



Webroot SecureAnywhere Endpoint Protection Cloud vs. Seven Traditional Endpoint Security Products

(February 2012)

Endpoint Security Performance Benchmark

Document: Webroot SecureAnywhere Endpoint Protection Cloud vs. Seven Traditional Endpoint Security Products (February 2012)

Authors: M. Baquiran, D. Wren

Company: PassMark Software

Date: 6 February 2012

File: Webroot_SecureAnywhere_vs_endpoint_security_competitors_6Feb2012.docx

Table of Contents

TABLE OF CONTENTS	2
REVISION HISTORY	3
REFERENCES	3
EXECUTIVE SUMMARY	4
OVERALL SCORE	5
PRODUCTS AND VERSIONS	6
PERFORMANCE METRICS SUMMARY	7
TEST RESULTS	9
BENCHMARK 1 – INITIAL SCAN TIME.....	9
BENCHMARK 2 – INSTALLATION SIZE.....	9
BENCHMARK 3 – INSTALLATION TIME.....	10
BENCHMARK 4 – BOOT TIME.....	10
BENCHMARK 5 – MEMORY USAGE DURING SYSTEM IDLE.....	11
BENCHMARK 6 – MEMORY USAGE DURING INITIAL SCAN.....	11
BENCHMARK 7 – BROWSE TIME.....	12
BENCHMARK 8 – FILE COPY, MOVE AND DELETE.....	12
BENCHMARK 9 – FILE COMPRESSION AND DECOMPRESSION.....	13
BENCHMARK 10 – FILE WRITE, OPEN AND CLOSE.....	13
DISCLAIMER AND DISCLOSURE	14
CONTACT DETAILS	14
APPENDIX 1 – TEST ENVIRONMENT	15
APPENDIX 2 – METHODOLOGY DESCRIPTION	16

Revision History

Rev	Revision History	Date
Edition 1	Initial version of this report.	02 February 2012

References

Ref #	Document	Author	Date
1	What Really Slows Windows Down (URL)	O. Warner, The PC Spy	2001-2009

Executive Summary

PassMark Software® conducted objective performance testing on eight (8) security software products, on Windows 7 Ultimate Edition (64-bit) from December 2011 to January 2012. This report presents our results and findings as a result of performance benchmark testing conducted for these endpoint security products.

The aim of this benchmark was to compare the performance impact of Webroot's SecureAnywhere Endpoint Protection cloud product with seven (7) Traditional Endpoint Security competitor products.

Testing was performed on all products using ten (10) performance metrics. These performance metrics are as follows.

- Initial Scan Time;
- Installation Size;
- Installation Time;
- Boot Time;
- Memory Usage during System Idle;
- Memory Usage during Initial Scan;
- Browse Time;
- File Copy, Move and Delete;
- File Compression and Decompression; and
- File Write, Open and Close.

Overall Score

PassMark Software assigned every product a score depending on its ranking in each metric compared to other products in the same category. In the following table the highest possible score attainable is 80; in a hypothetical situation where a product has attained first place in all ten (10) metrics. Endpoint Security products have been ranked by their overall scores:

Product Name	Overall Score
Webroot SecureAnywhere Endpoint Protection	78
Symantec Endpoint Protection 12.1 Small Business	55
ESET NOD32 Antivirus 4 Business	47
Microsoft Forefront Endpoint Protection	46
Kaspersky Endpoint Security 8.0	40
Trend Micro Worry Free Business Security 7.0 Standard	38
McAfee Total Protection for Secure Business	29
Sophos Endpoint Security 10.0	27

Products and Versions

For each security product, we have tested the most current and available version.

Manufacturer	Product Name	Release Year	Product Version	Date Tested
Webroot Software, Inc.	Webroot SecureAnywhere Endpoint Protection	2012	8.0.1.82	Jan-2012
Trend Micro Inc.	Trend Micro Worry Free Business Security 7 Standard	2011	7.0 SP1 Build 2360	Dec 2011
Kaspersky Lab	Kaspersky Endpoint Security 8.0	2011	8.1.0.646	Dec 2011
Sophos	Sophos Endpoint Security 10.0	2011	10	Dec 2011
McAfee, Inc.	McAfee Total Protection for Secure Business	2011	VirusScan, AntiSpyware Enterprise 8.8, ePO 4.6.0	Dec 2011
Symantec Corp	Symantec Endpoint Protection Small Business Edition	2011	12.1.671.4971	Dec 2011
ESET, spol. s r.o.	ESET NOD32 Antivirus 4 Business	2011	4.2.71.2	Dec 2011
Microsoft Corporation	Microsoft Endpoint Protection 2010	2011	2.0.657.0	Dec 2011

Performance Metrics Summary

We have selected a set of objective metrics which provide a comprehensive and realistic indication of the areas in which endpoint protection products may impact system performance for end users. Our metrics test the impact of the software on common tasks that end-users would perform on a daily basis.

All of PassMark Software's test methods can be replicated by third parties using the same environment to obtain similar benchmark results. Detailed descriptions of the methodologies used in our tests are available as "[Appendix 2 – Methodology Description](#)" of this report.

Benchmark 1 – Initial Scan Time

All security solutions have functionality designed to detect viruses and various other forms of malware by scanning files on the system. This metric measured the amount of time required to scan a set of clean files. Our sample file set comprised a total file size of 5.44 GB and was made up of files that would typically be found on end-user machines, such as media files, system files and Microsoft Office documents.

Benchmark 2 – Installation Size

In offering new features and functionality to users, security software products tend to increase in size with each new release. Although new technologies push the size limits of hard drives each year, the growing disk space requirements of common applications and the increasing popularity of large media files (such as movies, photos and music) ensure that a product's installation size will remain of interest to home users.

This metric aims to measure a product's total installation size. This metric is defined as the total disk space consumed by all new files added during a product's installation.

Benchmark 3 – Installation Time

The speed and ease of the installation process will strongly influence the user's first impression of the security software. This test measures the minimum installation time required by the security software to be fully functional and ready for use by the end user. Lower installation times represent security products which are quicker for a user to install.

Benchmark 4 – Boot Time

This metric measures the amount of time taken for the machine to boot into the operating system. Security software is generally launched at Windows startup, adding an additional amount of time and delaying the startup of the operating system. Shorter boot times indicate that the application has had less impact on the normal operation of the machine.

Benchmark 5 – Memory Usage during System Idle

This metric measures the amount of memory (RAM) used by the product while the machine and security software are in an idle state. The total memory usage was calculated by identifying all security software processes and the amount of memory used by each process.

The amount of memory used while the machine is idle provides a good indication of the amount of system resources being consumed by the security software on a permanent basis. Better performing products occupy less memory while the machine is idle.

Benchmark 6 – Memory Usage during Initial Scan

This metric measures the amount of memory (RAM) used by the product during an security scan. The total memory usage was calculated by identifying all endpoint protection software processes and the amount of memory used by each process during an security scan.

Benchmark 7 – Browse Time

It is common behavior for security products to scan data for malware as it is downloaded from the internet or intranet. This behavior may negatively impact browsing speed as products scan web content for malware. This metric measures the time taken to browse a set of popular internet sites to consecutively load from a local server in a user's browser window.

Benchmark 8 – File Copy, Move and Delete

This metric measures the amount of time taken to copy, move and delete a sample set of files. The sample file set contains several types of file formats that a Windows user would encounter in daily use. These formats include documents (e.g. Microsoft Office documents, Adobe PDF, Zip files, etc), media formats (e.g. images, movies and music) and system files (e.g. executables, libraries, etc).

Benchmark 9 – File Compression and Decompression

This metric measures the amount of time taken to compress and decompress different types of files. Files formats used in this test included documents, movies and images.

Benchmark 10 – File Write, Open and Close

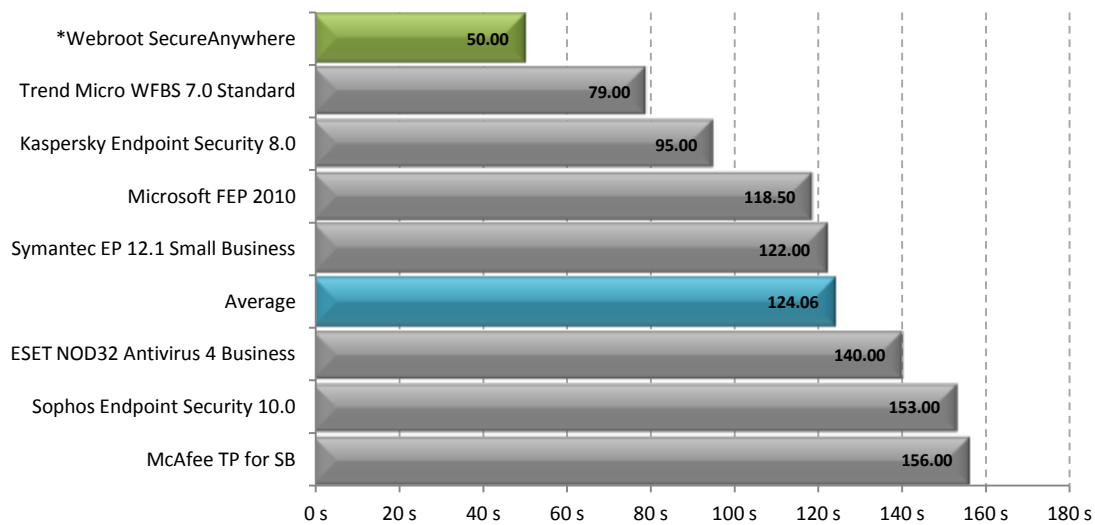
This benchmark was derived from Oli Warner's File I/O test at <http://www.thepcspy.com> (please see *Reference #1: What Really Slows Windows Down*). This metric measures the amount of time taken to write a file, then open and close that file.

Test Results

In the following charts, we have highlighted the results we obtained for Webroot SecureAnywhere Endpoint Protection in green. The average has also been highlighted in blue for ease of comparison.

Benchmark 1 – Initial Scan Time

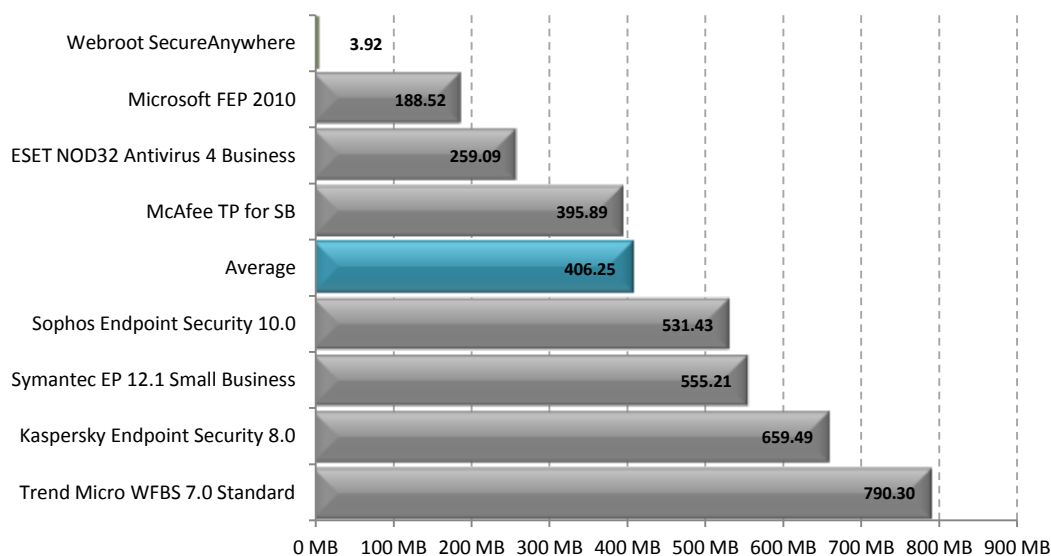
The following chart compares the average time taken to run an initial scan on a set of 8502 files (totaling 5.42 GB) for each Security product tested.



*This test was carried out on build 8.0.1.106 of Webroot SecureAnywhere Endpoint Protection.

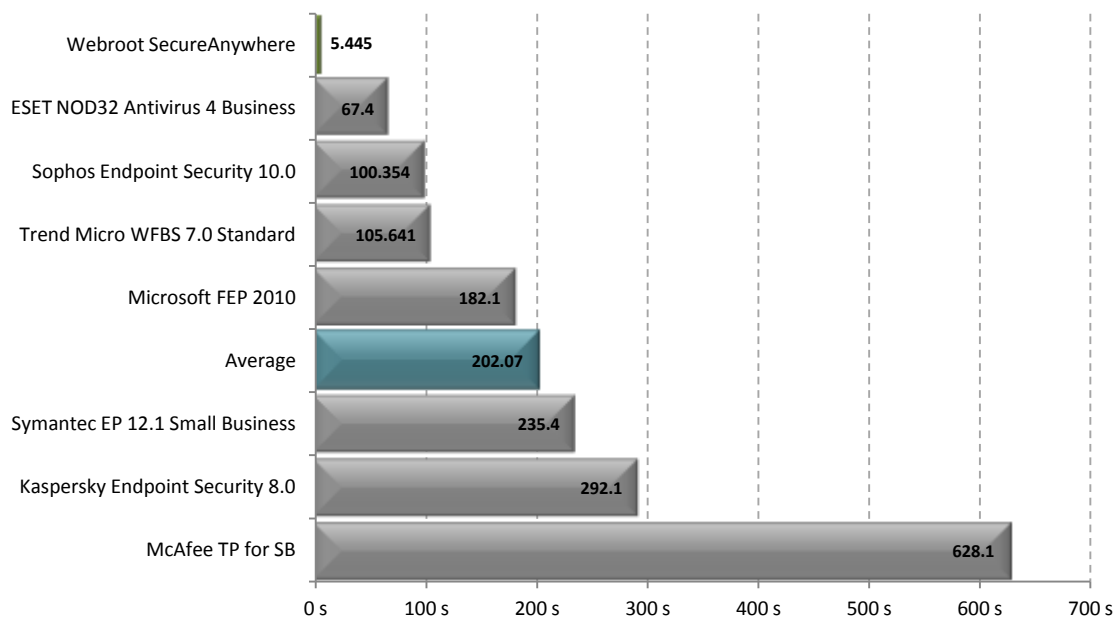
Benchmark 2 – Installation Size

The following chart compares the total size of files added during the installation of Endpoint Security products. Products with lower installation sizes are considered better performing products in this category.



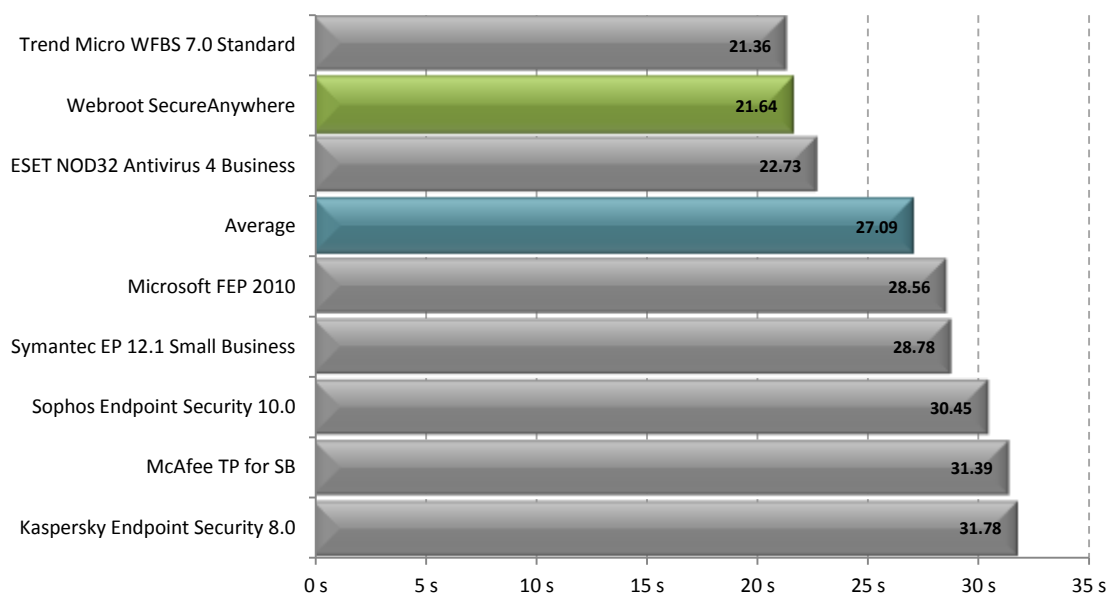
Benchmark 3 – Installation Time

The following chart compares the minimum installation time it takes for Endpoint Security products to be fully functional and ready for use by the end user. Products with lower installation times are considered better performing products in this category.



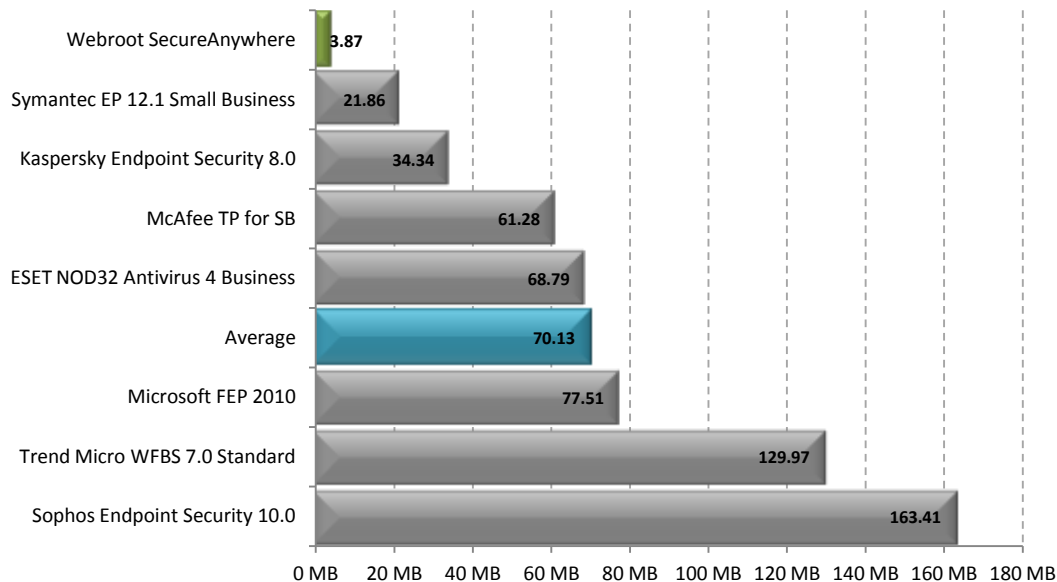
Benchmark 4 – Boot Time

The following chart compares the average time taken for the system to boot (from a sample of five boots) for each Endpoint Security product tested. Products with lower boot times are considered better performing products in this category.



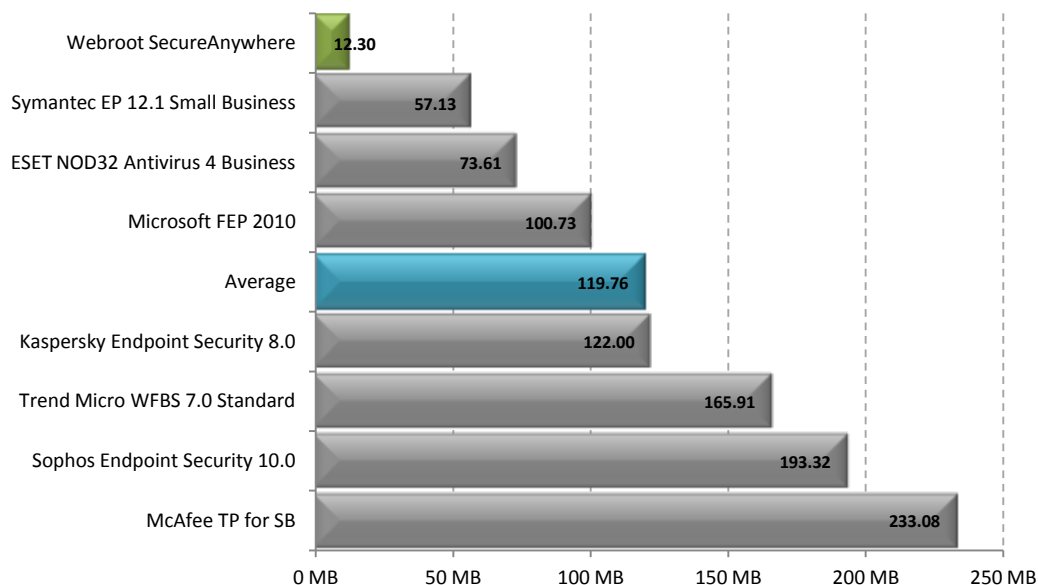
Benchmark 5 – Memory Usage during System Idle

The following chart compares the average amount of RAM in use by an Endpoint Security product during a period of system idle. This average is taken from a sample of ten memory snapshots taken at roughly 60 seconds apart after reboot. Products with lower idle RAM usage are considered better performing products in this category.



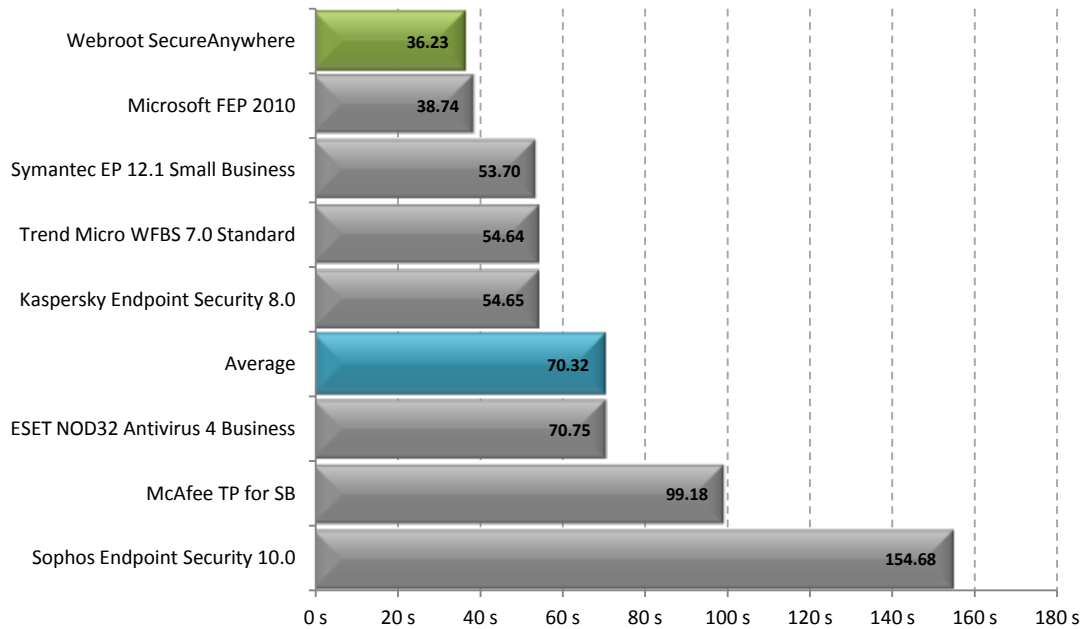
Benchmark 6 – Memory Usage during Initial Scan

The following chart compares the average amount of RAM in use by an Endpoint Security product during an initial scan on the main drive. This average is taken from a sample of ten memory snapshots taken at five second intervals during a scan of sample files which have not been previously scanned by the software. Products that use less memory during a scan are considered better performing products in this category.



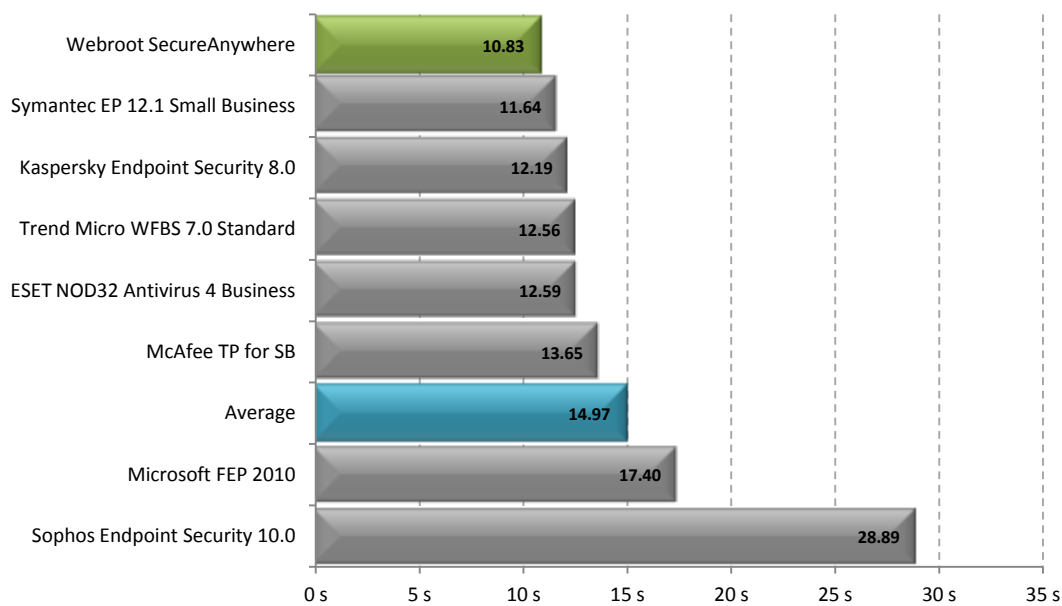
Benchmark 7 – Browse Time

The following chart compares the average time taken for Internet Explorer to successively load a set of popular websites through the local area network from a local server machine. Products with lower browse times are considered better performing products in this category.



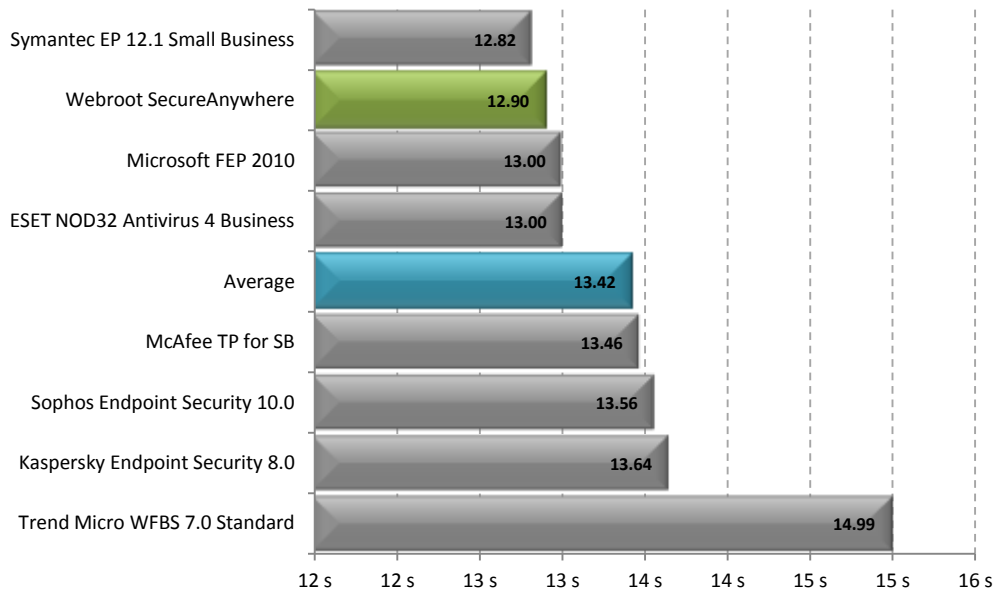
Benchmark 8 – File Copy, Move and Delete

The following chart compares the average time taken to copy, move and delete several sets of sample files for each Endpoint Security product tested. Products with lower times are considered better performing products in this category.



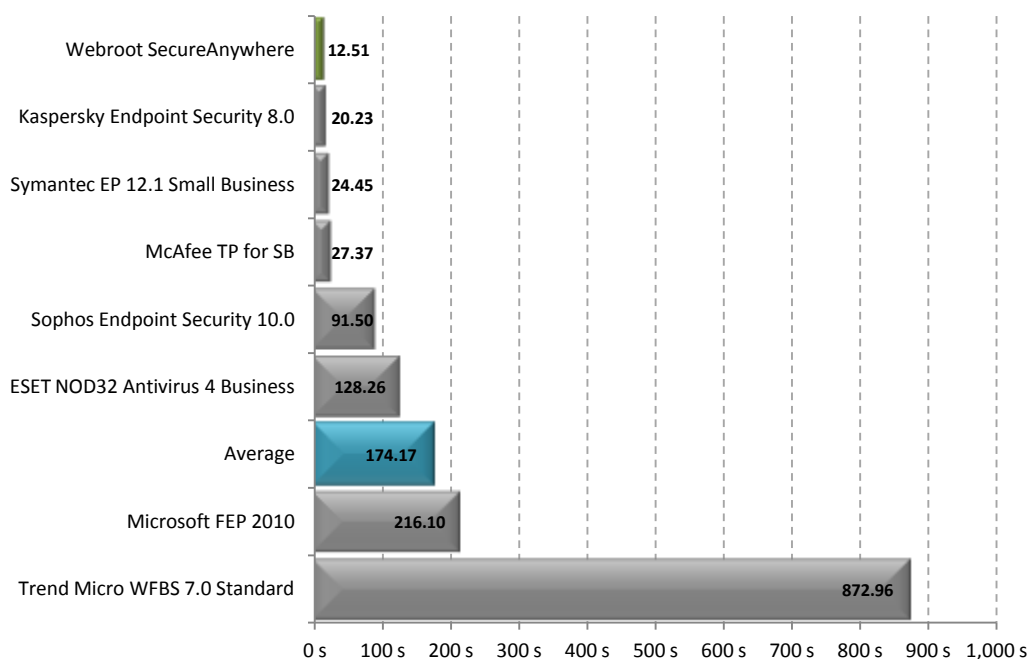
Benchmark 9 – File Compression and Decompression

The following chart compares the average time it takes for sample files to be compressed and decompressed for each Endpoint Security product tested. Products with lower times are considered better performing products in this category.



Benchmark 10 – File Write, Open and Close

The following chart compares the average time it takes for a file to be written to the hard drive then opened and closed 180,000 times, for each Endpoint Security product tested. Products with lower times are considered better performing products in this category.



Disclaimer and Disclosure

This report only covers versions of products that were available at the time of testing. The tested versions are as noted in the "Products and Versions" section of this report. The products we have tested are not an exhaustive list of all products available in these very competitive product categories.

Disclaimer of Liability

While every effort has been made to ensure that the information presented in this report is accurate, PassMark Software Pty Ltd assumes no responsibility for errors, omissions, or out-of-date information and shall not be liable in any manner whatsoever for direct, indirect, incidental, consequential, or punitive damages resulting from the availability of, use of, access of, or inability to use this information.

Disclosure

Webroot Software Inc. funded the production of this report. The list of products tested and the metrics included in the report were selected by Webroot.

Trademarks

All trademarks are the property of their respective owners.

Contact Details

PassMark Software Pty Ltd

Suite 202, Level 2
35 Buckingham St.
Surry Hills, 2010
Sydney, Australia

Phone + 61 (2) 9690 0444

Fax + 61 (2) 9690 0445

Web www.passmark.com

Appendix 1 – Test Environment

Endpoint Machine – Windows 7 (64-bit)

For our testing, PassMark Software used a test environment running Windows 7 Ultimate (64-bit) with the following hardware specifications:

CPU:	Intel Core i5 750 @ 2.66GHz
Video Card:	ATI Radeon 4350 1GB
Motherboard:	ASUS V-P7H55E, LGA1156
RAM:	4GB DDR3 RAM, 1333Mhz
HDD:	Samsung 1.5TB 7200RPM
Network:	Gigabit (1GB/s)

Web Page and File Server – Windows 2008 (32-bit)

The Web and File server was not benchmarked directly, but served the web pages and files to the endpoint machine during performance testing.

CPU:	Pentium 4 3200 MHz
Video Card:	Integrated Video
Motherboard:	Intel D865PERL
RAM:	1GB
HDD:	Seagate ST380023AS 80GB
Network:	Gigabit (1GB/s)

Management Console VM Server – Windows 7 (64-bit)

The server was not benchmarked directly, but was used as the host for Virtual Machines to which enterprise components of software was installed. After installation, the Management Console server was used to deploy endpoint software to clients and to schedule scans.

CPU:	AMD Phenom II x4 940 (Quad Core)
Video Card:	ASUS GeForce 9400GT
Motherboard:	Gigabyte GA-MA790XT-UD4P
RAM:	16GB PC3-10600 1333MHz DDR3 Memory
HDD:	Western Digital Caviar Green WD10EADS 1TB Serial ATA-II
Network:	Gigabit (1GB/s)

Appendix 2 – Methodology Description

Windows 7 Image Creation

As with testing on Windows Vista, *Norton Ghost* was used to create a “clean” baseline image prior to testing. Our aim is to create a baseline image with the smallest possible footprint and reduce the possibility of variation caused by external operating system factors.

The baseline image was restored prior to testing of each different product. This process ensures that we install and test all products on the same, “clean” machine.

The steps taken to create the base Windows 7 image are as follows:

1. Installation and activation of **Windows 7 Ultimate** Edition.
2. Disabled Automatic Updates.
3. Changed User Account Control settings to “Never Notify”.
4. Disable Windows Defender automatic scans to avoid unexpected background activity.
5. Disable the Windows firewall to avoid interference with security software.
6. Installed Norton Ghost for imaging purposes.
7. Disabled *Superfetch* to ensure consistent results.
8. Installed *HTTP Watch* for Browse Time testing.
9. Installed *Windows Performance Toolkit x64* for Boot Time testing.
10. Installed Active Perl for interpretation of some test scripts.
11. Install OSForensics for testing (Installation Size and Registry Key Count tests) purposes.
12. Disabled updates, accelerators and compatibility view updates in Internet Explorer 8.
13. Update to Windows Service Pack 1
14. Created a baseline image using Norton Ghost.

Benchmark 1 – On-Demand Scan Time

On-Demand Scan Time measures the amount time it took for each endpoint product to scan a set of sample files from the right-click context menu in Windows Explorer. The sample used was identical in all cases and contained a mixture of system files and Office files. In total there were 8502 files whose combined size was 5.42 GB. Most of these files come from the Windows system folders. As the file types can influence scanning speed, the breakdown of the main file types, file numbers and total sizes of the files in the sample set is given here.

.avi	247	1024MB	.jpg	2904	318MB	.wma	585	925MB
.dll	773	25MB	.mp3	333	2048MB	.xls	329	126MB
.exe	730	198MB	.png	451	27MB	.zip	14	177MB
.gif	681	63MB	.ppt	97	148MB			
.doc	160	60MB	.sys	501	80MB			
.docx	267	81MB	.wav	430	260MB			

Where possible this scan was run without launching the product’s user interface, by right-clicking the test folder and choosing the “Scan Now” option, though some products required entering the UI to scan a folder. To record the scan time, we have used product’s built-in scan timer or reporting system. Where this was not possible, scan times were taken manually with a stopwatch.

For each product, five samples were taken with the machine rebooted before each sample to clear any caching effects by the operating systems. Our final result was calculated as an average of five scans, with each scan having equal weighting.

Benchmark 2 – Installation Size

A product's Installation Size was previously defined as the difference between the initial snapshot of the Disk Space (C: drive) before installation and the subsequent snapshot taken after the product is installed on the system. Although this is a widely used methodology, we noticed that the results it yielded were not always reproducible in Vista due to random OS operations that may take place between the two snapshots. We improved the Installation Size methodology by removing as many Operating System and disk space variables as possible.

Using PassMark's **OSForensics** we created initial and post-installation disk signatures for each product. These disk signatures recorded the amount of files and directories, and complete details of all files on that drive (including file name, file size, checksum, etc) at the time the signature was taken.

The initial disk signature was taken immediately prior to installation of the product. A subsequent disk signature was taken immediately following a system reboot after product installation. Using **OSForensics**, we compared the two signatures and calculated the total disk space consumed by files that were new, modified, and deleted during product installation. Our result for this metric reflects the total size of all newly added files during installation.

The scope of this metric includes only an 'out of the box' installation size for each product. Our result does not cover the size of files downloaded by the product after its installation (such as engine or signature updates), or any files created by system restore points, pre-fetch files and other temporary files.

Benchmark 3 – Installation Time

This test measures the minimum Installation Time a product requires to be fully functional and ready for use by the end user. Installation time can usually be divided in three major phases:

- The **Extraction and Setup phase** consists of file extraction, the EULA prompt, product activation and user configurable options for installation.
- The **File Copy phase** occurs when the product is being installed; usually this phase is indicated by a progress bar.
- The **Post-Installation phase** is any part of the installation that occurs after the File Copy phase. This phase varies widely between products; the time recorded in this phase may include a required reboot to finalize the installation or include the time the program takes to become idle in the system tray.

To reduce the impact of disk drive variables, each product was copied to the Desktop before initializing installation. Each step of the installation process was manually timed with a stopwatch and recorded in as much detail as possible. Where input was required by the end user, the stopwatch was paused and the input noted in the raw results in parenthesis after the phase description.

Where possible, all requests by products to pre-scan or post-install scan were declined or skipped. Where it was not possible to skip a scan, the time to scan was included as part of the installation time. Where an optional component of the installation formed a reasonable part of the functionality of the software, it was also installed (e.g. website link checking software as part of an Security Product).

Installation time includes the time taken by the product installer to download components required in the installation. This may include mandatory updates or the delivery of the application itself from a download manager. We have noted in our results where a product has downloaded components for product installation.

We have excluded product activation times due to network variability in contacting vendor servers or time taken in account creation.

Benchmark 4 – Boot Time

PassMark Software uses tools available from the [Windows Performance Toolkit version 4.6](#) (as part of the Microsoft Windows 7 SDK obtainable from the [Microsoft Website](#)) with a view to obtaining more precise and consistent boot time results on the Windows 7 platform.

The boot process is first optimized with `xbootmgr.exe` using the command "`xbootmgr.exe -trace boot -prepSystem`" which prepares the system for the test over six optimization boots. The boot traces obtained from the optimization process are discarded.

After boot optimization, the benchmark is conducted using the command "`xbootmgr.exe -trace boot -numruns 5`". This command boots the system five times in succession, taking detailed boot traces for each boot cycle.

Finally, a post-processing tool was used to parse the boot traces and obtain the `BootTimeViaPostBoot` value. This value reflects the amount of time it takes the system to complete all (and only) boot time processes. Our final result is an average of five boot traces.

Benchmark 5 – Memory Usage during System Idle

The `Perflog++` utility was used to record process memory usage on the system at boot, and then every minute for another fifteen minutes after. This was done only once per product and resulted in a total of 15 samples. The first sample taken at boot is discarded.

The `PerfLog++` utility records memory usage of all processes, not just those of the anti-malware product. As a result of this, an anti-malware product's processes needed to be isolated from all other running system processes. To isolate relevant process, we used a program called `Process Explorer` which was run immediately upon the completion of memory usage logging by `PerfLog++`. `Process Explorer` is a Microsoft Windows Sysinternals software tool which shows a list of all DLL processes currently loaded on the system.

Benchmark 6 – Memory Usage during Initial Scan

The `PerfLog++` utility was used to record memory usage on the system while a malware scan is in progress. Please refer to the metric "`Memory usage – System Idle`" above for a description of the `PerfLog++` utility and an explanation of the method by which memory usage is calculated.

As some products cache scan locations, we take reasonable precautions to ensure that the security software does not scan the C:\ drive at any point before conducting this test. A manual scan on the C:\ drive is initiated at

the same time as the *PerfLog++* utility, enabling *PerfLog++* to record memory usage for 60 seconds at five second intervals.

Benchmark 7 – Browse Time

We used a script in conjunction with *HTTPWatch (Basic Edition, version 6.1)* to record the amount of time it takes for a set of 106 ‘popular’ websites to load consecutively from a local server. This script feeds a list of URLs into *HTTPWatch*, which instructs the browser to load pages in sequence and monitors the amount of time it takes for the browser to load all items on one page.

For this test, we have used *Internet Explorer 8 (Version 8.0.6001.18783)* as our browser.

The set of websites used in this test include front pages of high traffic pages. This includes shopping, social, news, finance and reference websites.

The Browse Time test is executed five times and our final result is an average of these five samples. The local server is restarted between different products and one initial ‘test’ run is conducted prior to testing to install *Adobe Flash Player*, an add-on which is used by many popular websites.

Benchmarks 8-10 – Real-Time Performance

We used a single script in testing Benchmarks 8-10. The script consecutively executes tests for Benchmarks 8-10. The script times each phase in these benchmarks using *CommandTimer.exe* and appends results to a log file.

Benchmarks 8 – File Copy, Move and Delete

This test measures the amount of time required for the system to copy, move and delete samples of files in various file formats. This sample was made up of 812 files over 760,867,636 bytes and can be categorized as documents [26% of total], media files [54% of total] and PE files (i.e. System Files) [20% of total].

The breakdown of the main file types, file numbers and total sizes of the files in the sample set is shown in the following table:

File format	Number	Size (bytes)
DOC	8	30,450,176
DOCX	4	13,522,409
PPT	3	5,769,216
PPTX	3	4,146,421
XLS	4	2,660,352
XLSX	4	1,426,054
PDF	73	136,298,049
ZIP	4	6,295,987
7Z	1	92,238
JPG	351	31,375,259
GIF	6	148,182
MOV	7	57,360,371

RM	1	5,658,646
AVI	8	78,703,408
WMV	5	46,126,167
MP3	28	191,580,387
EXE	19	2,952,914
DLL	104	29,261,568
AX	1	18,432
CPL	2	2,109,440
CPX	2	4,384
DRV	10	154,864
ICO	1	107,620
MSC	1	41,587
NT	1	1,688
ROM	2	36,611
SCR	2	2,250,240
SYS	1	37,528,093
TLB	3	135,580
TSK	1	1,152
UCE	1	22,984
EXE	19	2,952,914
DLL	104	29,261,568
AX	1	18,432
CPL	2	2,109,440
CPX	2	4,384
DRV	10	154,864
ICO	1	107,620
MSC	1	41,587
NT	1	1,688
ROM	2	36,611
SCR	2	2,250,240
SYS	1	37,528,093
TLB	3	135,580
TSK	1	1,152
UCE	1	22,984
Total	812	760,867,636

This test was conducted five times to obtain the average time to copy, move and delete the sample files, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 9 – File Compression and Decompression

This test measured the amount of time required to compress and decompress a sample set of files. For this test, we used a subset of the media and documents files used in the *File Copy, Move and Delete* benchmark. *CommandTimer.exe* recorded the amount of time required for *7zip.exe* to compress the files into a *.zip and subsequently decompress the created *.zip file.

This subset comprised 1,218 files over 783 MB. The breakdown of the file types, file numbers and total sizes of the files in the sample set is shown in the following table:

File Type	File Number	Total Size
.xls	13	9.23 MB
.xlsx	9	3.51 MB
.ppt	9	7.37 MB
.pptx	11	17.4 MB
.doc	17	35.9 MB
.docx	19	24.5 MB
.gif	177	1.10 MB
.jpg	737	66.2 MB
.png	159	48.9 MB
.mov	7	54.7 MB
.rm	1	5.39 MB
.avi	46	459 MB
.wma	11	48.6 MB
.avi	46	459 MB
.wma	11	48.6 MB
Total	1218	783 MB

This test was conducted five times to obtain the average file compression and decompression speed, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 10 – File Write, Open and Close

This benchmark was derived from Oli Warner's File I/O test at <http://www.thepcspy.com> (please see *Reference #1: What Really Slows Windows Down*).

For this test, we developed *OpenClose.exe*, an application that looped writing a small file to disk, then opening and closing that file. *CommandTimer.exe* was used to time how long the process took to complete 180,000 cycles.

This test was conducted five times to obtain the average file writing, opening and closing speed, with the test machine rebooted between each sample to remove potential caching effects.