PASSMARK® SOFTWARE

SentinelOne® Endpoint Protection Platform vs. Seven Competitors

(August 2017)

Windows 10

Performance Benchmark

Document: SentinelOne vs. Seven Competitors (August 2017)
Authors: M. Baquiran, D. Wren
Company: PassMark Software
Date: 8 August 2017
File: SentinelOne_EPP_vs_competitors_2017_Edition_1.docx
Edition 1

Table of Contents

Revision History

Rev	Revision History	Date
Edition 1	Initial version of this report.	8 August 2017

References

Ref #	Document	Author	Date
1	**What Really Slows Windows Down** (URL)	O. Warner, The PC Spy	2001-2017

Executive Summary

PassMark Software® conducted objective performance testing on eight (8) security software products, on Windows 10 (64-bit) between March and July 2017. 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 SentinelOne EPP (Endpoint Protection Platform) with seven (7) competitor products.

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

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

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 has been normalized to 100. This would be the score given if a product attained first place in all ten (10) metrics. Endpoint products have been ranked by their overall scores:

Product Name	Overall Score
SentinelOne Endpoint Protection Platform	76
Trend Micro Worry-Free Business Security Advanced	58
ESET Endpoint Security	56
Bitdefender GravityZone Business Security	56
Kaspersky Small Office Security	55
Symantec Endpoint Protection Cloud	51
Sophos Endpoint Protection	50
Malwarebytes Endpoint Security	48

Products and Versions

For each security product, we have tested the most current and publicly available version. The names and versions of products are given below:

Manufacturer	Product Name	Product Version	Date Tested
SentinelOne	SentinelOne	1.8.4.3694	July 2017
Trend Micro Inc.	Trend Micro Worry Free Business Security Advanced	19.0.2166	April 2017
Kaspersky Lab	Kaspersky Small Office Security	17.0.0.611 (d)	March 2017
Sophos	Sophos Endpoint Protection	Endpoint Security and Control 10.7	April 2017
Bitdefender	Bitdefender GravityZone Business Security	6.2.18.884	April 2017
Symantec Corp	Symantec Endpoint Protection Cloud	22.9.1.12	April 2017
ESET, spol. s r.o.	ESET Endpoint Security	6.5.2094.0	April 2017
Malwarebytes	Malwarebytes Endpoint Security	Anti-Malware (Corporate) 1.80.2.1012 Anti-Ransomware 0.9.17.689	April 2017

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 – 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 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 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 – 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 4 – CPU 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 security software on a permanent basis. 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 the security software's processes and the amount of memory used by each process.

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 – 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 7 – 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 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 – Network Throughput

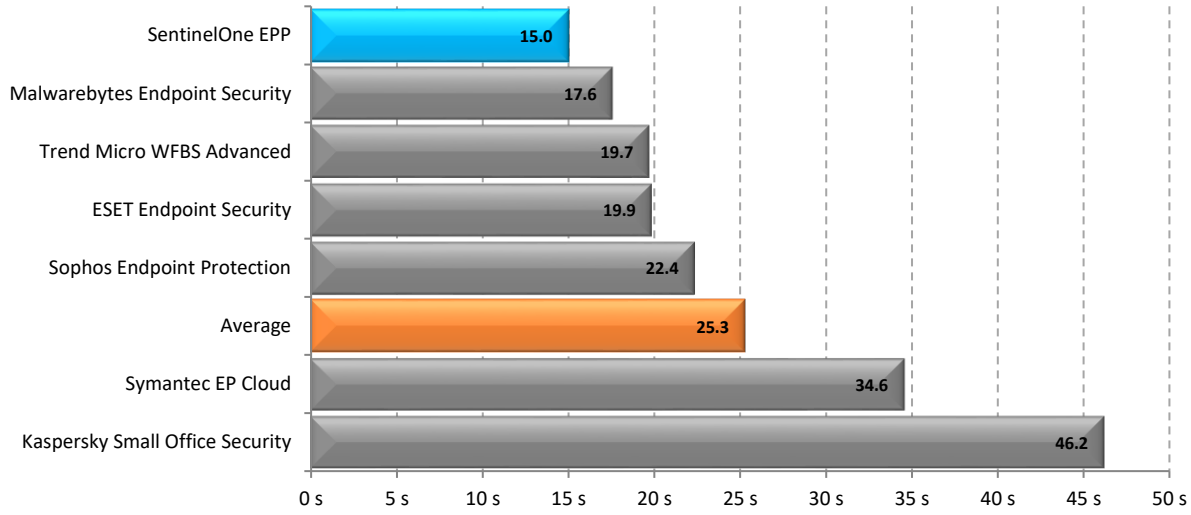
The metric measures the amount of time taken to download a variety of files from a local server using the HyperText Transfer Protocol (HTTP), which is the main protocol used on the web for browsing, linking and data transfer. Files used in this test include file formats that users would typically download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

Test Results

In the following charts, we have highlighted the results we obtained for SentinelOne EPP in blue. The competitor average has also been highlighted in orange for ease of comparison.

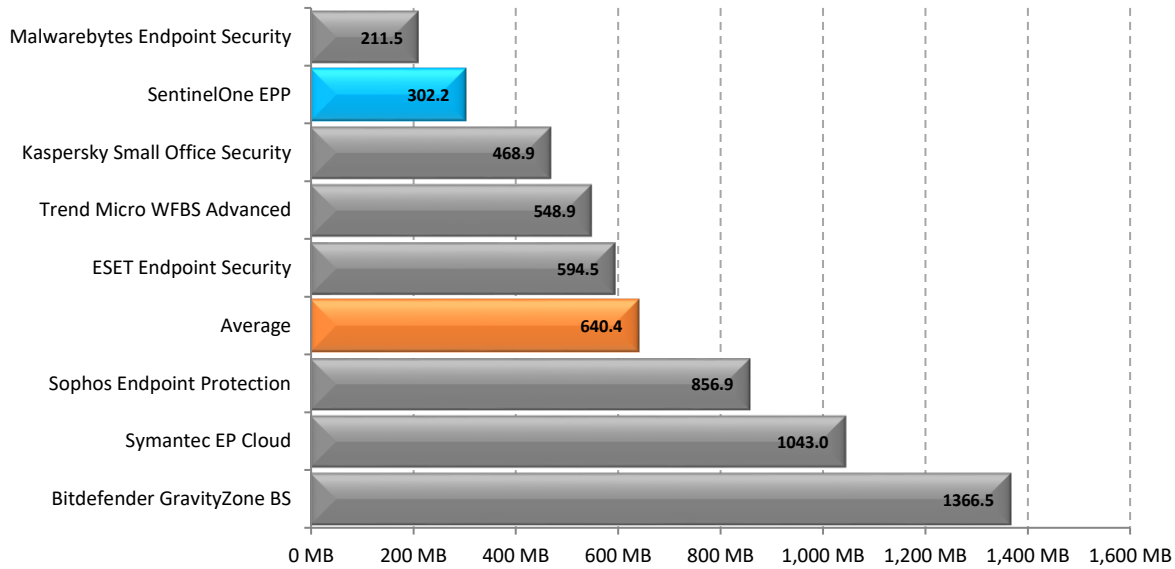
Benchmark 1 – Installation Time

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.



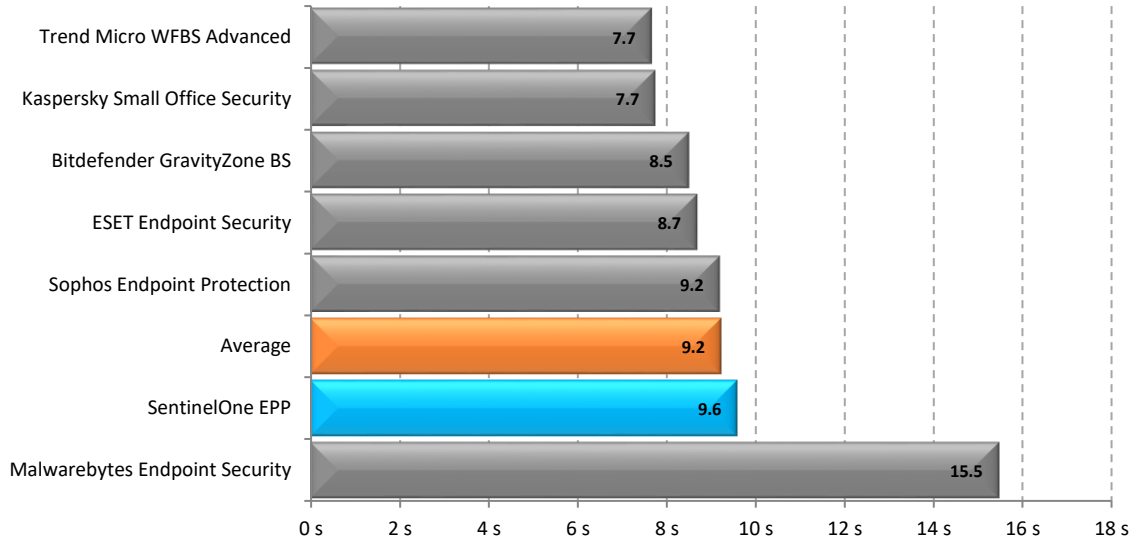
Benchmark 2 – Installation Size

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 – Boot Time

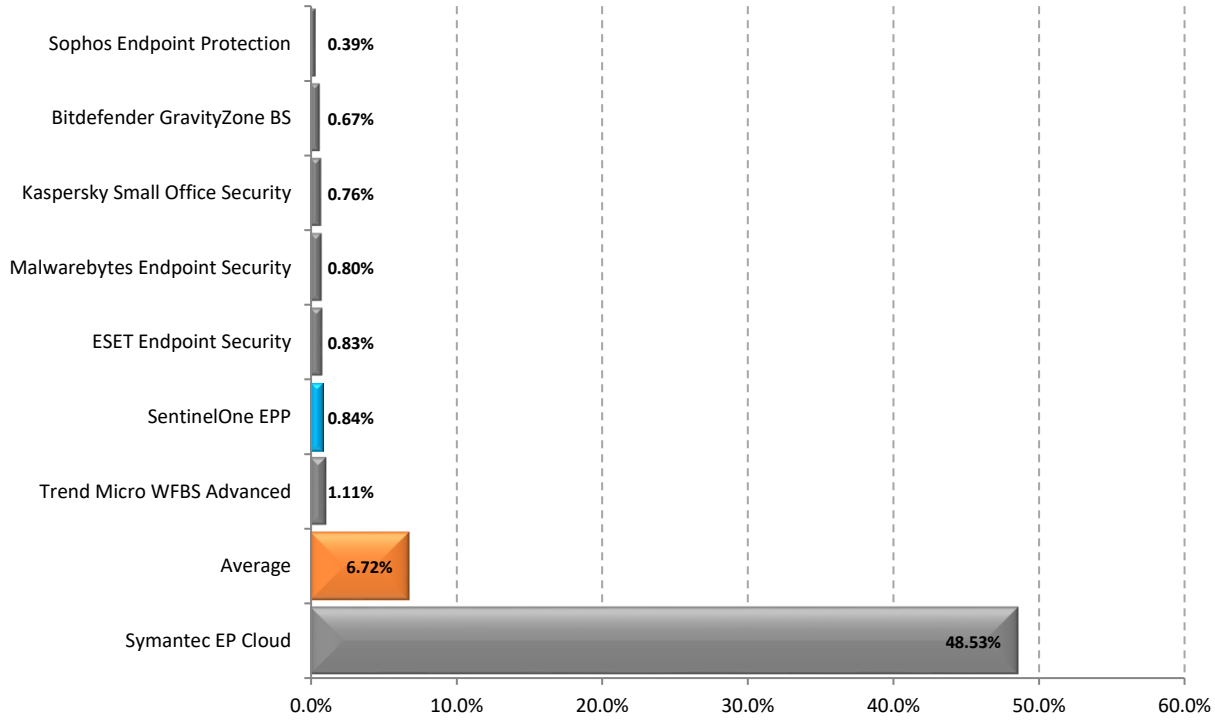
The following chart compares the average time taken for the system to boot (from a sample of five boots) for each endpoint security product tested. Products with lower boot times are considered better performing products in this category.*



**Symantec was omitted from this test as the boot time test could not reach an idle state with the product installed.*

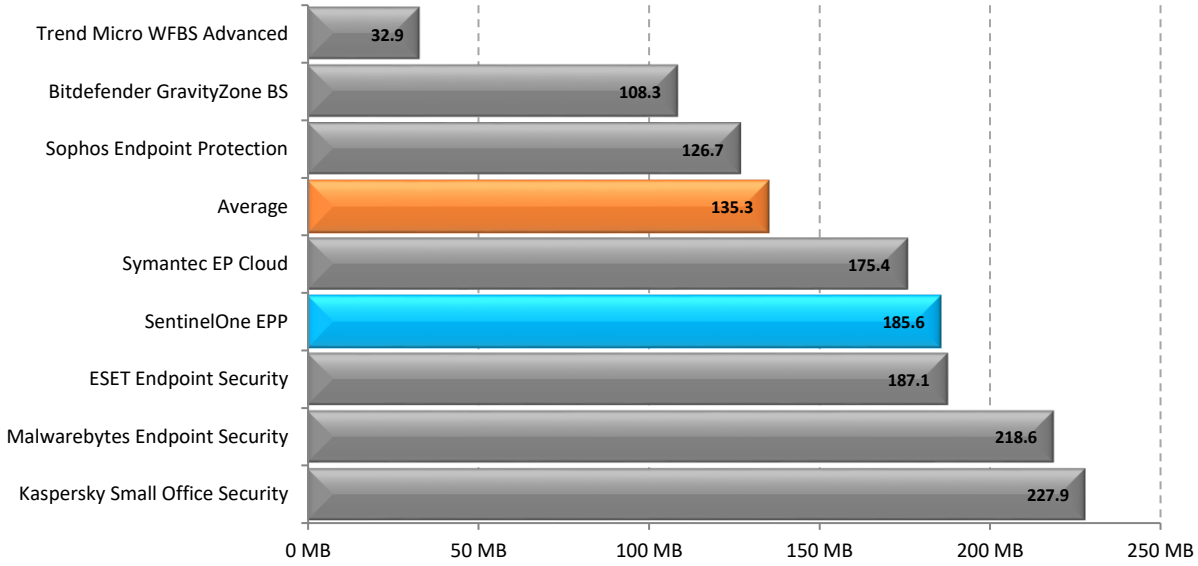
Benchmark 4 – CPU Usage during Idle

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



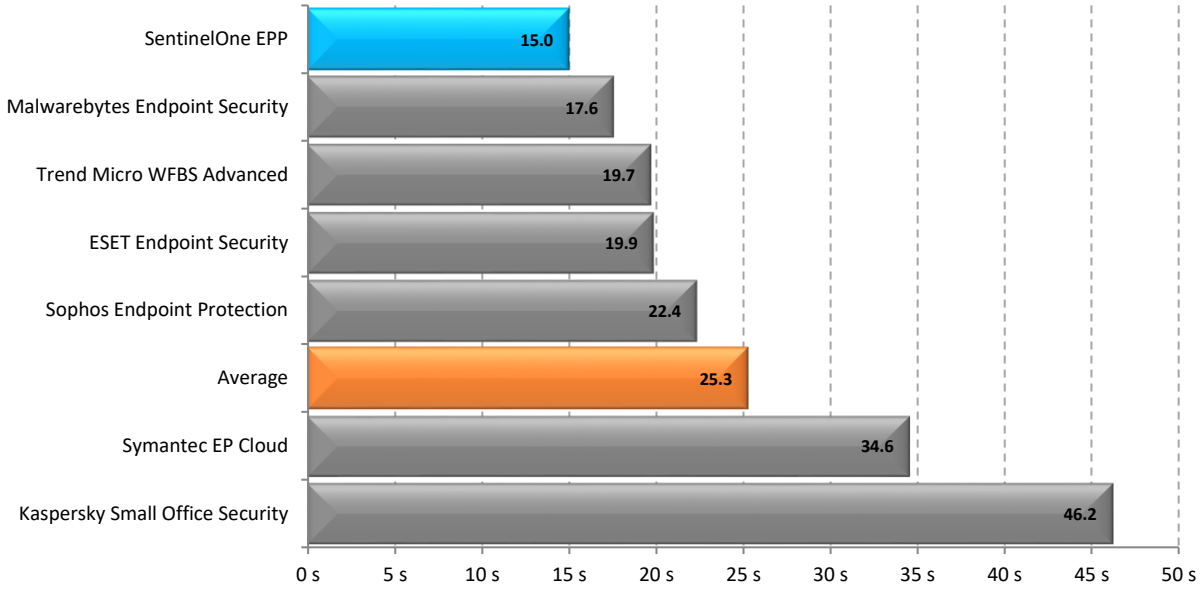
Benchmark 5 – Memory Usage during System Idle

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 – Browse Time

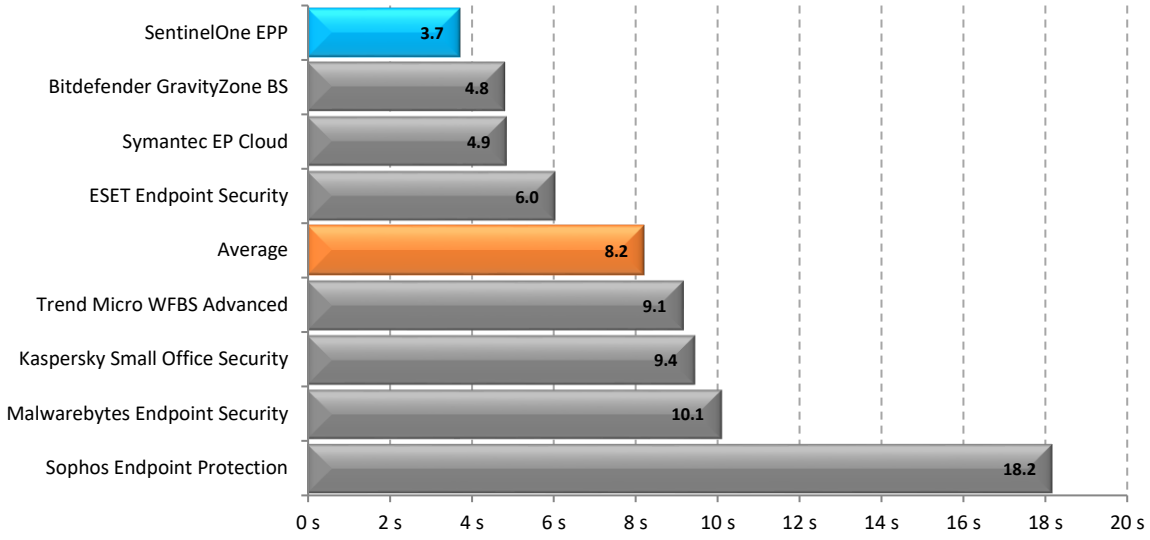
The following chart compares the average time taken for Internet Explorer to successively load a set of popular websites through the local area network from a local server machine. Products with lower browse times are considered better performing products in this category.*



** Bitdefender was excluded from this test as the test script was blocked by the application's phishing filter.*

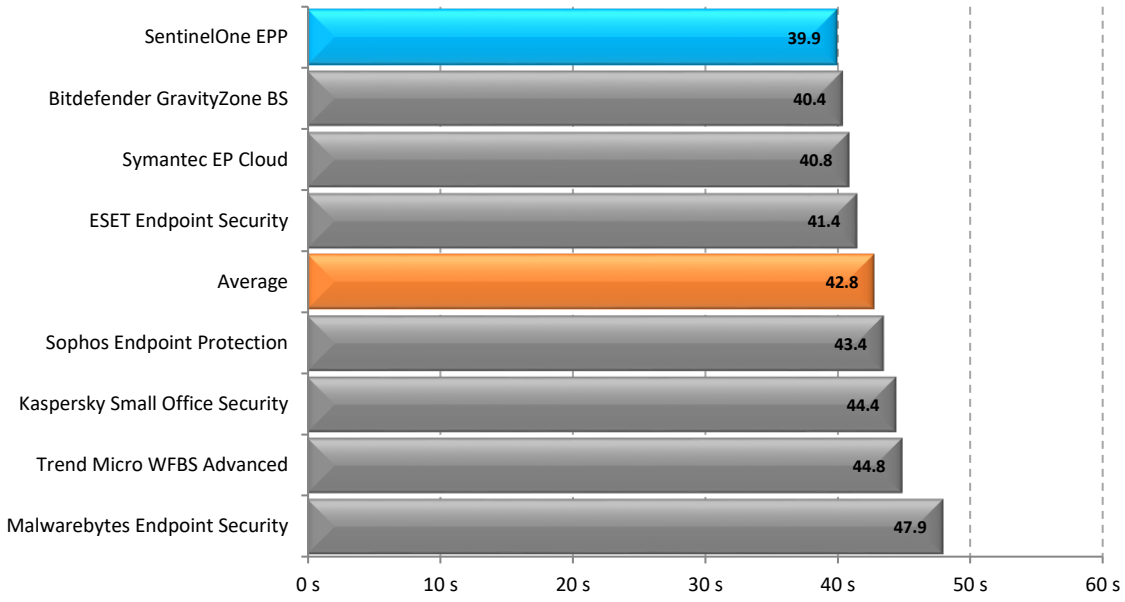
Benchmark 7 – File Copy, Move, and Delete

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.



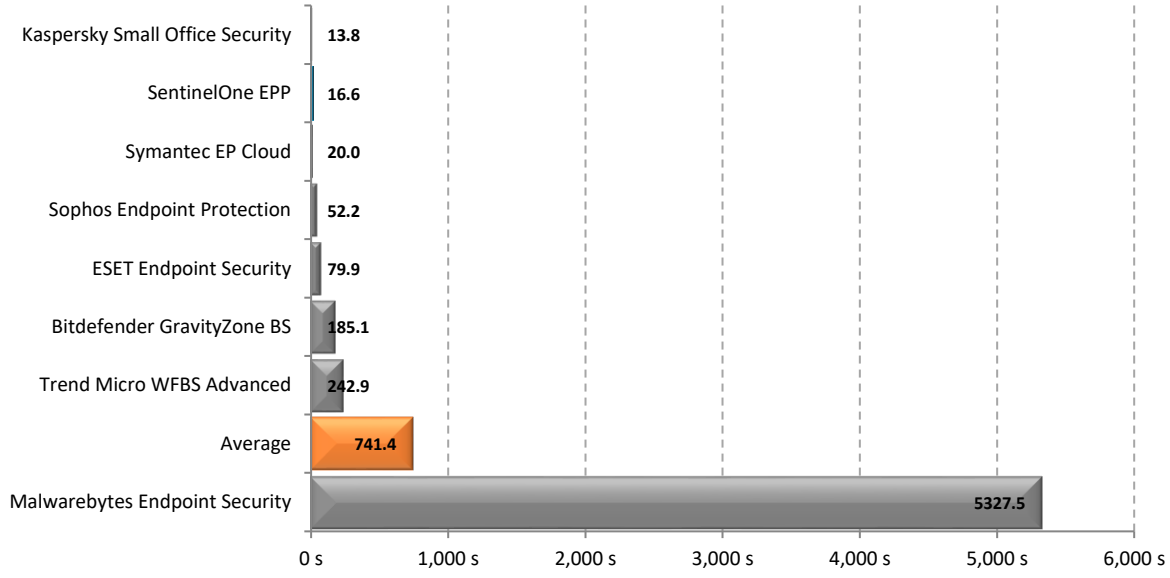
Benchmark 8 – File Compression and Decompression

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.



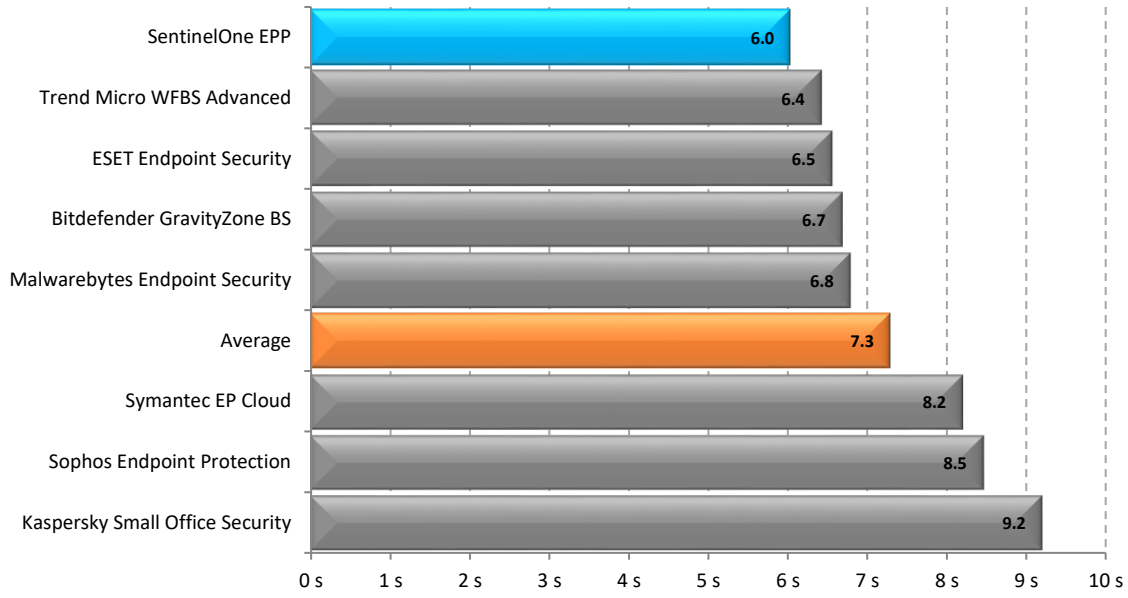
Benchmark 9 – File Write, Open, and Close

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.



Benchmark 10 – Network Throughput

The following chart compares the average time to download a sample set of common file types 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 included in this report are not an exhaustive list of all products available in these very competitive product categories. The products as well as test metrics presented in this report are only a subset selected by SentinelOne.

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

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

Trademarks

All trademarks are the property of their respective owners.

Contact Details

PassMark Software Pty Ltd
Level 5
63 Foveaux 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 10 Home (64-bit)

Model:	Lenovo H50W-50 i5
CPU:	Intel Core i5-4460 CPU @ 3.20GHz 3.20 GHz
Video Card:	NVIDIA GeForce GT 705
RAM:	8GB DDR3 RAM
SSD (Main Boot Drive):	Samsung SSD 850 PRO 512 GB
2nd Drive:	Samsung 1000GB 7200RPM HD103UJ
Network:	Gigabit (1Gb/s) switch
O/S:	Windows 10 Home 10.0 (Build 10240)

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.

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)

Appendix 2 – Methodology Description

Windows 10 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 10 image are as follows:

1. Installation and activation of **Windows 10**.
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. Disabled *Superfetch* to ensure consistent results.
7. Installed *HTTP Watch* for Browse Time testing.
8. Installed *Windows 10 Assessment and Deployment Kit (ADK)* for Boot Time testing.
9. Installed Active Perl for interpretation of some test scripts.
10. Install OSForensics for testing (Installation Size and Registry Key Count tests) purposes.
11. Disabled Windows updates.
12. Install important Windows updates.
13. Created a baseline image of the boot drive using OSForensics.

Benchmark 1 – 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 a 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. For all products tested, the installation was performed directly on the endpoint, either using a standalone installation package or via the management server web console.

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 2.2** 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 – Boot Time

PassMark Software uses tools available from the ***Windows Performance Toolkit*** (as part of the Microsoft Windows 10 ADK obtainable from the Microsoft Website).

The Boot Performance (fast startup) test is ran as an individual assessment via the Windows Assessment Console. The network connection is disabled and the login password is removed to avoid interruption to the test. The final result is taken as the total boot duration excluding BIOS load time.

Benchmark 4 – 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 500 samples. This test is conducted after restarting the endpoint machine and after five minutes of machine idle.

Benchmark 5 – Memory Usage during System Idle

The ***MemLog++*** 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 ***MemLog++*** 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 ***MemLog++***. ***Process Explorer*** is a Microsoft Windows Sysinternals software tool which shows a list of all DLL processes currently loaded on the system.

Benchmark 6 – Browse Time

We used a script in conjunction with ***HTTPWatch*** *(Basic Edition, version 9.1.13.0)* 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 11*** (11.0.9600.17801) 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 7-10 – Real-Time Performance

We used a single script in testing Benchmarks 7-10. The script consecutively executes tests for Benchmarks 7-10. The script times each phase in these benchmarks using ***CommandTimer.exe*** and appends results to a log file.

Benchmarks 7 – 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 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 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 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 – 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]. 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	Number	Size (bytes)
JPEG	343	30,668,312
GIF	9	360,349
PNG	5	494,780
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
PDF	73	136,298,049
ZIP	4	6,295,987
7Z	1	92,238
Total	**484**	**553,638,694**

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.