PASSMARK® SOFTWARE

Malwarebytes

Malwarebytes Endpoint Protection vs. Four Competitors (March 2018)

Performance Benchmark

Document: Malwarebytes Endpoint Protection vs. Four Competitors (March 2018)
Authors: M. Baquiran, D. Wren
Company: PassMark Software
Date: 9 March 2018
File: Malwarebytes_Endpoint_Protection_vs_Competitors.docx
Edition 1

Table of Contents

Revision History

Rev	Revision History	Date
Edition 1	Initial version of this report.	9 March 2018

References

Ref #	Document	Author	Date
1	**What Really Slows Windows Down** (URL)	O. Warner, The PC Spy	2001-2018

Executive Summary

PassMark Software® conducted objective performance testing on five (5) security software products, on Windows 10 (64-bit) between October 2017 and March 2018. This report presents our results and findings as a result of performance benchmark testing conducted for these endpoint security products.

The aim of this report is to compare the performance impact of Malwarebytes Endpoint Protection with four (4) competitor products. The following product description and user interface screenshot (*Figure 1*) were provided by Malwarebytes:

"*Malwarebytes Endpoint Protection is a next-generation Antivirus replacement that provides advanced threat prevention solution for endpoints that uses a layered approach with multiple detection techniques. This provides businesses with full attack chain protection against both known and unknown malware, ransomware, and zero-hour threats. Unified onto a single agent, Malwarebytes Endpoint Protection reduces the complexity and costs often associated with deploying multiple individual solutions.*

Malwarebytes has spent years helping organizations recover from successful infections. Our remediation expertise provides deep insight into how current endpoint protection technologies fail to keep organizations safe. With that intelligence, Malwarebytes introduced Malwarebytes Endpoint Protection—a superior, multivector defense solution. Malwarebytes breaks the attack chain by combining advanced malware detection and remediation technologies in a single platform. Multi-stage attack protection provides the ability to stop an attacker at every step."

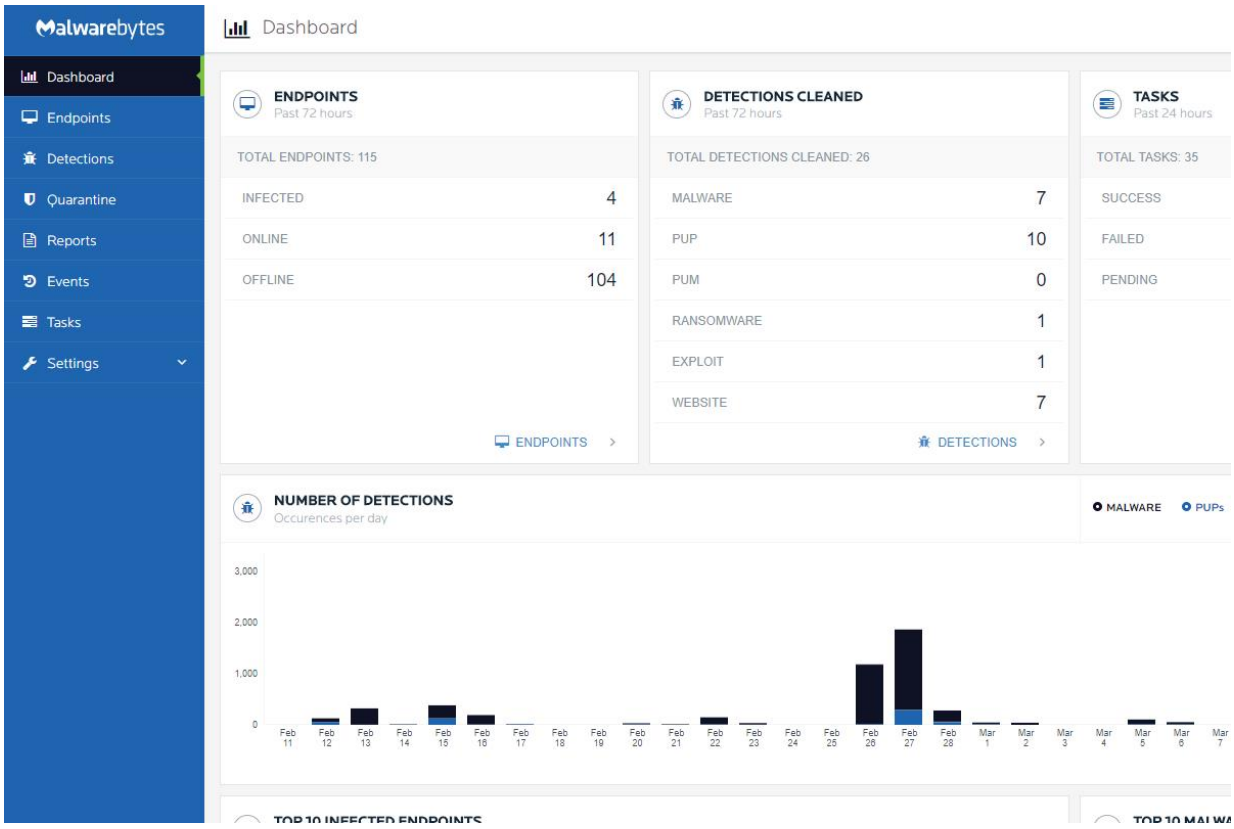


Figure 1: Screenshot of the Malwarebytes Endpoint Protection Dashboard

Testing was performed on all products using twelve (12) selected performance metrics.

These performance metrics are as follows.

- Boot Time;
- Installation Time;
- Installation Size;
- Scheduled Scan Time;
- CPU Usage during Scan;
- Browse Time;
- Network Throughput – Binary;
- Network Throughput – File Format;
- File Copy, Move, and Delete – Binary;
- File Copy, Move, and Delete – File Format;
- File Compression and Decompression – Binary; and
- File Compression and Decompression – File Format.

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 60, which would apply in a hypothetical situation where a product has attained first place in all twelve (12) metrics. Endpoint products have been ranked by their overall scores:

Product Name	Overall Score
Malwarebytes Endpoint Protection	51
Symantec Endpoint Protection Small Business Edition	43
Trend Micro Worry-Free Business Security	28
Sophos Endpoint	27
Kaspersky Endpoint Security	26

Products and Versions

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

Manufacturer	Product Name	Product Version	Date Tested
Malwarebytes	Malwarebytes Endpoint Protection	1.0.3996	Oct 2017
Trend Micro Inc.	Trend Micro Worry-Free Business Security	Security Agent 6.3.1200/13.1.2050	Feb 2018
Kaspersky Lab	Kaspersky Endpoint Security 10 for Windows	10.3.0.6294	Mar 2018
Sophos	Sophos Endpoint Advanced 10.8.1.1	Sophos Endpoint Advanced 10.8.1.1	Mar 2018
Symantec Corp	Symantec Endpoint Protection Small Business Edition (Symantec .cloud)	Cloud Agent 3.00.10.2737 Endpoint Protection NIS-22.11.2.7	Feb 2018

Performance Metrics Summary

The following test metrics have been selected to highlight certain areas in which security products impact system performance for end users, particularly areas involving common tasks that end-users 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 – 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 2 – 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 3 – 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 4 – Scheduled Scan Time

Most antivirus solutions are scheduled by default to scan the system regularly for viruses and malware. This metric measured the amount of time required to run a scheduled scan on the system. The scan is set to run at a specified time via the client user interface.

Benchmark 5 – 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 security software when performing a scan.

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 – Network Throughput – Binary

The metric measures the amount of time taken to download a set of binary 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. This sample set includes system files such as EXE, DLL, and SYS files.

Benchmark 8 – Network Throughput – File Format

The metric measures the amount of time taken to download a set of document and media 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. This sample set includes document and media files such as DOC, PPT, PDF, JPG, and WMV files.

Benchmark 9 – File Copy, Move, and Delete - Binary

This metric measures the amount of time taken to copy, move and delete a sample set of binary files. This sample set includes system files such as EXE, DLL, and SYS files.

Benchmark 10 – File Copy, Move, and Delete – File Format

This metric measures the amount of time taken to copy, move and delete a sample set of files. This sample set includes document and media files such as DOC, PPT, PDF, JPG, and WMV files.

Benchmark 11 – File Compression and Decompression – Binary

This metric measures the amount of time taken to compress and decompress different types of files. This sample set includes system files such as EXE, DLL, and SYS files.

Benchmark 12 – File Compression and Decompression – File Format

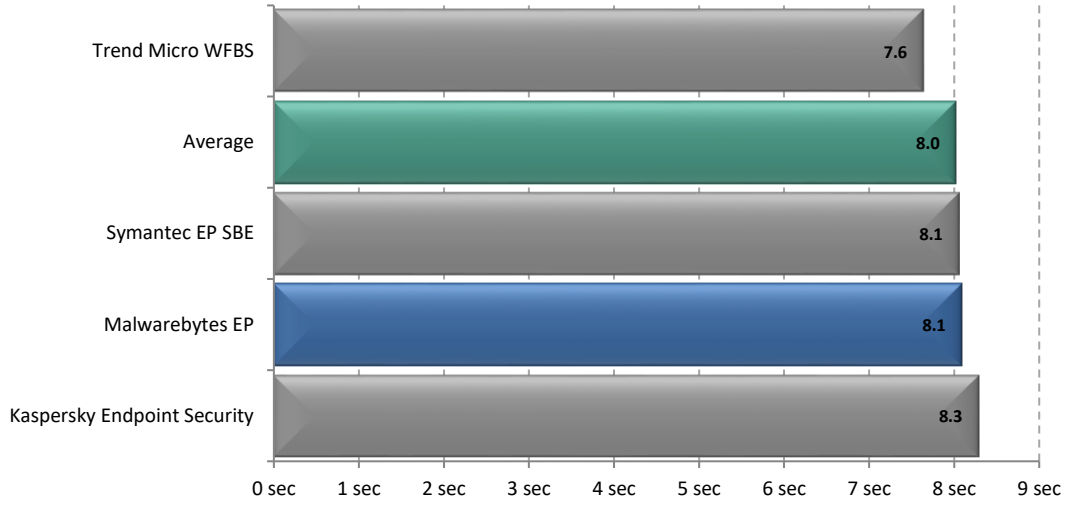
This metric measures the amount of time taken to compress and decompress different types of files. This sample set includes document and media files such as DOC, PPT, PDF, JPG, and WMV files.

Test Results

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

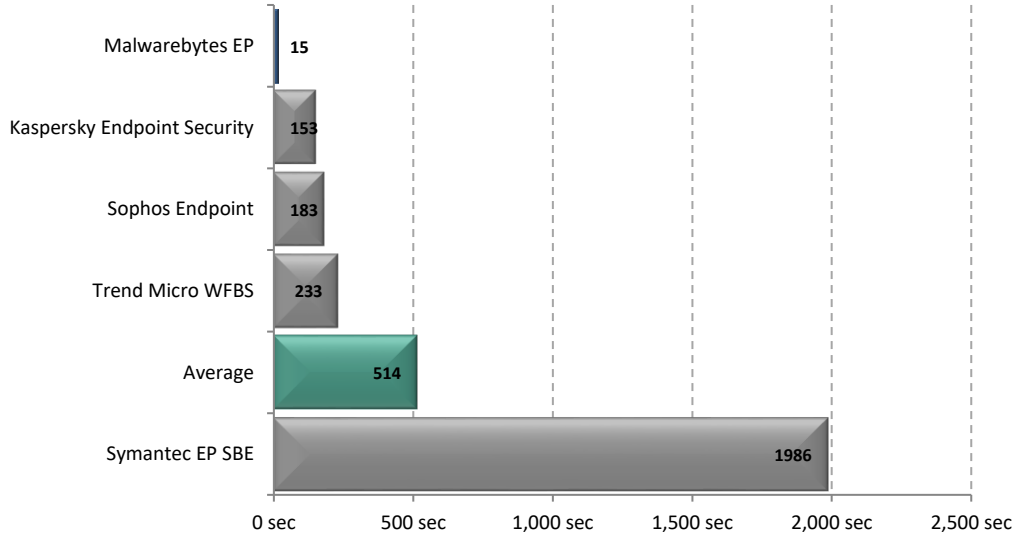
Benchmark 1 – Boot Time

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.



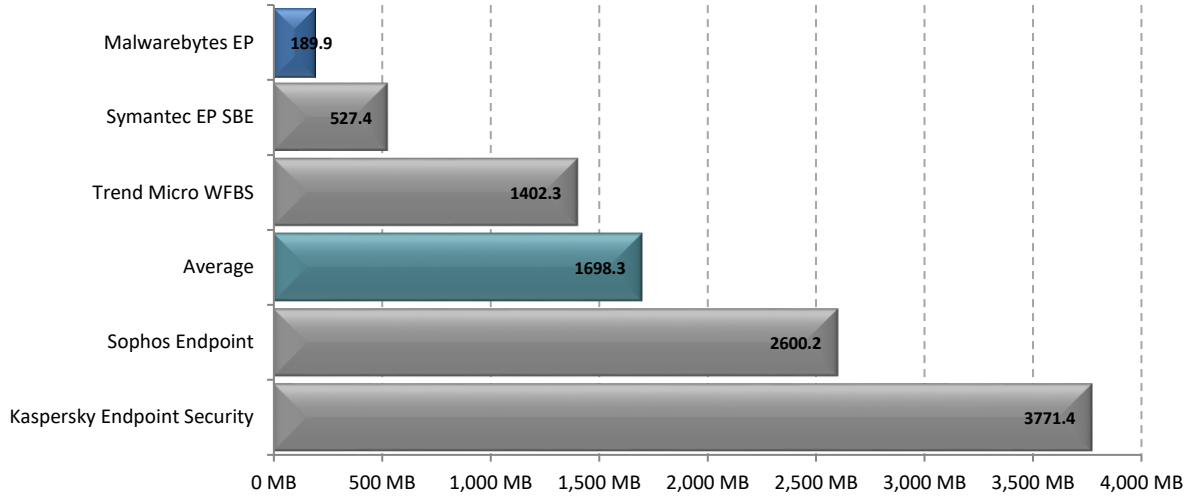
Benchmark 2 – Installation Time

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.



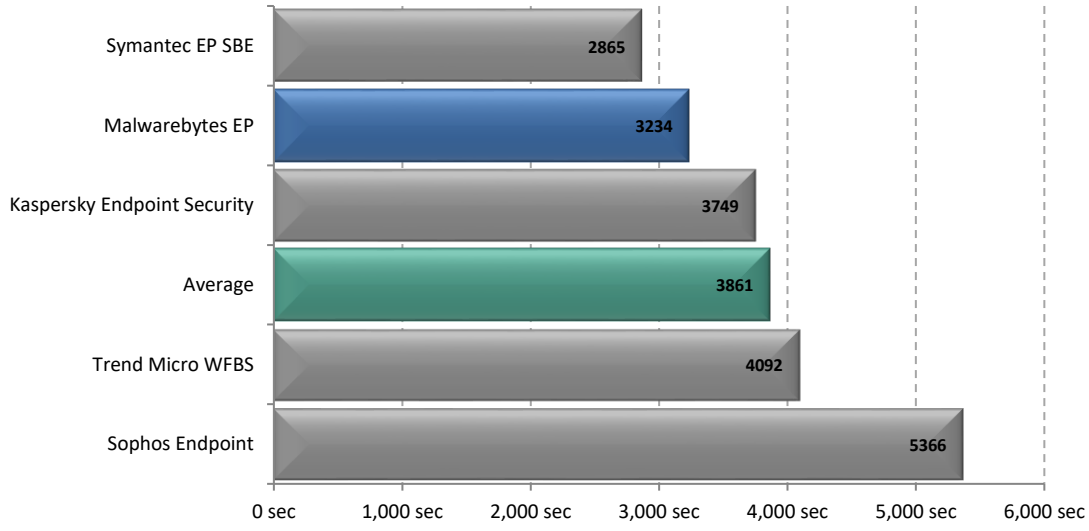
Benchmark 3 – Installation Size

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.[1]



Benchmark 4 – Scheduled Scan Time

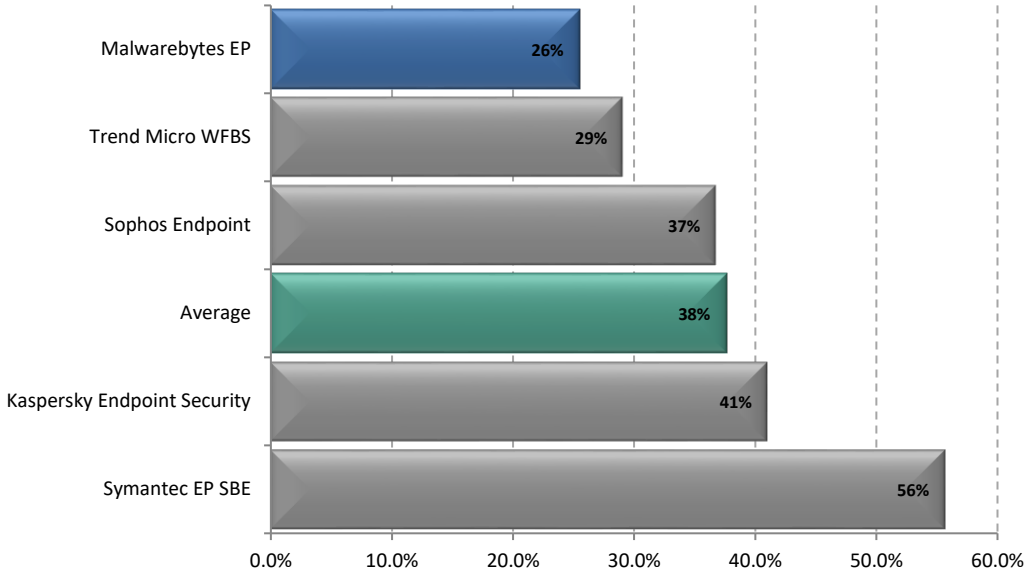
The following chart compares the average time taken to run a scheduled scan on the system for each security product tested.



[1] A Windows Update occurred immediately after installation of Sophos and Kaspersky and the new files from the update were thus included in the installation size calculation for these products. This is due to the difficulty in permanently disabling Windows Updates in Windows Home, in which certain security products re-enable the Windows Update service upon installation.

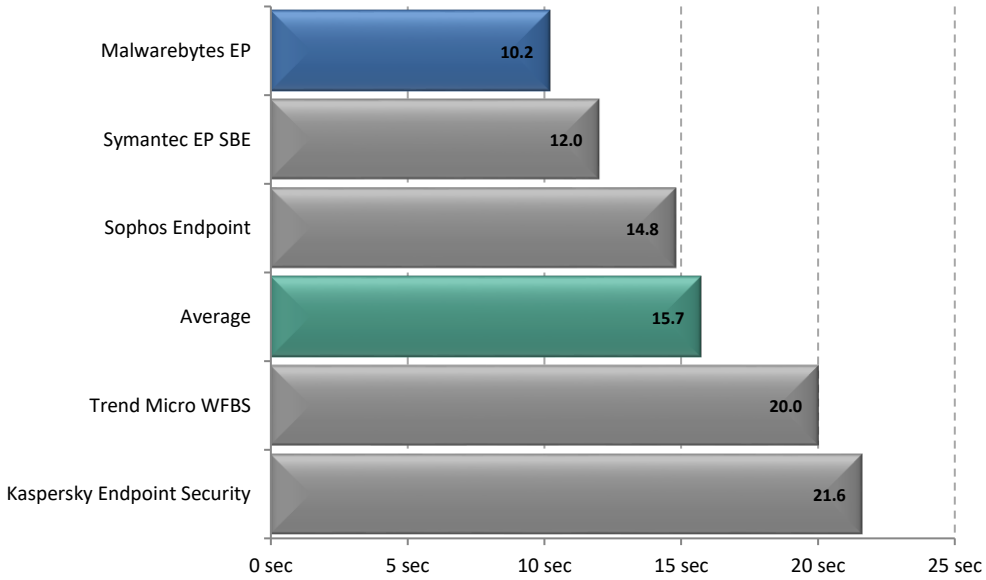
Benchmark 5 – CPU Usage during Scan

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.



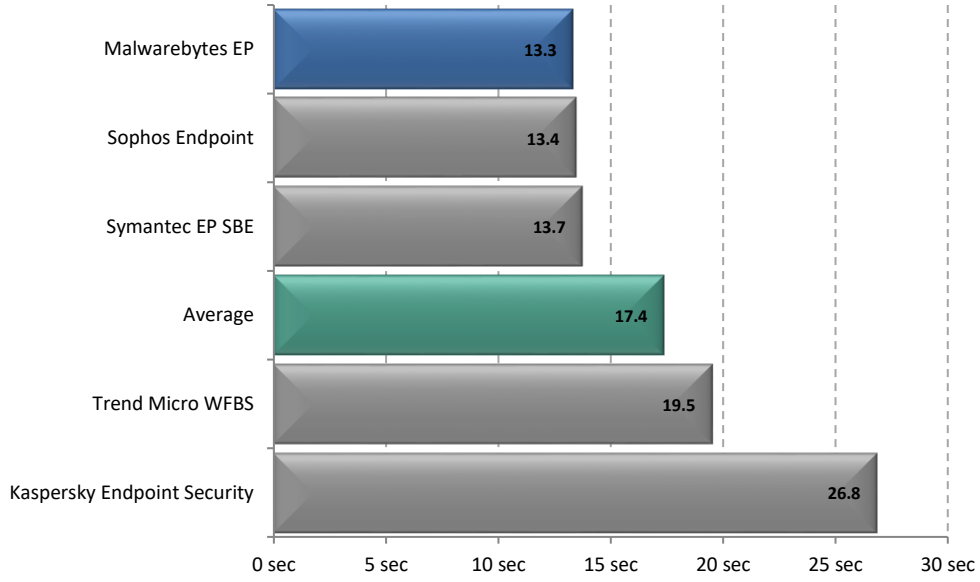
Benchmark 6 – Browse Time

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.



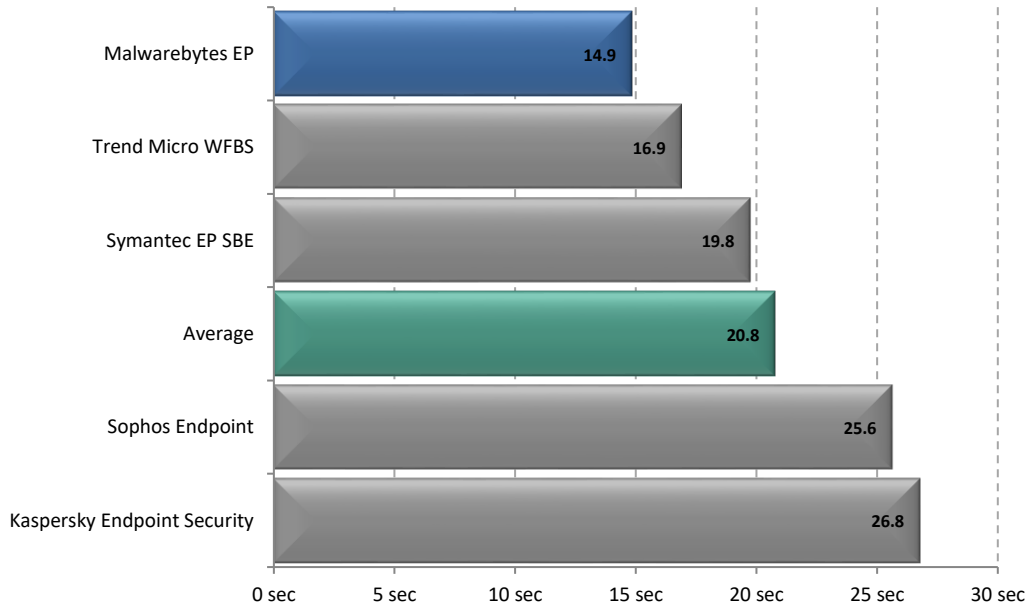
Benchmark 7 – Network Throughput - Binary

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



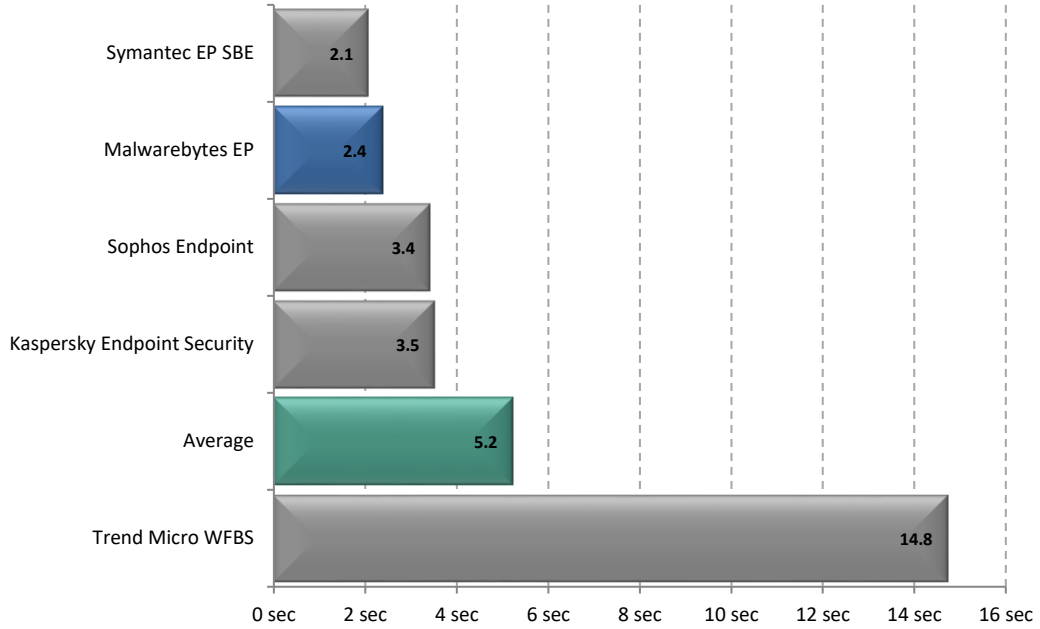
Benchmark 8 – Network Throughput – File Format

The following chart compares the average time to download a sample set of document and media files for each endpoint security product tested. Products with lower times are considered better performing products in this category.



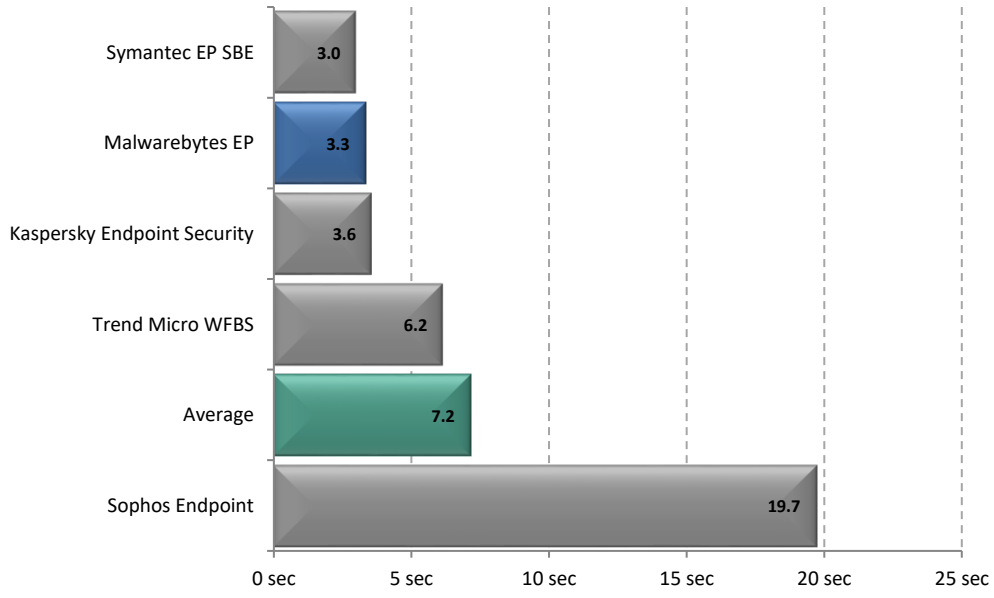
Benchmark 9 – File Copy, Move, and Delete - Binary

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



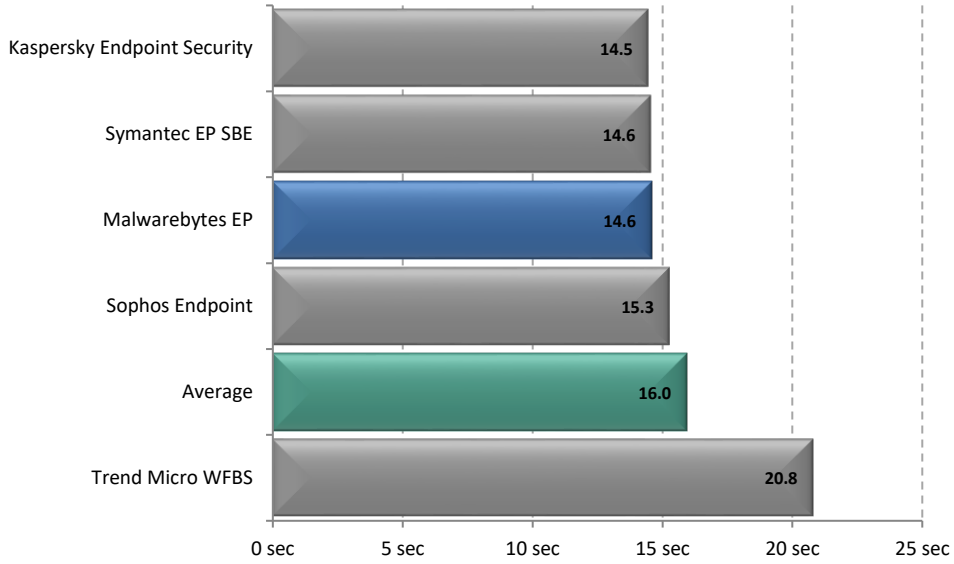
Benchmark 10 – File Copy, Move, and Delete – File Format

The following chart compares the average time taken to copy, move and delete a set of document and media files for each endpoint security product tested. Products with lower times are considered better performing products in this category.



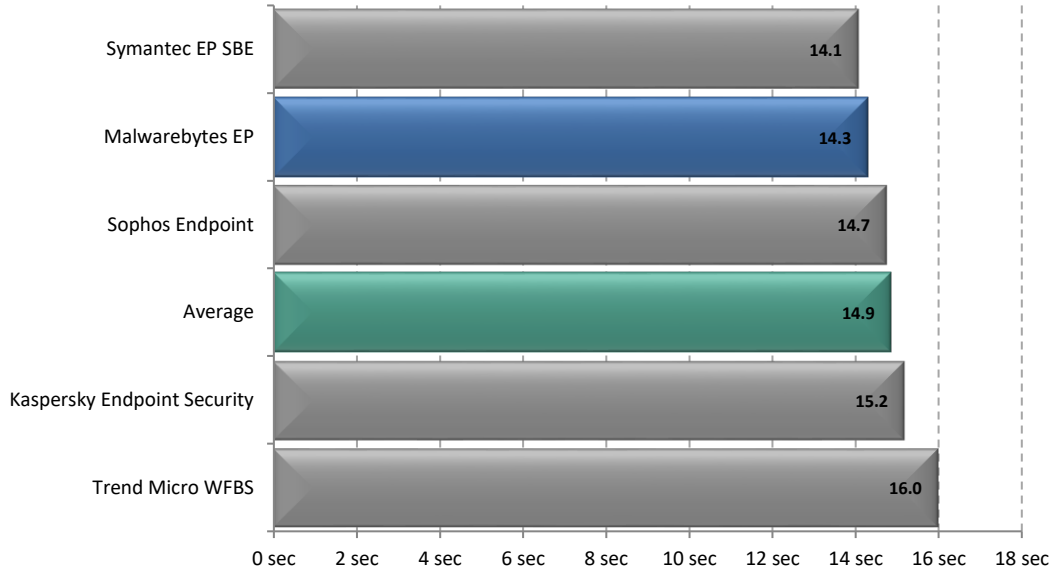
Benchmark 11 – File Compression and Decompression - Binary

The following chart compares the average time it takes for a set of binary 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 12 – File Compression and Decompression – File Format

The following chart compares the average time it takes for a set of document and media files to be compressed and decompressed 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

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

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 (64-bit)

For our testing, PassMark Software used a test environment running Windows 10 Home (64-bit) with the following hardware specifications:

Model:	Lenovo H50W-50 i5
CPU:	Intel Core i5-4460 CPU @ 3.20GHz 3.20 GHz
Video Card:	NVIDIA GeForce GT 705
Motherboard:	Foxconn 2ABF 3.10
RAM:	8GB DDR3 RAM
HDD:	Samsung SSD 850 PRO 512 GB
2nd Drive:	Samsung HD103UJ 1000GB 7200RPM
Network:	Gigabit (1Gbit/s)
O/S:	Windows 10 Home Version 1703 (OS Build 15063.540)

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
Motherboard:	Intel S1200BTL Server
RAM:	Kingston 8GB (2 x 4GB) ECC RAM, 1333Mhz
SSD:	OCZ 128GB 2.5” Solid State Disk
Network:	Gigabit (1Gbit/s)

Appendix 2 – Methodology Description

Windows 10 Image Creation

PassMark OSForensics was used to create a "clean" baseline image prior to testing. Our aim was 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. Changed User Account Control settings to "Never Notify".
3. Disable Windows Defender.
4. Disable the Windows firewall to avoid interference with security software.
5. Disabled *Superfetch* to ensure consistent results.
6. Installed *Windows Assessment and Deployment Kit* for Fast Boot Time testing.
7. Install OSForensics for testing (Installation Size test) purposes.
8. Update Windows to include current important updates.
9. Disabled Windows Update Service.
10. Created a baseline image using OSForensics.

Benchmark 1 – 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 result is taken as the total boot duration excluding BIOS load time.

Benchmark 2 – 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 3 – Installation Size

Using **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. However, any files automatically downloaded or added as a result of the product's installation will be included. For example, some security products re-enable the Windows Update service upon installation, causing a Windows update to immediately occur upon restart. In this case, the increased disk size as a result of the Windows update will be included in the calculated Installation Size.

Benchmark 4 – Scheduled Scan Time

This scan is configured as a full system scheduled scan from user interface. The default full system scheduled scan settings are kept (except for the start time), and the scan is scheduled to run at the next convenient time. 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.

The scan is run three times with a reboot between each run to remove potential caching effects. The result for this test is the average of the three scan times. Where this functionality is not available, the product is omitted from the metric, and given the lowest score for this metric.

Benchmark 5 – 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 an On-Demand Scan is run on a sample data set. The result is calculated as an average five sets of thirty CPU usage samples.

Benchmark 6 – Browse Time

This benchmark measures the time it takes to load a list of around 100 'popular' websites in ***Microsoft Edge*** (Version 40.15063.0.0) consecutively from a local server. The set of websites used in this test include front pages of high traffic pages. This includes shopping, social, news, finance and reference websites.

A few lines of javascript that load the next page in the chain once the current page has loaded, are added to each html page in the chain. Once the first page has been loaded completely, the javascript loads the second webpage in the chain. Once the second webpage has finished loading, the javascript loads the third page in the chain. This process is repeated until the final website in the chain has loaded. The start time and end time of this process are recorded and the difference is calculated in seconds to get the result for each round.

The above script is executed five times and the final result is an average of these five samples.

Benchmark 7 – Network Throughput – Binary

This benchmark measured how much time was required to download a sample set of binary files of various sizes and types over a 1Gbit/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.

This test set is made up of 559 files over 423,853,238 bytes and can be categorized as System Files [100%]. 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)
EXE	85	57,785,508
DLL	389	328,718,104
AX	2	36,864
CPL	4	4,218,880
CPX	4	8,768
DRV	21	517,600
ICO	2	215,240
MSC	2	83,174
NT	2	3,376
ROM	4	73,222
SCR	4	4,500,480

SYS	27	27,183,378
TLB	6	271,160
TSK	2	2,304
UCE	2	45,968
COM	1	18,944
XML	1	76,060
Total	**559**	**423,853,238**

This test was conducted five times to obtain an average, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 8 – Network Throughput – File Format

This benchmark measured how much time was required to download a sample set of document and media files of various sizes and types over a 1Gbit/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.

This set is made up of 505 files over 609,478,281 bytes and can be categorized as documents [32% of total] and media files [68% of total].

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
JPG	343	30,668,312
GIF	9	360,349
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
PNG	5	494,780
Total	**505**	**609,478,281**

This test was conducted five times to obtain an average, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 9 – File Copy, Move, and Delete - Binary

This test measures the amount of time required for the system to copy, move and delete samples of binary files. The xcopy, rmdir, and move commands were used to carry out the copy, move, and delete respectively, and ***CommandTimer.exe*** was used to time the test.

The data set is made up of 559 files over 423,853,238 bytes and can be categorized as System Files [100%]. 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)
EXE	85	57,785,508
DLL	389	328,718,104
AX	2	36,864
CPL	4	4,218,880
CPX	4	8,768
DRV	21	517,600
ICO	2	215,240
MSC	2	83,174
NT	2	3,376
ROM	4	73,222
SCR	4	4,500,480
SYS	27	27,183,378
TLB	6	271,160
TSK	2	2,304
UCE	2	45,968
COM	1	18,944
XML	1	76,060
Total	**559**	**423,853,238**

This test was conducted five times to obtain an average, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 10 – File Copy, Move, and Delete – File Format

This test measures the amount of time required for the system to copy, move and delete a set of document and media files in various file formats. The xcopy, rmdir, and move commands were used to carry out the copy, move, and delete respectively, and ***CommandTimer.exe*** was used to time the test.

The data set is made up of 505 files over 609,478,281 bytes and can be categorized as documents [32% of total] and media files [68% of total].

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
JPG	343	30,668,312
GIF	9	360,349
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
PNG	5	494,780
Total	**505**	**609,478,281**

This test was conducted five times to obtain an average, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 11 – File Compression and Decompression - Binary

This test measures the amount of time required to compress and decompress a set of binary files. ***CommandTimer.exe*** was used to record the amount of time required for *7zip.exe* to compress the files into a *.zip and subsequently decompress the created *.zip file.

The data set is made up of 559 files over 423,853,238 bytes and can be categorized as System Files [100%]. 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)
EXE	85	57,785,508
DLL	389	328,718,104
AX	2	36,864
CPL	4	4,218,880
CPX	4	8,768
DRV	21	517,600
ICO	2	215,240
MSC	2	83,174
NT	2	3,376

ROM	4	73,222
SCR	4	4,500,480
SYS	27	27,183,378
TLB	6	271,160
TSK	2	2,304
UCE	2	45,968
COM	1	18,944
XML	1	76,060
Total	**559**	**423,853,238**

This test was conducted five times to obtain an average, with the test machine rebooted between each sample to remove potential caching effects.

Benchmark 12 – File Compression and Decompression – File Format

This test measures the amount of time required to compress and decompress a set of document and media files. ***CommandTimer.exe*** was used to record the amount of time required for *7zip.exe* to compress the files into a *.zip and subsequently decompress the created *.zip file.

The data set is made up of 500 files over 609,478,281 bytes and can be categorized as documents [32% of total] and media files [68% of total].

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
JPG	343	30,668,312
GIF	9	360,349
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
PNG	5	494,780
Total	**505**	**609,478,281**

This test was conducted five times to obtain an average, with the test machine rebooted between each sample to remove potential caching effects.