planner Test

Tests were run with 100, 120 and 140 VMs to evaluate the user experience and resource consumption with different virtual desktop densities. Each VM was running the same VMware View Planner 2.1 Standard workload with Microsoft Word, Excel, PowerPoint, Internet Explorer, Outlook, Media Player, Adobe Reader, Firefox and 7-zip applications. Iterations - 7, think time - 20, ramp up time - 600, test type - local were used as the View Planner configuration.

For Kaspersky, Trend Micro and McAfee agentless solutions, one update task was scheduled for the security virtual appliance after 3 hours from the beginning of the workload. For Symantec Endpoint Protection (SEP), the communication settings were set to: Download - pull mode, heartbeat interval - 30 minutes, download randomization - enabled, randomization window - 1 hour. The high performance anti-malware policy was used for SEP. One update task was scheduled to update the definition on the SEP management server after 3 hours from the beginning of the workload.

The View Planner results were reported. To pass the View Planner test, 95% of the Group A response times during Steady-State must be 1.5 seconds or less. The 95% Group A response time was reported in this report. View Planner puts tasks into three groups (Group A, B and C). Group A includes 27 out of total 44 user operation types. For detail about View Planner results, please refer the VMware View Planner Installation and User Guide Ver 2.1.

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.

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 Fair Testing Charter, Tolly contacted the competing vendors inviting them to review the test methodology and their results prior to publication.

Trend Micro did not respond to our request. Symantec and McAfee responded to our invitation, reviewed the proposed test methodology and device configurations. McAfee did not provide any comments on the methodology or results prior to publication. Symantec reviewed the performance results and Tolly answered any and all questions. At time of publication, Symantec disputed its effectiveness results stating that it believed its score should have been 100% rather than 99.4%.

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.