TEST REPORT

Tolly.

#211101
February 2011
Commissioned by Trend Micro, Inc.

Trend Micro Deep Security 7.5 vs. McAfee and Symantec

Anti-virus Performance in VMware ESX Virtual Environments

Executive Summary

Server and desktop virtualization are essential elements of any IT strategy that seeks to decrease capital and operational expenditures . In the rush to implement virtualization technologies, many organizations simply deploy the same anti-virus solution that is in use on their physical server and desktop systems. Because these traditional anti-virus solutions are not designed specifically for virtual environments, they can create significant operational issues such as anti-virus (AV) storms, resource wastage and administrative overhead, and hamper the organization's objective of maximizing VM densities.

Trend Micro, Inc. commissioned Tolly to benchmark the performance within virtual environments of the Trend Micro Deep Security solution vs. McAfee Total Protection for Endpoint and Symantec Endpoint Protection 11.0. Specifically, this testing evaluated the impact each solution had on host system (physical server) resources especially as guest machine density increased to up to 100 virtual machines simultaneously running in a VMware ESX 4.1 environment.

TEST HIGHLIGHTS

The Trend Micro Deep Security Virtual Appliance:

1. Demonstrated consistently lower demand for system CPU, memory and disk I/O over traditional agent-based solutions even during periods when the workload was designed not to stress AV
2. Successfully avoided AV storm issues with scheduled scans and pattern updates that prevented other solutions from testing beyond 25 VMs
3. Demonstrated density improvements of 29% to 275% over McAfee and Symantec running test workloads

Tests showed that Trend Micro Deep Security, which provides an agentless virtual appliance-based approach to anti-virus protection optimized for virtualization, consistently consumed less CPU, RAM and disk I/O resources than the non VM-aware implementations where anti-virus agents and processing resided in each and every Windows 7 virtual machine.

In addition to consuming 1.7 to 8.5 times the resource overhead of the Trend Micro solution in the general workload test, the traditional AV solutions were seen to face AV storm challenges when tested at peak activities (i.e., running on-demand scans and signature updates) when operations on 25 VMs were triggered simultaneously. Specifically, when Tolly engineers attempted to remediate the competing systems immediately and, because the traditional solutions were not VM-aware, management station requests for, say, 25 virtual machines to run on-demand scans or update signature files triggered all of the virtual machines to begin execution of the function simultaneously resulting in a surge in demand on host resources such as CPU and memory.

Ultimately the savings in resource consumption afforded by Trend Micro Deep Security allows organizations to increase virtual machine densities, i.e. the number of VMs that can be run per host, enabling capital expenditure (CAPEX) and operational expenditure (OPEX) savings for the organization. The VM density improvement made possible because of Trend Micro's lower resource consumption and AV storm avoidance in the proprietary workload tests ranged from a minimum of 29% (when running a workload that did not stress AV) to a maximum of 275% (during AV storm periods) over McAfee and Symantec

Tolly engineers benchmarked security system resource utilization by running various workloads on up to 100 virtual machines simultaneously. A baseline was established by running a workload simulating various end-user functions on systems that had no endpoint security solution installed and measuring resource consumption.

Testing included benchmarking resource consumption when running specific anti-virus tasks (on-demand scan and signature updates) as well as a more general user workload with anti-virus protection present on each virtual machine.

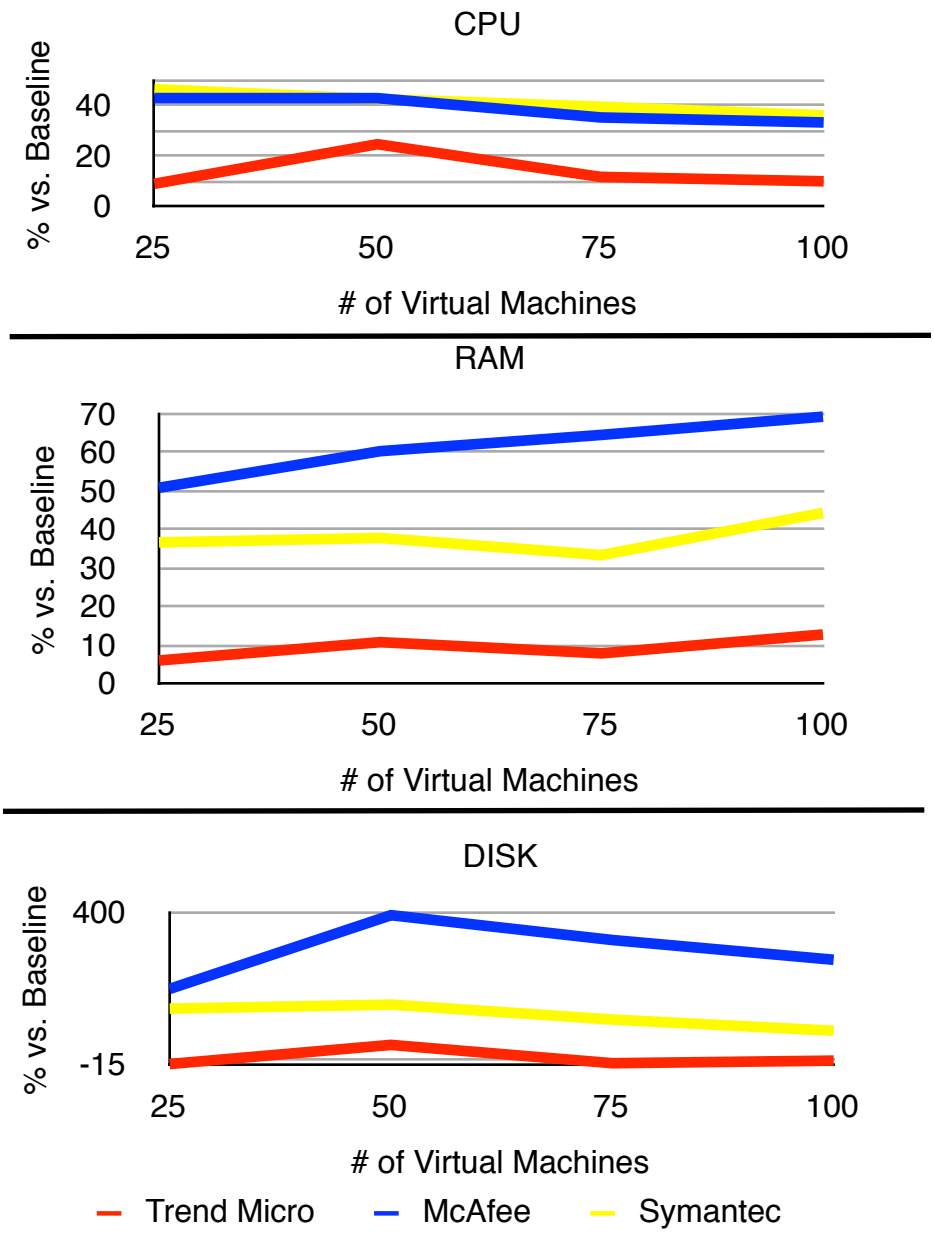
Anti-virus Resource Utilization with Simulated Workload (25 to 100 Virtual Machines)

Figure 1 illustrates average utilization levels of key system resources at the VMware ESX server level when running the primary test workload with up to 100 simultaneous virtual machines. (See Table 4 for individual data points.)

These figures include the resources used by the virtual machines as well as, for Trend Micro, the resources used by the Deep Security virtual appliance. See the Test Methodology and Testbed Setup section for details on the workloads and environment.

Both McAfee and Symantec solutions required that a separate instance of the AV agent run in each virtual machine. Trend Micro Deep Security required one instance of its virtual appliance per host. The figure illustrates how, at all VM density levels, and across all three resources - CPU, Memory and Disk Usage. Symantec and McAfee consumed 1.7 to 8.5 times the amount of resource overhead required by Trend Micro.[1]

Anti-virus VMware ESX 4.1 Host Resource Consumption vs. Baseline
Up to 100 Virtual Machines Running Proprietary Workload under Microsoft Windows 7
As reported by vCenter (Lower numbers are better)

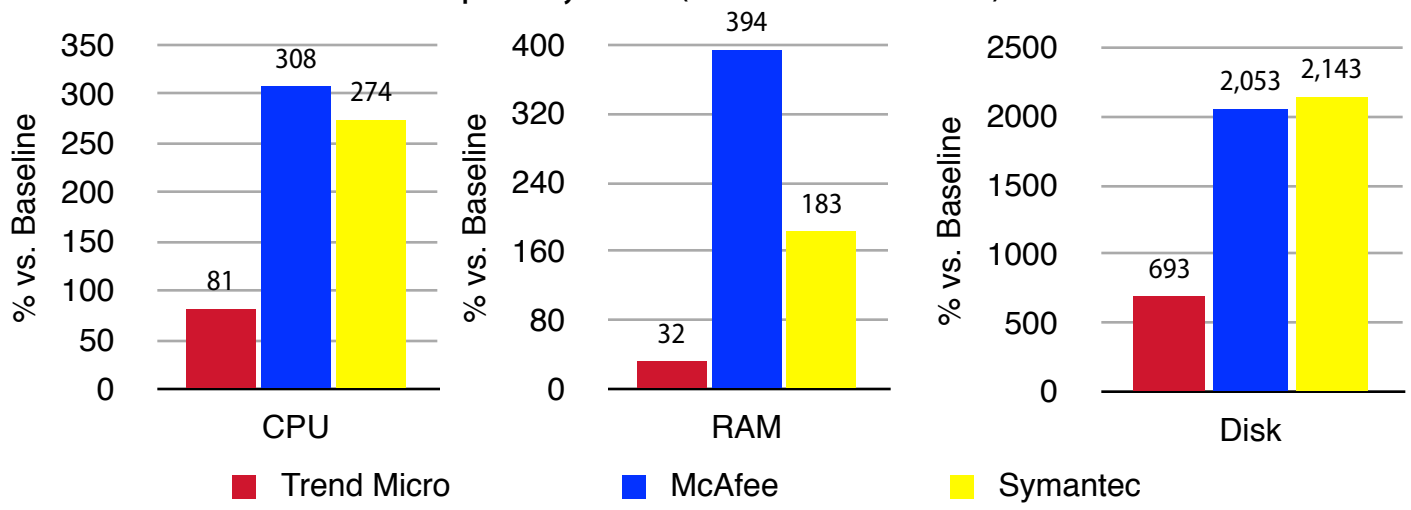


Note: All systems running proprietary workload in addition to scan. Baseline is proprietary workload running with no endpoint security solution installed. See report body for baseline values and detailed results. Utilization over baseline is calculated by subtracting baseline from result, dividing by baseline and multiplying by 100. As McAfee was unable to complete the 100 VM test, results for 100 were extrapolated from the 25, 50 and 75 VM tests. Average of 30 minute run. Disk usage results vary up to 30% and are include for reference purposes only.

Source: Tolly, October 2010

Figure 1

[1] The McAfee solution was unable to complete the 100 VM test despite multiple attempts and re-runs.. Tolly engineers extrapolated the McAfee 100 VM results from the McAfee 25, 50 and 75 VM test results.



Note: All systems running proprietary workload in addition to scan. Baseline is proprietary workload running with no endpoint security solution installed. Baseline values: Average CPU = 4,109.76 MHz, Average RAM = 7,893.28 MB, Average Disk = 1,741.23 KBps. Trend automatically runs only a single scan at one time. Other vendors triggered 25 simultaneous scans. Each vendor recommends various methods such as randomization for load-leveling on-demand scans. See report body for details. Utilization over baseline is calculated by subtracting baseline from result, dividing by baseline and multiplying by 100. Average of 30 minute run.

Source: Tolly, October 2010

Figure 2

Anti-virus On-Demand Scans (25 VMs) Test

Engineers evaluated how each solution responded to a security management system request to conduct a full scan on 25 virtual machines. Being resource intensive in nature, simultaneous scans can degrade overall user experience.

Trend Micro Deep Security was aware that it was running in an environment where resources were shared across all VMs and automatically scheduled scans to run serially - a maximum of 1 machine running at a time. As a result, Deep Security was able to successfully test at 25 and 50 VMs. Based on the resource utilization observed in these tests, Tolly projects that the Trend Micro solution could support a scenario of more than 100 VMs.

By default, the other solutions (that are unaware of the shared, virtual environment) attempted to initiate simultaneous scans of all 25 machines. Figure 2 provides the average resource results for those tests where McAfee resource consumption overhead was 2.8 times more than Trend Micro for CPU and 11 times for RAM. Symantec resource consumption overhead was 2.4 times more than Trend Micro for CPU and 4.7 times for RAM.

In addition, the 25 VM data set for Symantec and McAfee does not provide the complete picture with respect to reliability and user experience. The surge in resource demand from the McAfee and Symantec solutions often degraded the user systems. In particular, neither Symantec nor McAfee solutions were able to be tested beyond 25 VMs. In the Symantec test, 2 agents lost connectivity with the management server during the test and disk latency (not illustrated in the figures) was noted to average 31 ms. With the McAfee on-demand scan scenario, disk latency was noted to average 80 ms. During the test, 14 out of 25 users were not able to access their desktops. See Table 2 for additional commentary.

Traditional solutions generally recommend two approaches to avoid virtual environment resource contention - randomization and grouping. Neither of these approaches provides any virtualization awareness and, thus, were outside the scope of this test.

With randomization, an administrator can set up the randomization period to let endpoints run tasks with random start times. For time consuming tasks like full scan, this time period needs to be very long

(more than a day or a week depending upon the host's VM density) to increase the chances that client tasks won't overlap each other. As a result, when facing a critical security threat, enterprise administrators may not be able to remediate their systems immediately. Also, the random tasks may degrade user experience if they run when system usage is already high.

Anti-virus Solution Scalability Under VMware ESX 4.1
On-Demand Scan Scenarios of Virtual Machines Running Microsoft Windows 7

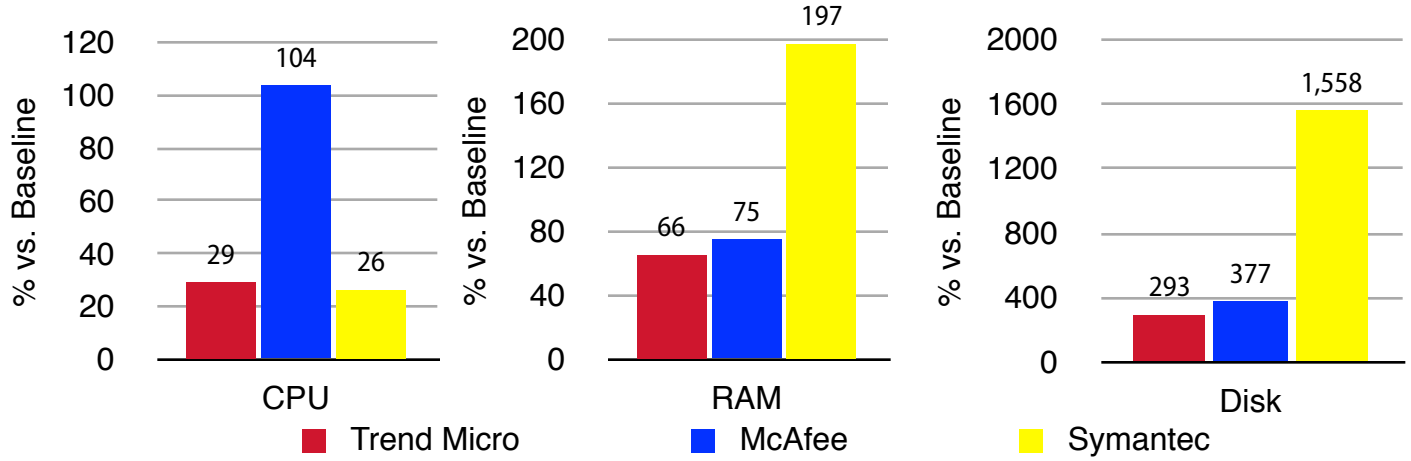
Vendor	Product	Number of Virtual Machines Targeted for On-Demand Scan			
		25	50	75	100
Trend Micro, Inc.	Deep Security 7.5	Yes, completely stable	Yes, completely stable	Yes (projected, not tested)	Yes (projected, not tested)
McAfee	Total Protection for Endpoint	Yes, but with stability problems	Because of instability problems with 25 simultaneous scans, Tolly engineers did not attempt greater numbers. McAfee offers a randomization option in its client task that could provide load distribution for such both scheduled and manually triggered tasks.		
Symantec	Endpoint Protection 11.0	Yes, but with stability problems	Because of instability problems with 25 simultaneous scans, Tolly engineers did not attempt greater numbers. Symantec recommends configuring scheduled tasks for randomization. This would spread the on-demand scan requests for 100 virtual machines to approximately 160 hours by default. Manually triggered tasks cannot have randomized start times.		

Note: Trend Micro is the only virtualization-aware solution tested and automatically staggers on-demand scans so that scans are performed serially.

Source: Tolly, October 2010

Table 1

Anti-virus Solution VMware ESX 4.1 Host Resource Consumption vs. Baseline
Request Signature Update of 50 Virtual Machines Running Microsoft Windows 7
As reported by vCenter (Lower numbers are better)



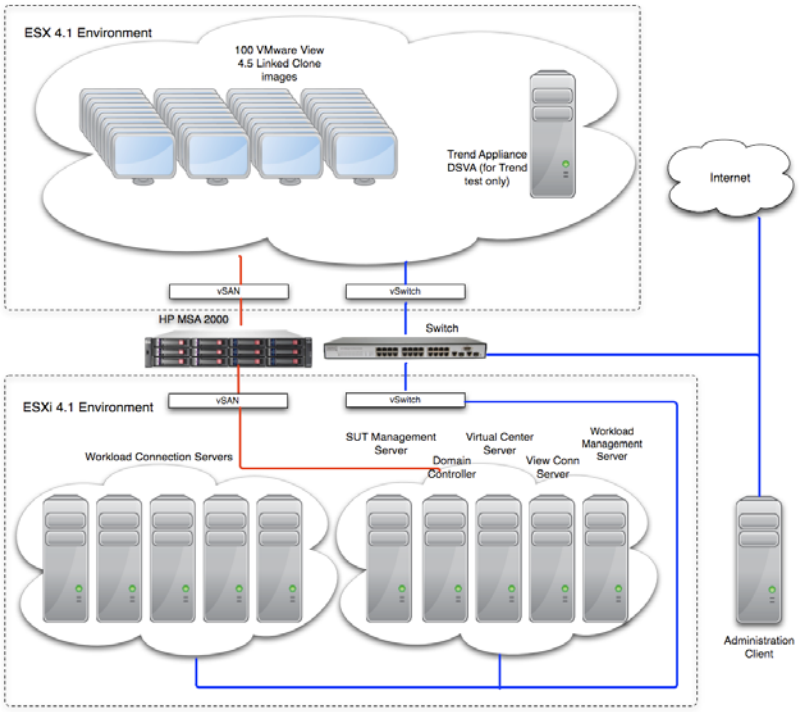
Note: All systems running proprietary workload in addition to test task. Baseline is proprietary workload running with no endpoint security solution installed. Baseline values: Average CPU = 8,434.91 MHz, Average RAM = 14,119.62 MB, Average Disk = 2,341.41 KBps. Trend only needs to download the signature file to its single virtual security appliance. Other vendors triggered 25 simultaneous updates. Each vendor recommends various methods for load-leveling updates. See report body for details. Utilization over baseline is calculated by subtracting baseline from result, dividing by baseline and multiplying by 100. Average of 15 minute run.

Source: Tolly, October 2010

Figure 3

With grouping, an administrator can assign VMs to different groups and schedule client tasks by group. This approach requires administrative work and makes the enterprise IT management more complicated. New VMs need to be allocated manually to groups and, if VMs get migrated from one host to the other for load balancing or other reasons, administrators have to update the group assignments accordingly.

Virtualized Anti-virus Test Environment



Source: Tolly, October 2010

Figure 4

Systems Under Test

Vendor	Product	Components	Virtual Machine Aware	Implementation
Trend Micro, Inc.	Deep Security 7.5	Trend Micro Deep Security Manager version 7.5.1378; Trend Micro Deep Security Virtual Appliance 7.5.0.1600; Filter Driver 7.0.0.894; Default configuration. Assigned the pre-configured Windows Anti-Malware Protection security profile.	Yes	Automatic, single virtual appliance. Agentless client communicates via VMware vShield API
McAfee	Total Protection for Endpoint	McAfee ePolicy Orchestrator 4.5; McAfee Agent for Windows 4.5.0 Minor Version 1270; McAfee VirusScan(R) Enterprise 8.7.0 Minor version 570 with Hot Fix 2; McAfee AntiSpyware Enterprise 8.7 Minor version 129; McAfee Host Intrusion Prevention 7.0.0 minor Version 1070; McAfee SiteAdvisor(R) Enterprise Plus 3.0.0 Minor version 476 All with default policies. Cancelled pre-configured Full Scan and Update client tasks.	No	Traditional endpoint client
Symantec	Endpoint Protection 11.0	Version 11.0.6100.645	No	Traditional endpoint client

Source: Tolly, October 2010

Table 2

Anti-virus Signature (Pattern) Update (50 VMs) Test

Engineers evaluated how each solution responded to a systemwide anti-virus pattern update request. Pattern updates, while less resource-intensive than full scans, are still known to create performance degradation and raise operational challenges especially if they are run during regular business hours.

Engineers ran the signature update scenario with 50 virtual machines. Where the traditional solutions required that the signature files be updated in each virtual machine, the Trend Micro solution required only a single copy of the signature file that resided on the Trend Micro Deep Security appliance and was used for all the VMs monitored by Trend Micro. Thus, where the resource consumption of the traditional solutions were notably higher in either CPU or RAM, the Trend Micro resource consumption was consistently lower. See Figure 3.

Engineers also noted that network security managers implementing the Trend Micro solution need not be concerned about virtual machine's that are "offline" during the time that the signature update process takes place. With traditional implementations VMs must be online to receive updates.

As with the simultaneous on-demand scan test, the requirement to process updates on all 50 virtual machines at once on the McAfee and Symantec solutions had resource and performance implications at the overall system level.

With Symantec, most VMs triggered memory alarms in VMware's vCenter management station as Symantec's signature update task fully consumed the 1GB RAM allocation in each of the machines. 10 of 50 users' VMware View desktops became disconnected during this test.

Although not used for this test, engineers noted that the McAfee solution included a task for idle VMs to update their signature files once each day. While engineers cancelled this task, it was noted that the task would still initiate automatically.

As with Symantec, the resources consumed when 50 VMs are being updated simultaneously can be significant and engineers noted that VMware ESX system CPU usage remained at 100% for more than 10 minutes in some test runs and that the entire virtualized system demonstrated severely degraded performance.

VM Density (Consolidation) Comparisons

Most virtualization efforts calculate sizing based mostly on the primary VM workloads, and do not take into account the disruptive traditional AV workload. As part of this test, Tolly also attempted to evaluate the impact of AV efficiency on VM density. Density improvements can be calculated in various ways - (a) when AV is idle, and (b) when AV solutions are performing immediate client tasks like on-demand scans and signature updates.

Trend Micro, Inc.

Deep Security 7.5

VMware Anti-virus Performance

Tested October 2010

Nominal VM density (AV idle)

Here the focus was primarily on the resource footprint of the AV solution at rest, while the

VMware Performance Host Testbed Components

Component	Version/Build
VMware ESX	4.1.0
VMware vCenter Server	4.1.0 build 258902
VMware View Composer Server	2.1 build 277387
VMware View Connection Server	4.5.0
VMware vShield Manager	4.1 build 310451
Server Hardware	2x Xeon x5680 (Hexacore) running at 3.33GHz with 192 GB of DDR 3 RAM (Total of 24 logical cores)
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

Source: Tolly, October 2010 Table 3

primary workload was running but no specific AV task had been triggered. The VM density improvement with the Trend Micro solution was 34.5% and 29% over Symantec for CPU and memory respectively. Similarly, the VM density improvement was 31.4% and 42.4% over McAfee for CPU and memory respectively. See Table 5.

True VM density (Full Scans)

Using AV idle nominal densities does not account for the peak AV activities, which is why virtualization deployments are increasingly seeing "AV storms" that starve the ESX host and the VM workloads. As seen in the testing, AV scans and updates are resource-intensive in all three areas of CPU, memory and disk usage. and it can vary with the system and workload which resource will become the bottleneck.

The VM density improvement with the Trend Micro solution was 106% and 114% over Symantec for CPU and memory respectively. Similarly, the VM density improvement was 124.9% and 273.5% over McAfee for CPU and memory respectively.

Trend Micro Deep Security

Trend Micro has architected its Deep Security 7.5 offering to be "virtual machine aware." Unlike traditional agent-based solutions Deep Security focuses on reducing operational security issues such as anti-virus storms, resource wastage and administrative overhead. Deep Security provides an agentless approach to anti-virus protection optimized for virtualization that aims to deliver faster performance, higher VM consolidation, easier manageability and faster "time to protect" for virtualized assets.

Source: Trend Micro, October 2010

Anti-Virus VMware ESX 4.1 Host Resource Consumption vs. Baseline
Up to 100 Virtual Machines Running Proprietary Workload under Microsoft Windows 7
As reported by vCenter (Lower numbers are better)

Number of virtual machines	AV Solution		ESX Host Baseline Resource Utilization/% Increase over Baseline		
			CPU (GHz)/%	RAM (GB)/%	Disk (KBps)/%
25	Baseline		4.113 GHz	6.306 GB	1.705 KBps
	Trend Micro	% increase over baseline	8.86%	5.94%	-13.26%
	McAfee		43.04%	50.83%	191.82%
	Symantec		46.58%	36.63%	138.05%
50	Baseline		8.467 GHz	11.908 GB	2.592 KBps
	Trend Micro	% increase over baseline	24.65%	10.7%	38.98%
	McAfee		43.02%	60.34%	393.09%
	Symantec		42.73%	37.78%	148.91%
75	Baseline		12.645 GHz	17.325 GB	3.381 KBps
	Trend Micro	% increase over baseline	11.61%	7.79%	-11.03%
	McAfee		35.33%	64.57%	325.32%
	Symantec		39.61%	33.33%	108.22%
100	Baseline		17.197 GHz	22.468 GB	5.417 KBps
	Trend Micro	% increase over baseline	9.86%	12.7%	-4%
	McAfee		33.33%	69.31%	271.43%
	Symantec		36.14%	44.31%	77.61%

Note: Baseline values represent 30 minute test runs of a proprietary workload running with no anti-virus/endpoint security solution installed. Lower percentage increases in resource consumption are better. In many cases, the test runs were not complete at the expiration of the test window. The McAfee solution was unable to complete the 100 VM test despite multiple attempts and re-runs. Tolly engineers extrapolated the McAfee 100 VM results from the McAfee 25, 50 and 75 VM test results. Disk usage results vary up to 30% and are included for reference purposes only.

Source: Tolly, October 2010 Table 4

Test Methodology and Testbed Setup

All tests were conducted using the same hardware infrastructure and, thus, were conducted serially for each system. Table 2 provides the details of the solutions under test, the virtual machine guest systems, and Table 3 provides details of the virtual machine host environment for the performance host.

It should be noted that the physical server CPU consisted of 24 logical cores which meant that systems configured for 100 virtual machines oversubscribed the physical CPU resource by approximately 4:1. Testers noted that that, over the course of the test, the CPU resource was not identified as a bottleneck.

A VMware ESXi host was used to run other infrastructure used for the test including the various management servers required by the systems under test as well as the load generator systems.

The Trend Micro solution was implemented as a virtual appliance and used the VMware API to communicate with the guest machines. This API conducts that communication via the virtual network interface.

The other solutions were not "virtual machine-aware" and, thus, were implemented in the same manner as if 100 physical Windows machines were deployed.

At the time that the test environment was finalized, McAfee's solution for endpoint security in virtualized environments, McAfee Management for Optimized Virtual Environments (MOVE) was not yet available for VMware host environments

All products under test were with their default anti-virus policies. Pre-configured scheduled full scan and update tasks were cancelled.

Primary Workload

The primary tests used a proprietary workload which, in turn, was broken down into three levels of activity:

High: 55% of the guest machines ran scripts using Microsoft Outlook, Word, Excel, Powerpoint, Internet Explorer and Adobe Reader applications. Low: 35% of the guest machines ran scripts using Microsoft Outlook, Word, Internet Explorer and Adobe Reader applications. Idle: 10% of the guest machines were booted to Windows and allowed to remain idle.

This workload was used for all the tests and served as the background workload for the on-demand scan and signature update tests. Windows firewall and Windows defender were turned off on all guest virtual machines.

For the primary workload tests, Tolly engineers launched the workload which automatically logged in all users with VMware View clients and ran the application scripts.

Script activities included editing email and Microsoft Office documents, paging through Adobe PDF documents and browsing the web. The workload did not include any I/O-intensive or file copy tasks. Runs were 30 minutes in length.

On-Demand Scan and Signature Update Tests

Tolly engineer launched the primary workload to serve as background load and then assigned one full scan or update task from the management server to all guest virtual machines under test. Runs were 15 minutes length.

All performance results were captured from VMware vCenter at 20 second intervals.

VM Density Improvement - Proprietary Workload: Trend vs. Competitor
(Nominal Density)

	CPU	RAM	DISK
McAfee	31.4%	42.4%	236%
Symantec	34.6%	29%	174%

VM Density Improvement - On-Demand Scan: Trend vs. Competitor
(True Density)

	CPU	RAM	DISK
McAfee	124.9%	273.5%	171.6%
Symantec	106.0%	114.1%	183%

Note: Based on resource consumption, figures in table represent the scaling/density improvement potential of Trend Micro vs. each competitor.
Nominal density refers to systems running a load that does not stress the AV.
True density refers to a load that drives the AV solution.

Source: Tolly, October 2010 Table 5

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. Symantec responded and worked with Tolly engineers. Symantec recommended the use of its randomization feature to distribute resource-intensive workloads across an extended period of time.

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.

211101-uv-3-kt - 04Feb2011VerP