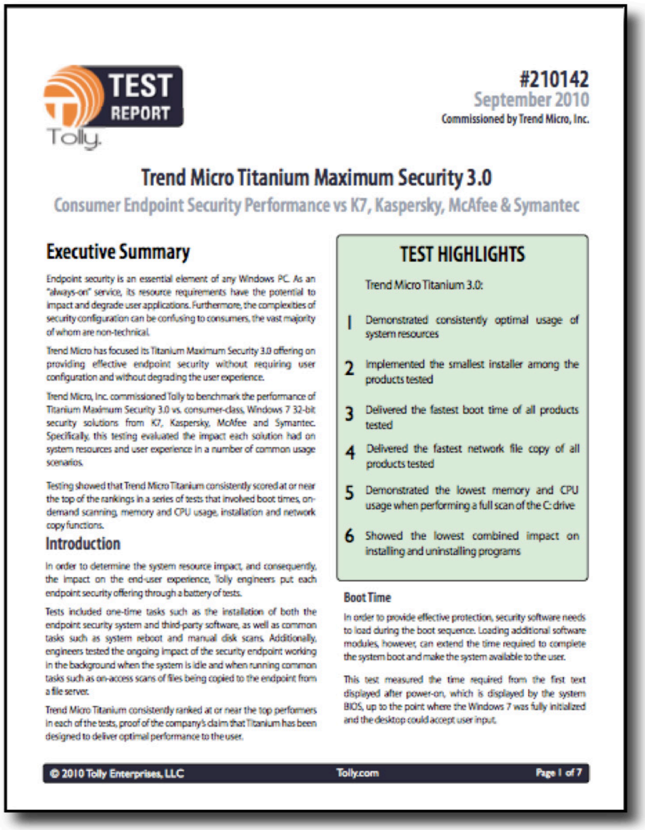
APPENDIX to Tolly Document 210142

Consumer-class Endpoint Security: Functionality & Performance Evaluation

Trend Micro vs. comparable solutions from: K7, Kaspersky Lab, McAfee, & Symantec

Tolly Report #210142A-
Commissioned by
Trend Micro, Inc.
Published September 2010



TEST REPORT
Tolly.

#210142
September 2010
Commissioned by Trend Micro, Inc.

Trend Micro Titanium Maximum Security 3.0

Consumer Endpoint Security Performance vs K7, Kaspersky, McAfee & Symantec

Executive Summary

Endpoint security is an essential element of any Windows PC. As an "always-on" service, its resource requirements have the potential to impact and degrade user applications. Furthermore, the complexities of security configuration can be confusing to consumers, the vast majority of whom are non-technical.

Trend Micro has focused its Titanium Maximum Security 3.0 offering on providing effective endpoint security without requiring user configuration and without degrading the user experience.

Trend Micro, Inc. commissioned Tolly to benchmark the performance of Titanium Maximum Security 3.0 vs. consumer-class, Windows 7 32-bit security solutions from K7, Kaspersky, McAfee and Symantec. Specifically, this testing evaluated the impact each solution had on system resources and user experience in a number of common usage scenarios.

Testing showed that Trend Micro Titanium consistently scored at or near the top of the rankings in a series of tests that involved boot times, on-demand scanning, memory and CPU usage, installation and network copy functions.

Introduction

In order to determine the system resource impact, and consequently, the impact on the end-user experience, Tolly engineers put each endpoint security offering through a battery of tests.

Tests included one-time tasks such as the installation of both the endpoint security system and third-party software, as well as common tasks such as system reboot and manual disk scans. Additionally, engineers tested the ongoing impact of the security endpoint working in the background when the system is idle and when running common tasks such as on-access scans of files being copied to the endpoint from a file server.

Trend Micro Titanium consistently ranked at or near the top performers in each of the tests, proof of the company's claim that Titanium has been designed to deliver optimal performance to the user.

TEST HIGHLIGHTS

Trend Micro Titanium 3.0:

1 Demonstrated consistently optimal usage of system resources

2 Implemented the smallest installer among the products tested

3 Delivered the fastest boot time of all products tested

4 Delivered the fastest network file copy of all products tested

5 Demonstrated the lowest memory and CPU usage when performing a full scan of the C: drive

6 Showed the lowest combined impact on installing and uninstalling programs

Boot Time

In order to provide effective protection, security software needs to load during the boot sequence. Loading additional software modules, however, can extend the time required to complete the system boot and make the system available to the user.

This test measured the time required from the first text displayed after power-on, which is displayed by the system BIOS, up to the point where the Windows 7 was fully initialized and the desktop could accept user input.

© 2010 Tolly Enterprises, LLC Tolly.com Page 1 of 7

Trend Micro, Inc.

Titanium Maximum Security 3.0

Tested August 2010

Consumer Endpoint Security for Windows 7

Introduction

This document is an appendix to Tolly document #210142 published in September, 2010. This appendix contains a more detailed test methodology as well as tabular results of each of the individual test runs that were summarized in the main document.

This document is a supplement to and should only be read in conjunction with Tolly document #210142 which can be found on http://www.tolly.com.

Solutions Under Test (SUT)

The evaluation included generally available production versions of products from some vendors and beta versions of products from other vendors. Trial versions of products were used when available. See Table 1 for product details.

Consumer Endpoint Security Systems Under Test

Vendor	Product	Version	Status
Trend Micro, Inc.	Titanium Maximum Security	3.0.1303 (Most components v 1.5.1381. Virus Scan engine 9.200.1007)	Full complement of tests run with default settings which specifies compressed files are not scanned in real time.
K7 Computing Private Ltd.	K7 TotalSecurity	10.0.00.31 Antivirus ver 9.47.1238	GA
Kaspersky Lab	PURE	9.0.0.192	
McAfee	Total Protection 2010	10.5.195 (McAfee has apparently changed the main version from 4 to 10 with this release.)	GA (as of late July 2010).

Consumer Endpoint Security Systems Under Test

Vendor	Product	Version	Status
Symantec	Norton 360	4.1.0.32	GA
Symantec	Norton Internet Security 2011	18.1.0.30 (Note: Symantec claims that this is an invalid release number and that it should be 18.0.1.33. The release number referenced by Tolly is provided by Symantec in the WIndows 7 control panel display.)	Beta

Note: Trial versions were used unless otherwise noted.

Source: Tolly, August 2010 **Table 1**

Application Software Environment

For the purposes for this test, engineers used a base Windows system with all system updates installed as of 10Aug2010 and installed only the requisite benchmarking application. Testers made a backup system image before installing any endpoint security product. After a given product was tested, the system was restored to the system image created before the SUT was installed. See Table 2.

Endpoint User Application Software Environment

Vendor	Application	Description
Epsilon Squared	InstallRite 2.5	Used to measure disk utilization
Source: Tolly, August 2010		**Table 2**

Data Files for Performance Tests

Endpoint security solutions not only scan static files ("data at rest") but also inspect files that are being copied to/from the computer ("data in motion"). Copy performance tests provide insights into potential degradation (lengthening) of copy time that is introduced by the inspection process.

Current generation computers are generally equipped with high-speed hard drives as well as Gigabit Ethernet network connections and, thus, are able to transfer/copy even files of several megabytes almost instantaneously. Thus, tests of relatively small files are of little interest as users are unlikely to be concerned if, say, one solution requires 2.0 seconds to copy a file and another requires 2.4 seconds - 20% longer - as such differences are unlikely to impact the user experience. Thus, this test will use a test corpus that includes many files so that the cumulative impact of scanning (real time and/or batch) can be demonstrated.

Data for File Copy & Scan Tests

Trend Micro has assembled a corpus that, compressed, is approximately 6GB in size. The corpus contains a wide variety of files that are indicative of what can be found on a typical user PC. This corpus, called "TPM", was decompressed to provide a series of folders and data (~5,000 files and folders in all) that was used for the file copy tests and as additional data that for the scan tests.

Data For Microsoft MSI Installer Test

The testing also involves running a Microsoft installer package. This test used the .NET Compact Framework 2.0 Redistributable. The file name is NETCFSetupv2.msi. It is 24.5MB and dated 27 March 2006. It can be downloaded from Microsoft at http://www.microsoft.com/downloads/details.aspx?familyid=9655156b-356b-4a2c-857c-e62f50ae9a55&displaylang=en. (Note: this is a developer package for use with the Microsoft .NET system and the systems it references in its description are the target systems for eventual distribution of systems build by .NET and not of this particular installer itself.) This was used to simulate an end-user installing an application and monitoring the effects and overhead of antivirus software scanning the files being installed.

Test Results

The following table contains the individual run results.

Performance Evaluation Results (Individual runs)

Description	Baseline	Trend Micro	K7	Kaspersky	McAfee	Symantec 360	Symantec NIS
Installer Size (MB approximate)	N/A	56	56.4	90.9	126 (starts with a 3MB downloader)	116 (starts with 2MB downloader)	87
Installation Time (mm:ss)	N/A	2:25	00:32.5	02:04	~10:00 including download time. Installation requires current software to be download which required approximately 08 mins.	03:38 (stub downloader. Time includes download of program.)	3:38 followed by upgrade to latest version via "Live Update"
Installation Effort	N/A	7 Steps	8 Steps	9 Steps	10 Steps	4 Steps	4 Steps
Uninstallation Time (mm:ss)	N/A	00:57	00:14.4	00:51	01:06	00:23	00:20
Disk Utilization (# Files added/Total Size in KB) as per InstallRite 2.5c compared to baseline	N/A	5,372/ 292,749	232/ 183,986	6,048/ 772,598	1,396/ 333,120	1,469, 507,727 ----------- DIsk utilization before installer manually removed was: 638,265	1,411, 370,115

Performance Evaluation Results (Individual runs)

Description	Baseline	Trend Micro	K7	Kaspersky	McAfee	Symantec 360	Symantec NIS
System Memory Footprint: Idle (MB) delta above baseline. Committed memory (combination of kernel and user)	669, 672, 676 [672.3]	756.6, 745, 741, 748 [747.7] Delta = 75.4	812, 823.5 844, 849.5 [832.23] Delta = 159.925	768, 779, 783, 770 [775] Delta = 102.7	862, 860 878 862 [865.5] Delta = 193.2	727, 732, 731, 746 [734] Delta = 61.7	700, 708, 683, 682 [693.25] Delta = 20.95
Memory Footprint: Busy - Full Scan for 5 minutes (MB)- delta above baseline. Committed memory (combination of kernel and user)	N/A	815, 875, 867, 817 [843.5] Delta = 171.2	955, 959.5 969.5 966.3 [962.575] Delta = 290.275	915, 1153, 1030, 1127 [1,056.25] Delta = 383.95	879. 882.9 902, 880.5 [886.1] Delta = 213.8	936, 930, 1097, 959 [980.5] Delta = 308.2	930, 1010, 1120, 1024 [1021] Delta = 348.7
End-user Perspective: Boot Time from BIOS to desktop (seconds) [average]	29.5, 30.2, 30.5 [30.06]	35.6, 33, 33 [33.866]	33.8, 36.4, 34.8 [35]	36.3, 40.8, 42.1 [39.73]	34, 33, 33.9 [33.63]	[13.1, 48.0, 12.9, 45.0, 13.3, 48.3 [47.1]	37.8 37.5, 38.3 [37.866]

Quick Scan: Time (seconds) {objects} [average]	N/A	4.1, [133]
		4.3, [133]
		4.3,[133]
		[4.233]
			9.9, {169}
			8.8, {169}
			8.0, {169}
			(8.9)
				37, {3153}
				05, {2974}
				05, {2974}
				[15.66]
					95, {392}
					61, {392}
					52, {392}
					[69.33]
						27, {4985}
						9, {4916}
						9, {4964}
						[15]
							12.5, {4745}
							9.4, {4921}
							8.8, {4944}
							[10.233]

Performance Evaluation Results
(Individual runs)

Description	Baseline	Trend Micro	K7	Kaspersky	McAfee	Symantec 360	Symantec NIS

Full Scan (C: drive): Time (mm:ss) {objects}	N/A	07:28, {47843}
		07:21, {47844}
		07:19, {47831}
		[07:22/7.38 min]
			24:03 {53987},
			24:05 {53988},
			24:09 {53990}
			(24:056/24.09m)
				29:59, {363705}
				23:23, {344385}
				25:03, {361648}
				(26.13 min)
					17:01,
					11:25
					10:44
					{57497 files, 39937 registry entries}
					(13:05/13.08 min)
						Product does not allow custom scan of C: only to be specified. Full scan includes all hard drives on the system.	10:33, {115397}
							01:17,{68121}
							01:14, {68121}
							(04:21/4.35min)

Full Scan (C: drive): Average CPU utilization, first 5 minutes of scan (%) and Standard Deviation (STDEV)	N/A	33.397, 38.029, 33.692 [35.04] STDEV = 2.593	34.836, 35.160, 35.293 [35.096] STDEV = 0.235	73.953, 78.730, 82.149 [78.277] STDEV = 4.117	45.265, 45.547, 46.458 [45.79] STDEV = 0.586	35.909, 41.222, 36.380 [37.837] STDEV = 2.941	33.586, 41.293, 39.561 [38.146] STDEV = 4.043
Network Copy From Server (TPM Corpus) mm:ss	02:18 02:12, 02:20 (02:16/2.28 min)	03:18, 2:42, 2:27 (02:49/2.82 min)	09:35, 09:09, 09:11 (09:18/9.305 min)	04:43, 3:30, 3:25 (03:53/3.877 min)	4:45, 4:06, 4:06 (04:19/4.32 min)	04:34, 04:08, 04:07 [04:16 /4.266 min)	03:58, 03:39, 03:35 [03:44/3.73 min)
MSI File Installation Time (seconds) [average]	5, 5, 5	5.0 5.1 4.9 [5.0]	9.2, 8, 7.8 [8.066]	5.0, 5.8, 4.5 [5.1]	11.1, 10.1, 10.2 [10.466]	6.2, 6.0 4.9 [5.7]	5.2, 4.5 4.1 [4.6]
MSI File Uninstallation Time (seconds) [average]	3, 3, 3	3.1, 2.9, 3.0 [3.0]	7.3, 6.5, 7 [6.933]	4.3, 4.4, 4.2 [4.3]	9.6, 9.9, 9.8 [9.766]	4.8, 4.8 4.9 [4.833]	4.4, 4.8, 4.6 [4.6]

Source: Tolly, August 2010 **Table 3**

Test Methodology & Setup

The following tables describe the procedure to be followed for each test as well as the data that will be recorded by the test engineer.

Prior to testing, the operating system, and applications were installed and a system restore point was created. After each vendor test was complete, the system was restored to the restore point made prior to the installation of any endpoint security system.

Performance Methodology

Unless otherwise noted, performance tests are run three times and the results are averaged. The performance system and data files used for copy tests are described elsewhere in this document. System protection is turned OFF.

Performance Evaluation Methodology			
Description	**Procedure**	**Data Recorded**	**Notes**
Installer Size	Measure the disk space required by the standalone product installer	Size in MB	Some security solutions stream the latest version from a server from a base installer. Such a situation will be noted and sizes of both elements noted where possible
Installation Time/Effort	Measure the elapsed time required to install the solution. Do not include time taken to enter license key	Elapsed time	Note number of steps
Uninstallation Time	Measure the the elapsed time required to uninstall the solution.	Elapsed time	

Performance Evaluation Methodology			
Description	**Procedure**	**Data Recorded**	**Notes**
Disk Utilization	Measure the available hard drive space on the install drive prior to the installation as a baseline. Measure the available hard drive space after the SUT is installed and updated with current signature file. InstallRite 2.5c (Epsilon Squared, Inc.)	Delta between baseline and SUT installed	Installers are manually deleted and are NOT included in the disk utilization total.
Memory Footprint: Idle	Measure the RAM consumed on an idle system with no endpoint security solution installed to use as a baseline. Measure the RAM consumed on the system with the SUT loaded but not actively scanning. Data recorded after the system CPU has entered an idle state which is approximately 10 minutes after boot. Perfmon utility is used to record "committed bytes" for 5 minutes after idle state is entered. Test is run four times with a system reboot between tests.	Committed bytes (average). Calculate results by subtracting baseline from each vendor result. Four Runs.	

Performance Evaluation Methodology

Description	Procedure	Data Recorded	Notes
Memory Footprint: Busy	Measure the RAM and CPU (Average) consumed when SUT is running a disk scan. Measure committed bytes using perfmon for the the first five minutes of a full scan run.	Committed bytes and CPU (average). Calculate RAM results by subtracting baseline from each vendor result. Four Runs.	
Boot Time: End-user perspective	Measure elapsed time as it would appear for the user from the first BIOS screen until the desktop appears and "busy" icon vanishes.	Elapsed time	
Scan Tests It is critically important that the data on the target drive for the scan be identical across runs and vendors. Target drive should be: Base state (OS and test applications installed) plus SUT plus TPM data set unzipped to folders on target drive. Engineer will verify that ZIP performance data is not on the target disk and/or TPM data used for local/network copy functions is not duplicated on the target drive for the scan.			
Full Scan: Time and Avg CPU	Run full scan of boot drive with a single copy of the TPM corpus in the root	Number of files scanned, Elapsed time and average CPU	Drive should be virus-free before scan tests are run.
QuickScan: Time	Run "Quick" scan of boot drive	Number of files scanned, Elapsed time	Different products might have a different scope of coverage for "quick" scans. Thus, results may NOT be directly comparable. Engineer must confirm scope of quick scan methods for each product.

Performance Evaluation Methodology

Description	Procedure	Data Recorded	Notes
File Copy Tests They payload for the file copy tests will be the TPM corpus in an uncompressed state. The corpus will be copied FROM the server to the C drive of the performance machine in the network test. The MSFT XCOPY utility will be used to run the tests.			
Network Copy From Server	Verify that target local drive (C:) has 0% fragmentation. Copy folder containing test files from network share to target system. Start timer when mouse released, end timer when "copying" dialogue disappears. Run three times and average results. Delete folder on target before additional runs. Empty, defrag (if non-zero) and reboot before each run.	Elapsed time, average of three runs	
MSI File Installation Time	Run installer and note the elapsed run time	Elapsed time	Manual measurement so tolerance/variance is +/- 1 second.
MSI File Uninstallation Time	Run uninstall. Note time beginning when "Remove" is clicked	Elapsed time	
Source: Tolly, August 2010			**Table 4**

About Tolly…

The Tolly Group companies have been delivering world-class IT services for 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 e-mail 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 Tolly's Fair Testing Charter, Tolly personnel invited representatives from the competing companies to review the testing. Only K7 and Symantec accepted this offer. Tolly reviewed their concerns and re-ran tests where appropriate and updated results and/or noted competitor concerns in this document.

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.

210142A-uv2-kt-14Sep10-verD