PASSMARK® SOFTWARE

Symantec Endpoint Protection vs. Windows Defender

Performance Benchmarks

Windows 8

July 2014

Document: Endpoint Protection 2014 - Performance Testing - SEP vs Defender - Edition 2.docx
Authors: M. Baquiran, D. Wren
Company: PassMark Software
Date: 24 July 2014
Edition: 1

Table of Contents

Revision History

Rev	Revision History	Date
Edition 1	Initial version of this report.	13 February 2014
Edition 2	Updated with results for a newer version of Symantec Endpoint Protection.	2 July 2014

References

Ref #	Document	Author	Date
1	**What Really Slows Windows Down** (URL)	O. Warner, The PC Spy	2001-2014

Executive Summary

PassMark Software® conducted objective performance testing on Windows Defender and Symantec Endpoint Protection, on Windows 8 during February and July 2014. This report presents our results from these performance tests.

Benchmarking was performed using thirteen performance metrics to assess product performance and system impact on the endpoint or client machine. The metrics which were used in testing are as follows:

- Word Document Launch and Open Time;
- Internet Explorer Launch Time;
- On-Demand Scan Time;
- CPU Usage during Scan;
- Browse Time;
- File Copy, Move and Delete;
- Network Throughput;
- File Compression and Decompression;
- File Write, Open and Close;
- Memory Usage during System Idle;
- Memory Usage during Scan;
- CPU Usage during System Idle; and
- Boot Time.

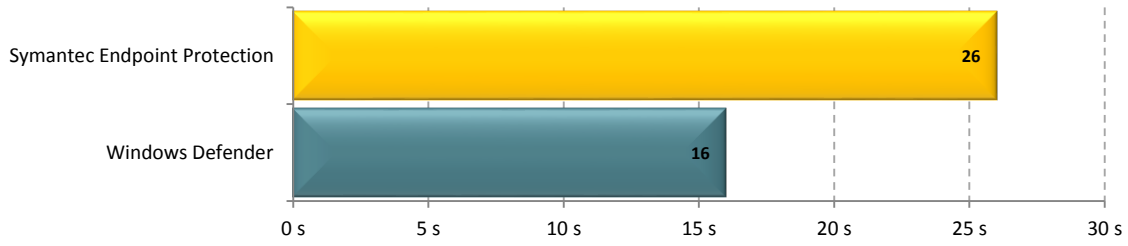
Score and Rank

PassMark Software assigned each product a score depending on its ranking in each metric. Each product has scored points based on its rank out of the number of products tested in each category. The following table shows how rank in a metric relates to its attained score in a category with two (2) products:

Test Rank	Points Scored
1	2
2	1

We added the scores attained from each metric for each product to obtain the overall score and rank. For a hypothetical product which achieves first rank in every metric, the highest possible score attainable in testing is 26. The following table shows the overall score and result attained by each product from our testing in order of rank:

Overall Score



Products and Versions

Windows 8 Security products:

Manufacturer	Product Name	Date Tested	Product Version
Symantec Corp	Symantec Endpoint Protection 12.1	Jul 2014	12.1.5013.5000
Microsoft Corp	Windows Defender	Feb 2014	4.3.215.0

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 – Word Document Launch and Open Time

This metric measures how much security software impacts on the responsiveness and performance of the endpoint system. Microsoft Word was chosen for this test because office software is commonly found on business computers. To test a product's performance in this metric, we measured the amount of time taken to launch a large, mixed media document from Microsoft Word. To allow for caching effects by the operating system, both the initial launch time and the subsequent launch times were measured. Our final result is an average of these two measurements.

Benchmark 2 – Internet Explorer Launch Time

Similar to the Word Document Launch and Open Time metric, this metric is one of many methods to objectively measure how much a product impacts on the responsiveness of the system. This metric measures the amount of time it takes to launch the user interface of Internet Explorer 8. To allow for caching effects by the operating system, both the initial launch time and the subsequent launch times were measured. Our final result is an average of these two measurements.

Benchmark 3 – On-Demand Scan Time

All endpoint protection 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 5.42 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 4 –CPU Usage during Scan

The amount of load on the CPU while security software conducts a malware scan may prevent the reasonable use of the endpoint machine until the scan has completed. This metric measured the percentage of CPU used by endpoint protection software when performing a scan.

Benchmark 5 – Browse Time

It is common behaviour for security products to scan data for malware as it is downloaded from the internet or intranet. This behaviour 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 6 – File Copy, Move and Delete

This metric measures the amount of time taken to move, copy 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 7 – Network Throughput

The metric measures the amount of time taken to download a variety of files from a local server using the HyperText Transfer Protocol (HTTP), which is the main protocol used on the web for browsing, linking and data transfer. Files used in this test include file formats that users would typically download from the web, such as images, archives, music files and movie files.

Benchmark 8 – 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 9 – 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.

Benchmark 10 – Memory Usage during System Idle

The amount of memory used while the machine is idle provides a good indication of the amount of system resources being consumed by the endpoint protection software on a permanent basis. This metric measures the amount of memory (RAM) used by the product while the machine and endpoint protection software are in an idle state. The total memory usage was calculated by identifying all endpoint protection software processes and the amount of memory used by each process.

Benchmark 11 – Memory Usage during Scan

This metric measures the amount of memory (RAM) used by the product during an antivirus 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 antivirus scan.

Benchmark 12– CPU Usage during System Idle

This metric measures the average amount of load placed on the CPU during system idle by the security software.

Benchmark 16 – Boot Time

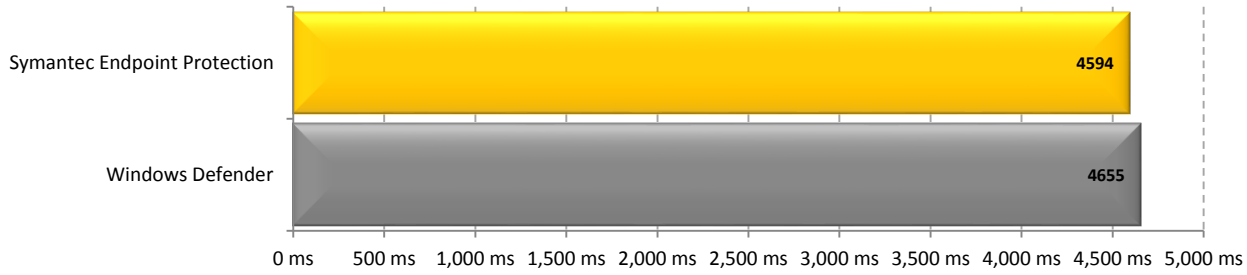
This metric measures the amount of time taken for the machine to boot into the operating system. Security software is generally launched at Windows startup, adding an additional amount of time and delaying the startup of the operating system. Shorter boot times indicate that the application has had less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

Windows Defender vs. Symantec Endpoint Protection – Test Results

In the following charts, we have highlighted the results we obtained for Symantec Endpoint Protection in yellow. The average has also been highlighted in grey for ease of comparison.

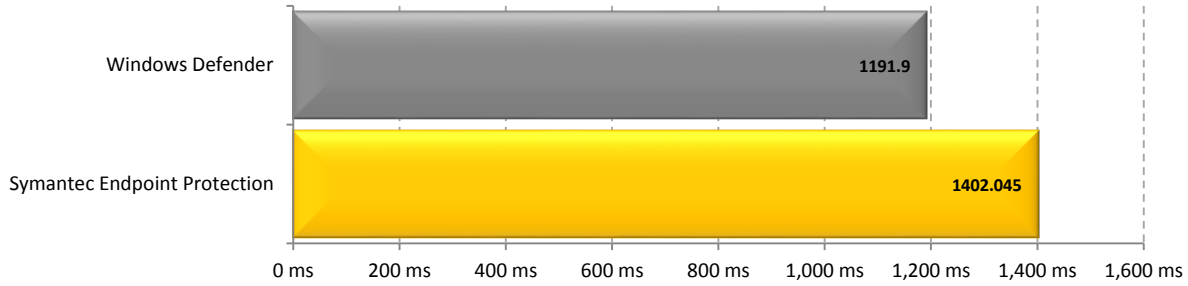
Benchmark 1 – Word Document Launch and Open Time (milliseconds)

The following chart compares the average time taken to launch Microsoft Word and open a 10MB document. Products with lower launch times are considered better performing products in this category.



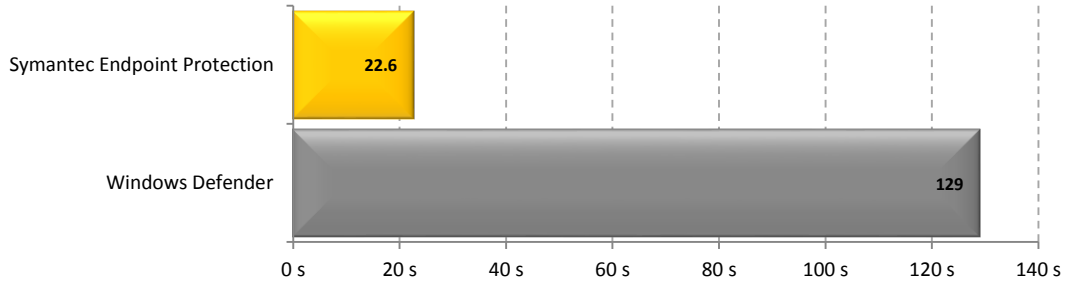
Benchmark 2 – Internet Explorer Launch Time (milliseconds)

The following chart compares the average time taken for Internet Explorer to successively load. Products with lower load times are considered better performing products in this category.



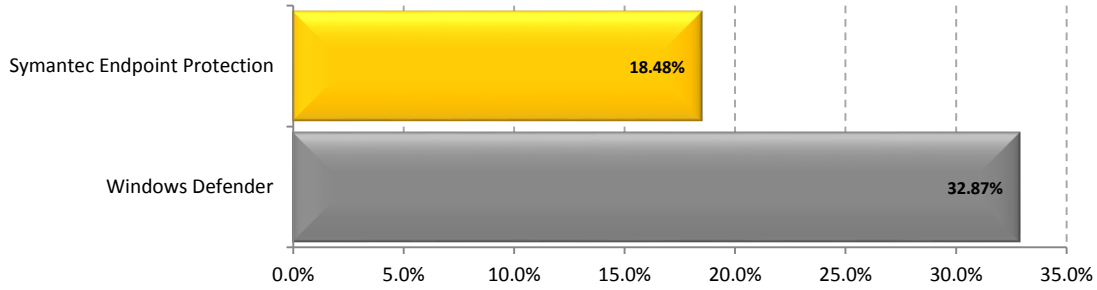
Benchmark 3 – On-Demand Scan Time (seconds)

The following chart compares the average time taken to scan a set of media files, system files and Microsoft Office documents that totaled 5.42 GB. Our final result is calculated as an average of five scans, with each scan having equal weighting. Products with lower scan times are considered better performing products in this category.



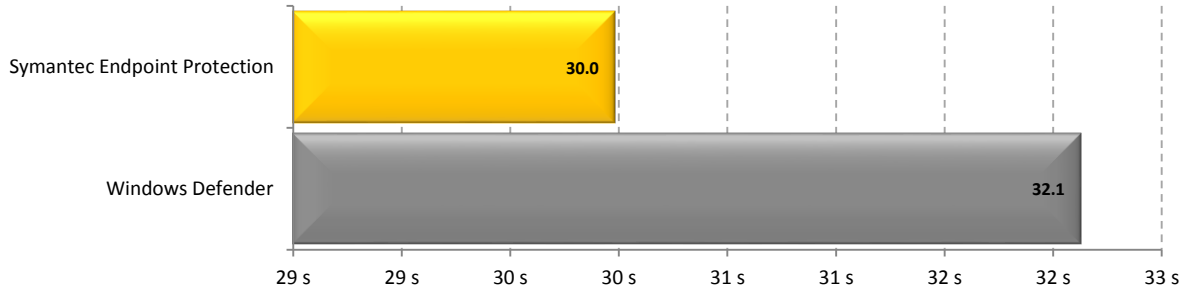
Benchmark 4 – CPU Usage during Scan Time (percent)

The following chart compares the average CPU usage during a scan of a set of media files, system files and Microsoft Office documents that totaled 5.42 GB. Products with lower CPU usage are considered better performing products in this category.



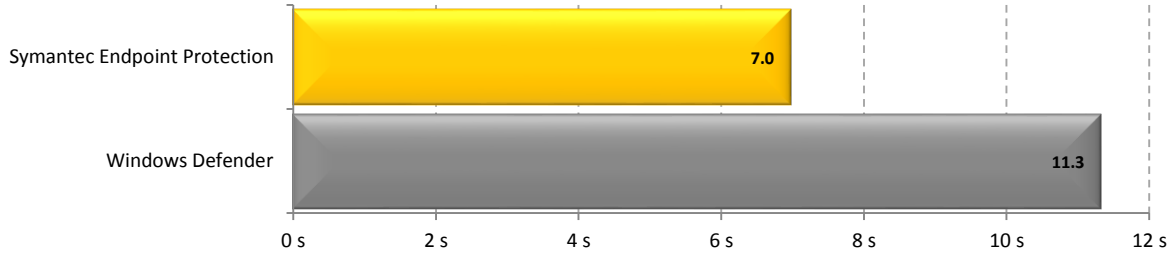
Benchmark 5 – Browse Time (percent)

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.



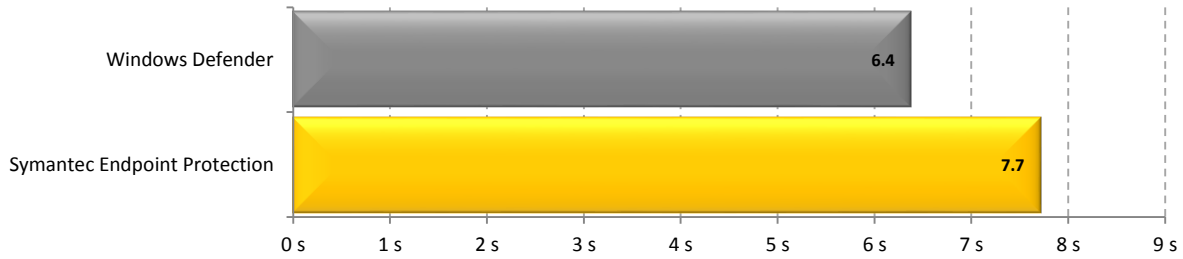
Benchmark 6 – File Copy, Move and Delete (seconds)

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



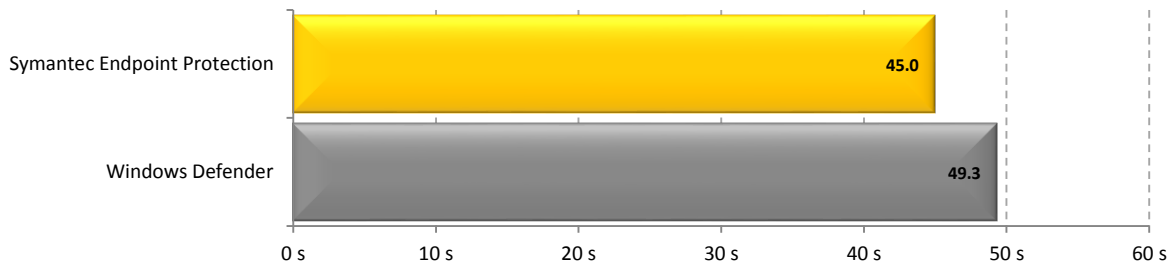
Benchmark 7 – Network Throughput (seconds)

The following chart compares the average time to download a sample set of common file types for each product tested. Products with lower times are considered better performing products in this category.



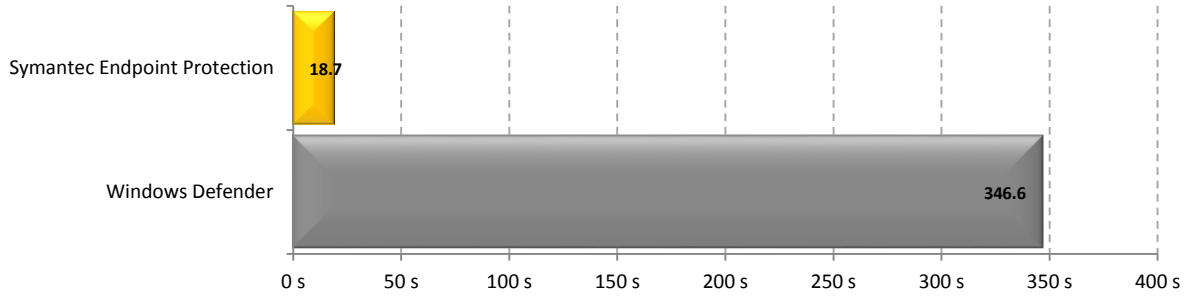
Benchmark 8 – File Compression and Decompression (seconds)

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



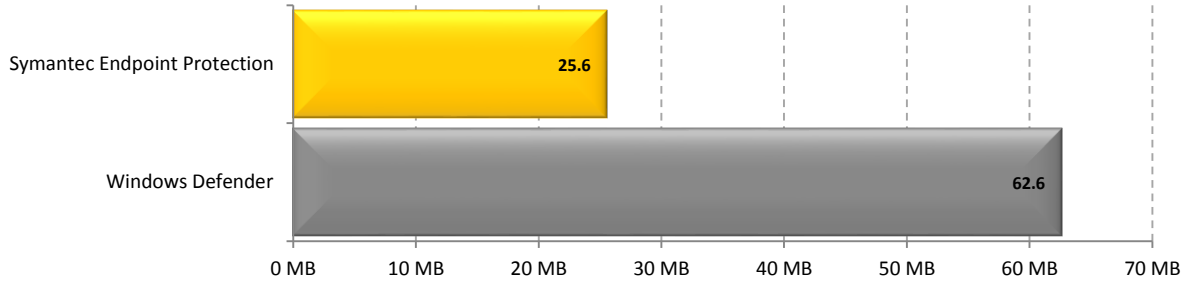
Benchmark 9 – File Write, Open and Close (seconds)

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 Internet Security product tested. Products with lower times are considered better performing products in this category.



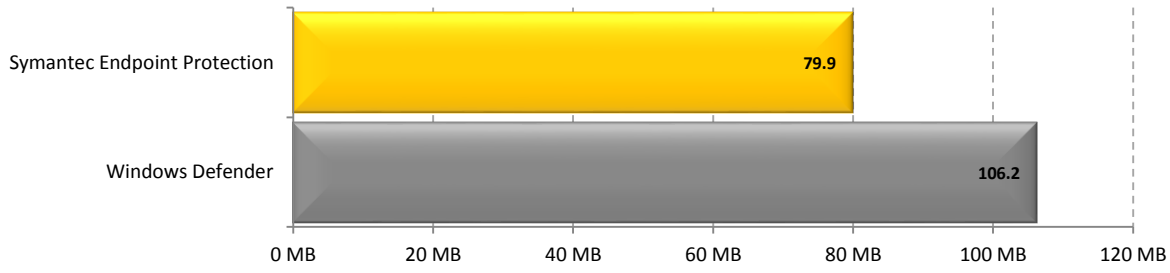
Benchmark 10 – Memory Usage during System Idle (megabytes)

The following chart compares the average amount of RAM in use by each 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 that use less memory during idle are considered better performing products in this category.



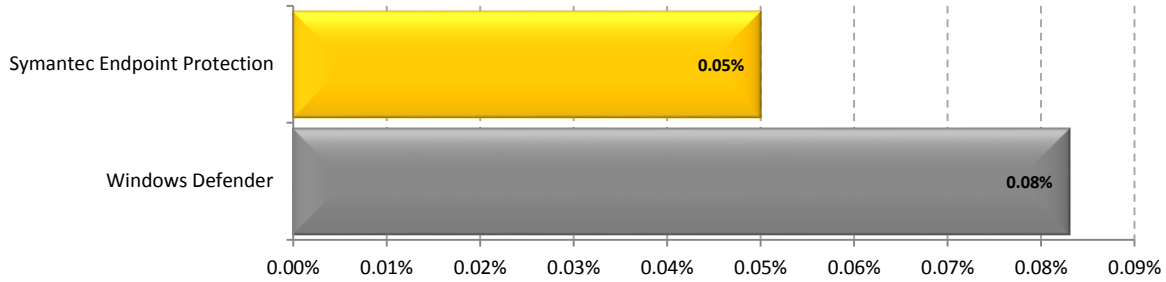
Benchmark 11 – Memory Usage during Scan (megabytes)

The following chart compares the average amount of RAM in use by each product during an antivirus scan. 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.



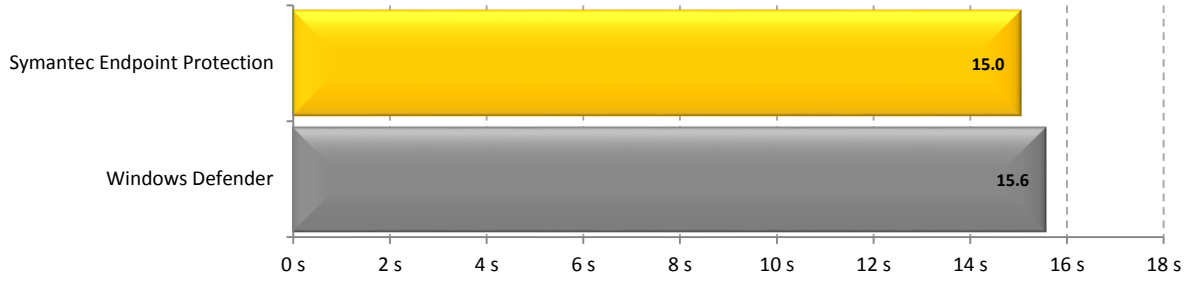
Benchmark 12 – CPU Usage during System Idle (percent)

The following chart compares the average CPU usage during system idle. Products with lower CPU usage are considered better performing products in this category.



Benchmark 13 –Boot Time (seconds)

The following chart compares the average time taken for the system to boot (from a sample of five boots) for each product tested. Products with lower boot 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 the competitive enterprise security market.

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

Symantec Corporation funded the production of this report, selected the test metrics, and supplied some of the test scripts used for the tests.

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 8 (64-bit)

For our testing, PassMark Software used a test environment running Windows 8 (64-bit) with the following hardware specifications:

Model:	HP Pavilion P6-2300A
CPU:	Intel Core i5 750 @ 2.66GHz
Video Card:	1GB nVIDIA GeForce GT 620M
Motherboard:	Foxconn 2ABF 3.10
RAM:	6GB DDR3 RAM
HDD:	Hitachi HDS721010CLA630
	Split into 2 partitions, the boot drive and the test data drive
Network:	Gigabit (1GB/s)
Video:	1GB nVIDIA GeForce GT 620M

Web Page and File Server – Windows 2012 (64-bit)

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

Model:	Generic Hardware
CPU:	Intel Xeon E3-1220v2 CPU
Video Card:	Kingston 8GB (2 x 4GB ECC RAM)
Motherboard:	Intel S1200BTL Server
RAM:	Kingston 8GB (2 x 4GB) ECC RAM, 1333Mhz
SSD:	OCZ 128GB 2.5” Solid State Disk
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.

Model:	Generic Hardware
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

Benchmark 1 – Word Document Launch and Open Time

The average launch time of Word interface was taken using ***AppTimer*** *(v1.0.1008)*. This includes the time to launch the Word 2013 (15.0.4420.1017) application and open a 10MB document. This test was practically identical to the User Interface launch time test. For each product tested, we obtained a total of fifteen samples from five sets of three Word launches, with a reboot before each set to clear caching effects by the operating system. When compiling the results the first of each set was separated out so that there was a set of values for the initial launch after reboot and a set for subsequent launches.

We have averaged the subsequent launch times to obtain an average subsequent launch time. Our final result for this test is an average of the subsequent launch average and the initial launch time.

AppTimer is publically available from the PassMark Website.

Benchmark 2 – Internet Explorer Launch Time

The average launch time of Internet Explorer interface was taken using ***AppTimer***. For each product tested, we obtained a total of fifteen samples from five sets of three Internet Explorer launches, with a reboot before each set to clear caching effects by the operating system. When compiling the results the first of each set was separated out so that there was a set of values for the initial launch after reboot and a set for subsequent launches.

For this test, we have used ***Internet Explorer 10*** (Version 10.0.12) as our test browser.

We have averaged the subsequent launch times to obtain an average subsequent launch time. Our final result for this test is an average of the subsequent launch average and the initial launch time.

Benchmark 3 – 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 4 – CPU Usage during Scan

CPUAvg is a command-line tool which samples the amount of CPU load approximately two times per second. From this, ***CPUAvg*** calculates and displays the average CPU load for the interval of time for which it has been active.

For this metric, ***CPUAvg*** was used to measure the CPU load on average (as a percentage) by the system while the Scan Time test was being conducted. The final result was calculated as an average five sets of thirty CPU load samples.

Benchmark 5 – 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

Benchmarks 6 – 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 809 files over 683,410,115 bytes and can be categorized as documents [28% of total], media files [60% of total] and PE files (i.e. System Files) [12% of total].

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 7 – Network Throughput

This benchmark measured how much time was required to download a sample set of binary files of various sizes and types over a 100MB/s network connection. The files were hosted on a server machine running Windows Server 2012 and IIS 7. ***CommandTimer.exe*** was used in conjunction with ***GNU Wget*** (version 1.10.1) to time and conduct the download test.

The complete sample set of files was made up of 553,638,694 bytes over 484 files and two file type categories: media files [74% of total] and documents [26% of total].

This test was conducted five times to obtain the average time to download this sample of files, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 8 – 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 404 files over 277,346,661 bytes. 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 format	Category	Number	Size (bytes)
DOC	Documents	8	30,450,176
DOCX	Documents	4	13,522,409
PPT	Documents	3	5,769,216
PPTX	Documents	3	4,146,421
XLS	Documents	4	2,660,352
XLSX	Documents	4	1,426,054
JPG	Media	351	31,375,259
GIF	Media	6	148,182
MOV	Media	7	57,360,371
RM	Media	1	5,658,646
AVI	Media	8	78,703,408
WMV	Media	5	46,126,167
	Total	**404**	**277,346,661**

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 9 – 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.

Benchmark 10 – 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.

Our final result is calculated as the total sum of Private Bytes used by each process belonging to the endpoint security software.

Benchmark 11 – Memory Usage during 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 antivirus 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.

Our final result is calculated as the total sum of Private Bytes used by each process belonging to the endpoint security software during the malware scan.

Benchmark 12 – CPU Usage during System Idle

CPUAvg is a command-line tool which samples the amount of CPU load two times per second. From this, ***CPUAvg*** calculates and displays the average CPU load for the interval of time for which it has been active.

For this metric, ***CPUAvg*** was used to measure the CPU load on average (as a percentage) during a period of system idle for five minutes. This test is conducted after restarting the endpoint machine and after five minutes of machine idle.

Benchmark 16 – Boot Time

PassMark Software uses tools available from the ***Windows Performance Toolkit*** (as part of the Microsoft Windows 8 ADK obtainable from the Microsoft Website).

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.