

WEBROOT[®]
an **opentext**™ company

Webroot Business Endpoint Protection vs. Eight Competitors

Performance Benchmark

May 2021

Document: Webroot Business Endpoint Protection vs. Eight Competitors Performance Benchmark
Authors: J. Han, D. Wren
Company: PassMark Software
Date: 28 May 2021
File: Webroot_Business_Endpoint_Protection_Performance_Benchmarks_Ed2.pdf
Edition: 2

Table of Contents

REVISION HISTORY	3
REFERENCES	3
EXECUTIVE SUMMARY	4
OVERALL SCORE	5
PRODUCTS AND VERSIONS	6
PERFORMANCE METRICS SUMMARY	7
TEST RESULTS	10
BENCHMARK 1 – INSTALLATION TIME.....	10
BENCHMARK 2 – INSTALLATION SIZE.....	11
BENCHMARK 3 – BOOT TIME.....	12
BENCHMARK 4 – CPU USAGE DURING IDLE.....	13
BENCHMARK 5 – CPU USAGE DURING SCAN.....	14
BENCHMARK 6 – MEMORY USAGE DURING SYSTEM IDLE.....	15
BENCHMARK 7 – MEMORY USAGE DURING INITIAL SCAN.....	16
BENCHMARK 8 – MEMORY USAGE DURING SCHEDULED SCAN.....	17
BENCHMARK 9 – ON-DEMAND SCAN TIME.....	18
BENCHMARK 10 – SCHEDULED SCAN TIME.....	19
BENCHMARK 11 – BROWSE TIME.....	20
BENCHMARK 12 – FILE COPY, MOVE, AND DELETE.....	21
BENCHMARK 13 – FILE COMPRESSION AND DECOMPRESSION.....	22
BENCHMARK 14 – FILE WRITE, OPEN, AND CLOSE.....	23
BENCHMARK 15 – NETWORK THROUGHPUT.....	24
DISCLAIMER AND DISCLOSURE	25
CONTACT DETAILS	25
APPENDIX 1 – TEST ENVIRONMENT	26
APPENDIX 2 – METHODOLOGY DESCRIPTION	27

Revision History

Rev	Revision History	Date
Edition 1	Initial version of this report.	19 May 2021
Edition 2	Updated Webroot logo.	28 May 2021

References

Ref #	Document	Author	Date
1	What Really Slows Windows Down (URL)	O. Warner, The PC Spy	2006

Executive Summary

PassMark Software® conducted objective performance testing on nine (9) security software products, on Windows 10 (64-bit) during March-May 2021. 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 Business Endpoint Protection product with eight (8) competitor products.

Testing was performed on all products using fifteen (15) performance metrics. These performance metrics are as follows:

- Installation Time
- Installation Size
- Boot Time
- CPU Usage during Idle
- CPU Usage during Scan
- Memory Usage during System Idle
- Memory Usage during Initial Scan
- Memory Usage during Scheduled Scan
- On-Demand Scan Time
- Scheduled Scan Time
- Browse Time
- File Copy, Move, and Delete
- File Compression and Decompression
- File Write, Open, and Close
- 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 fifteen (15) metrics. Endpoint products have been ranked by their overall scores:

Product Name	Overall Score
Webroot Business Endpoint Protection	83
ESET Endpoint Security	69
Kaspersky Endpoint Security Cloud	62
F-Secure Protection Service for Business	61
Malwarebytes Endpoint Protection	57
McAfee Endpoint Security	56
BitDefender GravityZone Business Security	49
Trend Micro Worry-Free Business Security Services	39
Sophos Intercept X	25

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
Webroot Inc.	Webroot Business Endpoint Protection	9.0.30.75	May 2021
Trend Micro Inc.	Trend Micro Worry-Free Business Security Services	6.7.1518/14.2.1271	Mar 2021
Kaspersky Lab	Kaspersky Endpoint Security Cloud	11.5.0.590	Mar 2021
Sophos Ltd.	Sophos Intercept X	2.15.4	Mar 2021
Bitdefender	BitDefender GravityZone Business Security	6.6.24.337	Mar 2021
ESET, spol. s r.o.	ESET Endpoint Security	8.0.2028.0	Mar 2021
F-Secure	F-Secure Protection Service for Business	21.3	Mar 2021
McAfee, LLC	McAfee Endpoint Security	10.7	Mar 2021
Malwarebytes	Malwarebytes Endpoint Protection	1.2.0.869	Mar 2021

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 CPU resources 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 CPU utilization while the machine and security software are in an idle state.

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 an on-demand scan.

Benchmark 6 – 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 7 – Memory Usage during Initial Scan

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

Benchmark 8 – Memory Usage during Scheduled Scan

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

Benchmark 9 – On-Demand 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 982 MB 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 10 – Scheduled Scan Time

Most security 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 or management console.

Benchmark 11 – 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 12 – 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 13 – 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 14 – 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 15 – Network Throughput

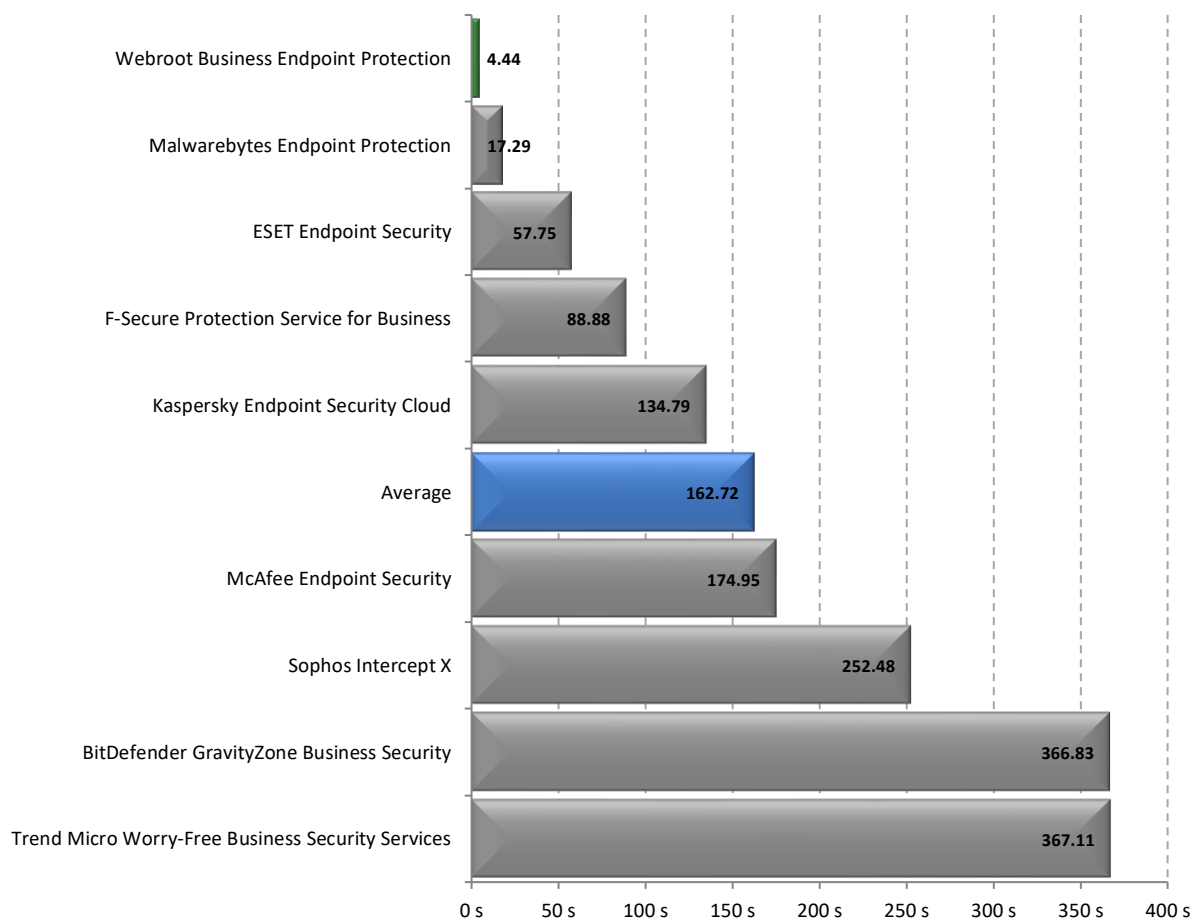
The metric measures the amount of time taken to download a variety of files from a local server using the Hypertext Transfer Protocol (HTTP), which is the main protocol used on the web for browsing, linking and data transfer. Files used in this test include file formats that users would typically download 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 Webroot Business Endpoint Protection in green. The average result has also been highlighted in blue for ease of comparison.

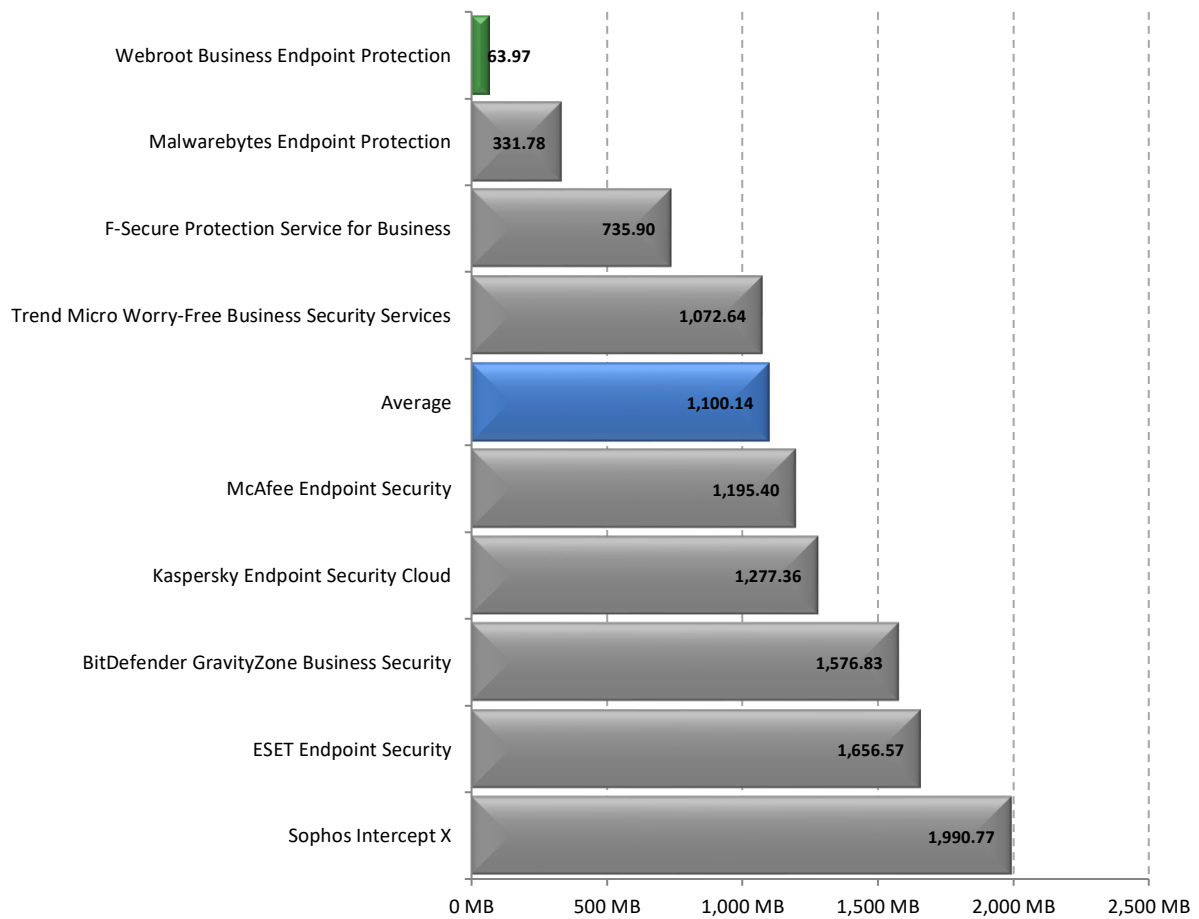
Benchmark 1 – Installation Time

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.



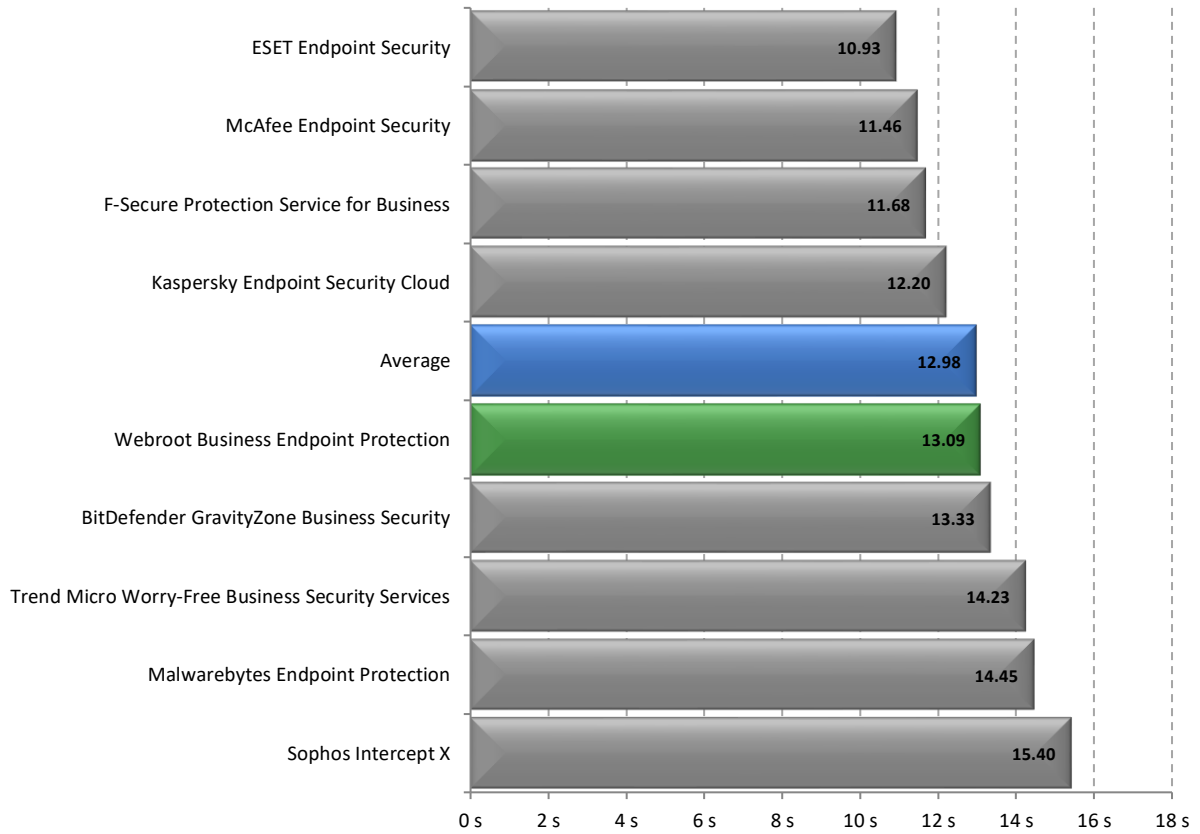
Benchmark 2 – Installation Size

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.



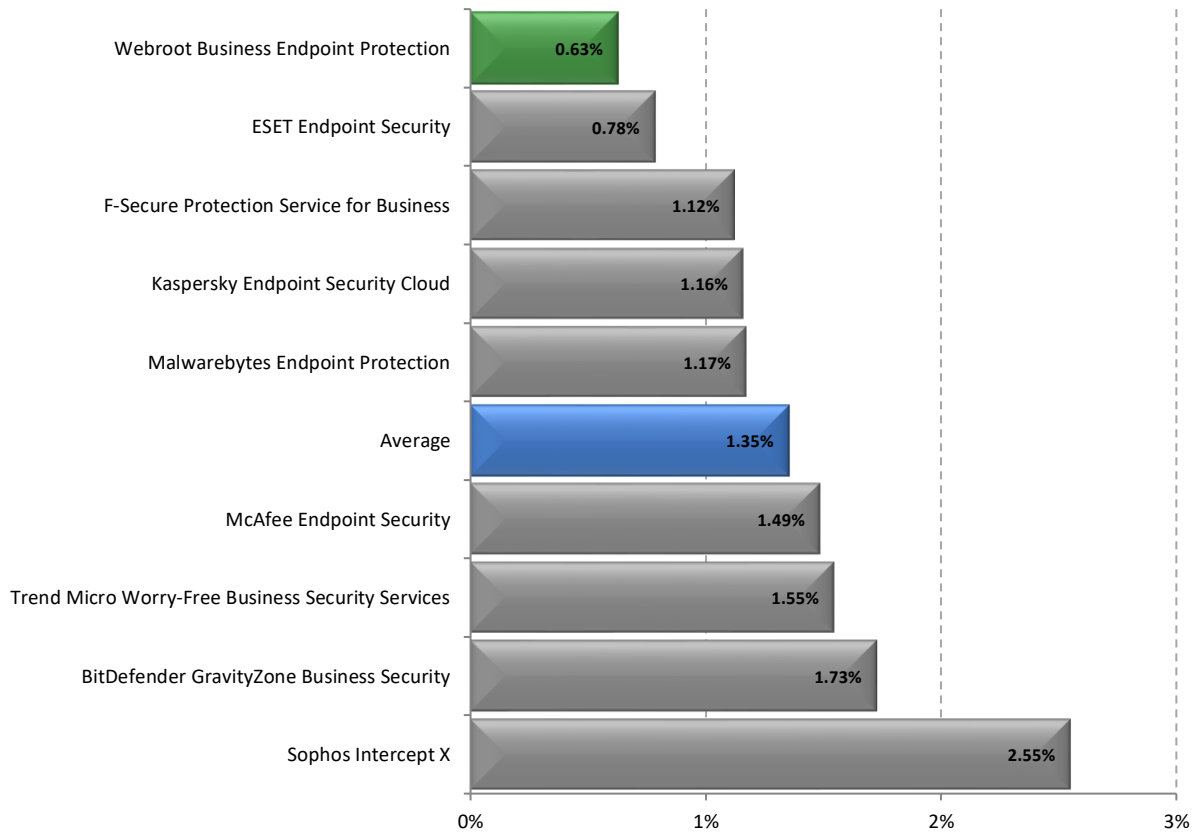
Benchmark 3 – Boot Time

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.



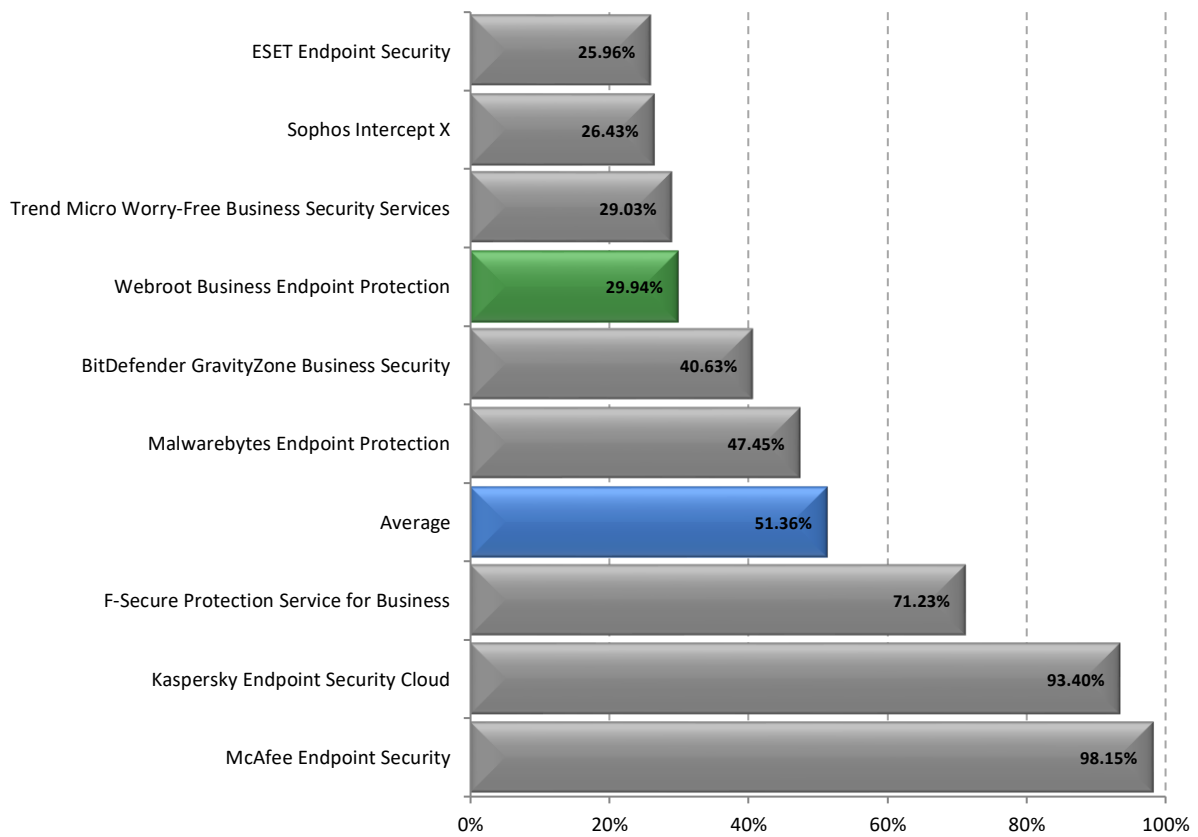
Benchmark 4 – CPU Usage during Idle

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



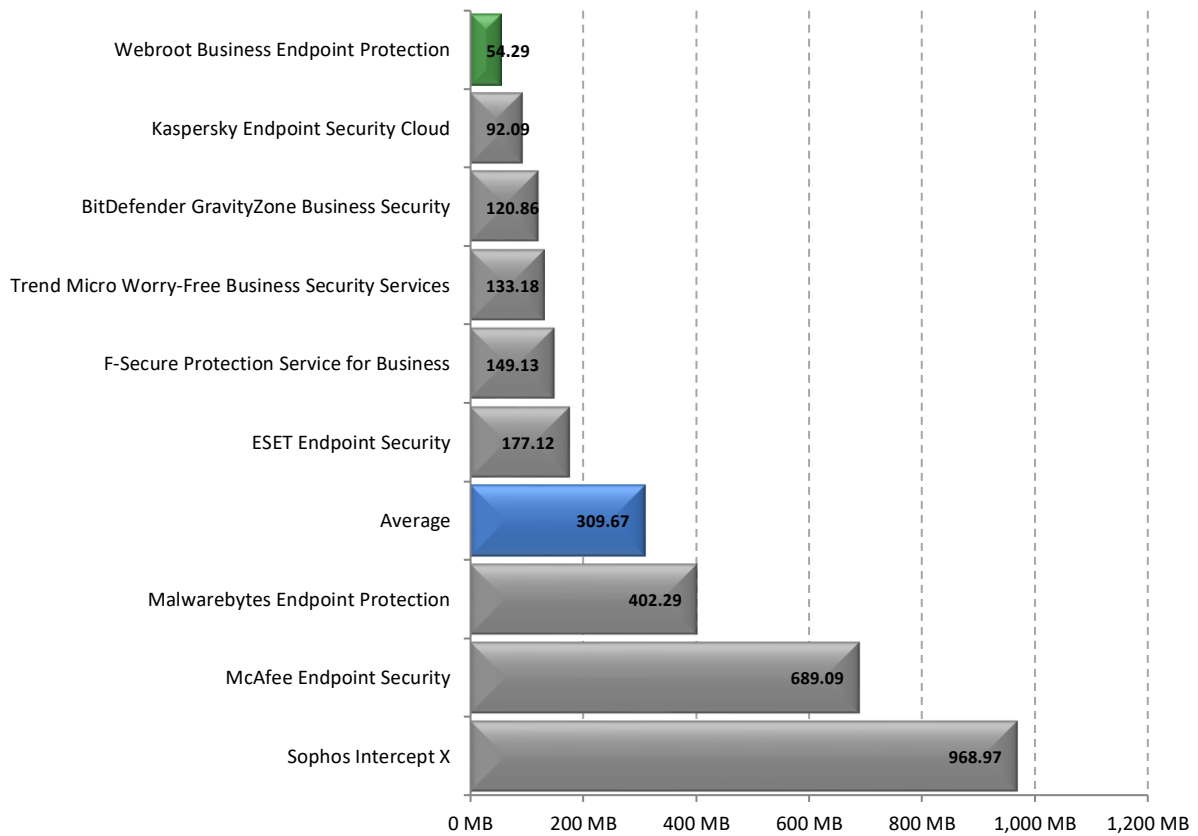
Benchmark 5 – CPU Usage during Scan

The following chart compares the average CPU usage during an on-demand scan of sample files. Products with lower CPU usage are considered better performing products in this category.



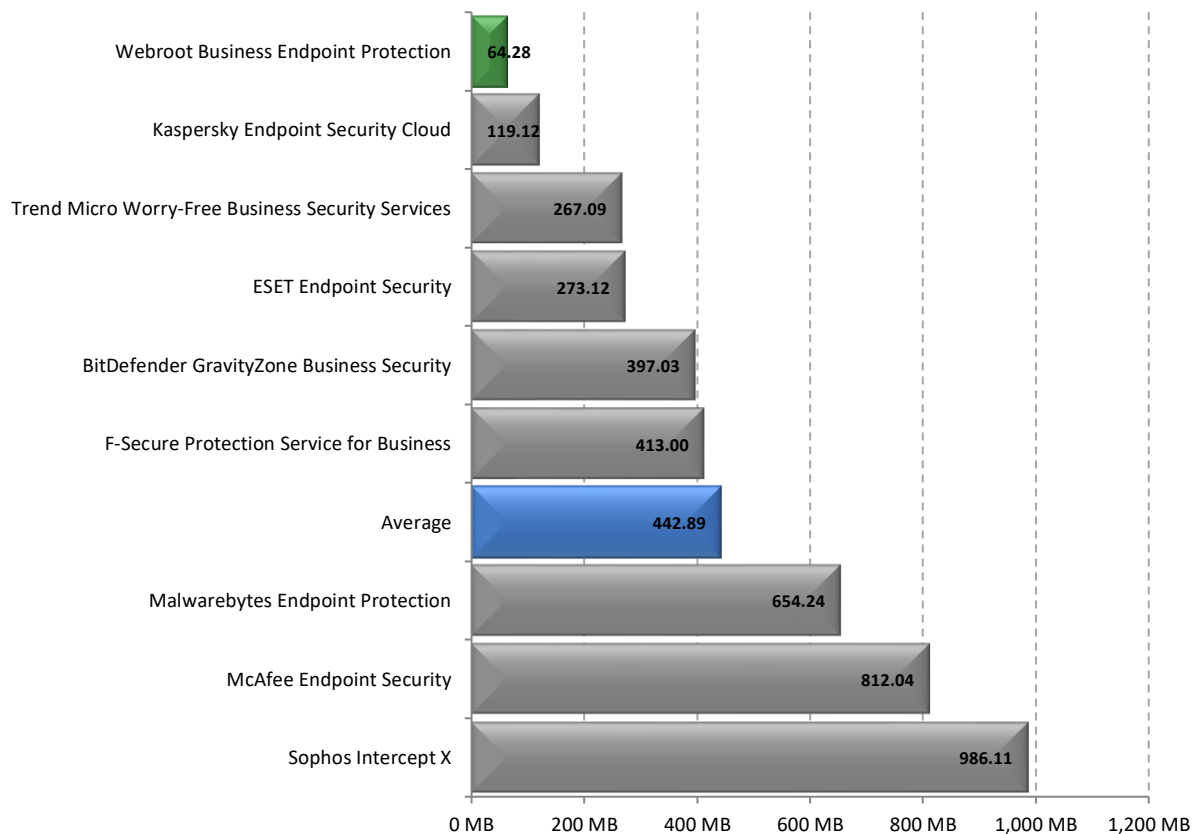
Benchmark 6 – Memory Usage during System Idle

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.



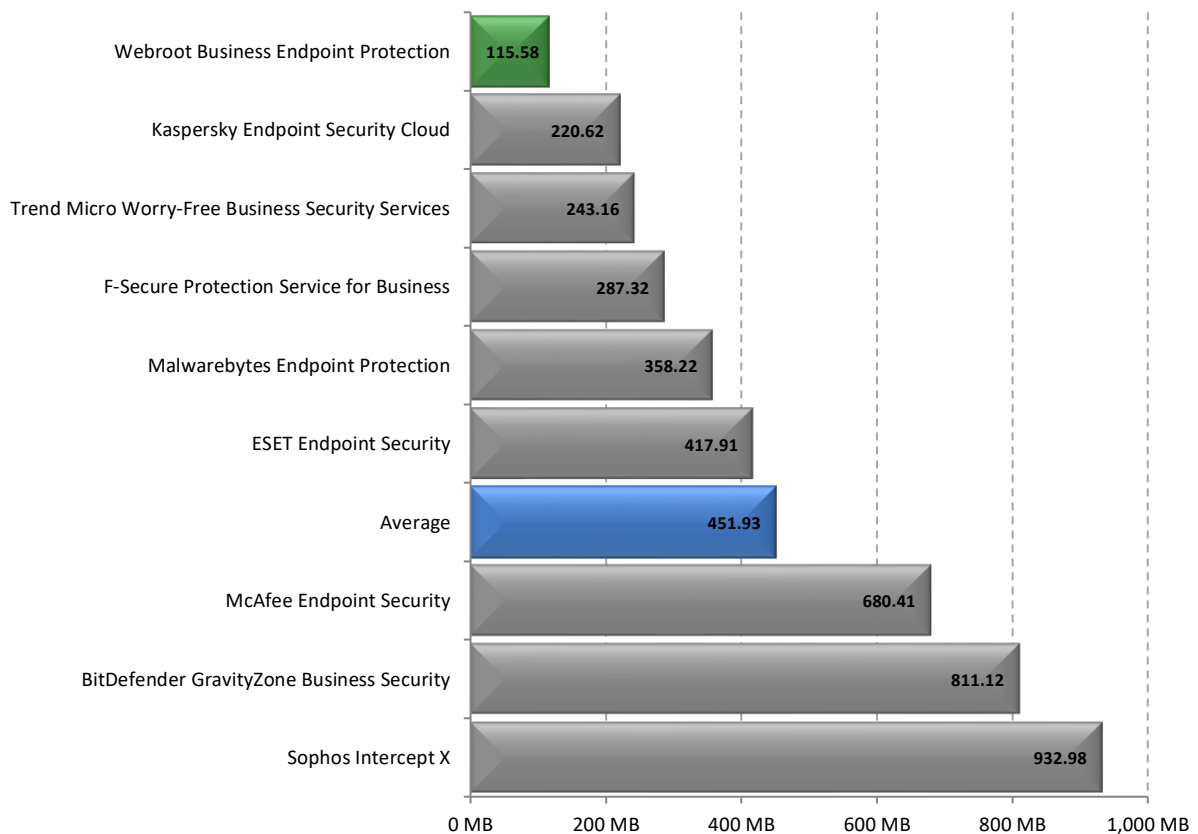
Benchmark 7 – Memory Usage during Initial Scan

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 twelve 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.



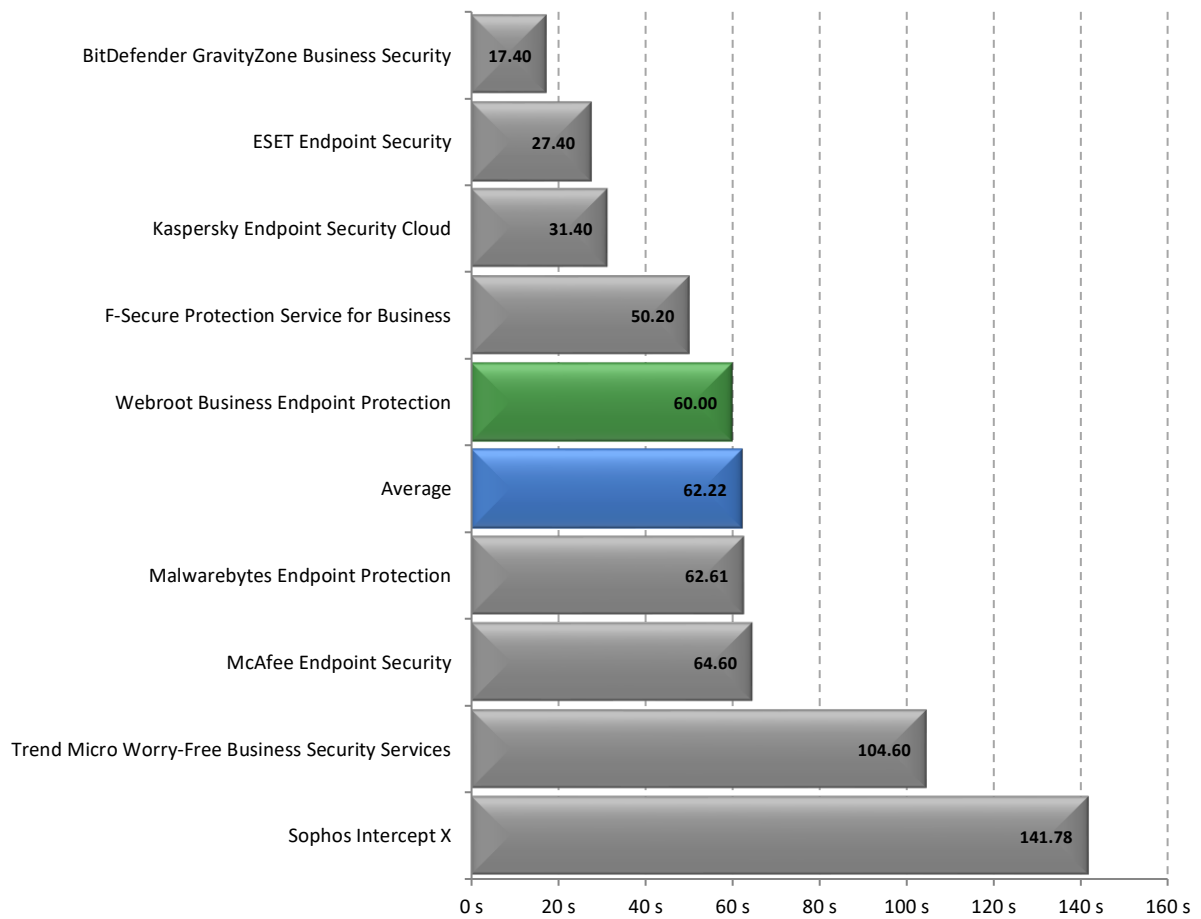
Benchmark 8 – Memory Usage during Scheduled Scan

The following chart compares the average amount of RAM in use by an endpoint security product during a scheduled scan on the endpoint. This average is taken from a sample of five memory snapshots taken at five second intervals. Products that use less memory during a scan are considered better performing products in this category.



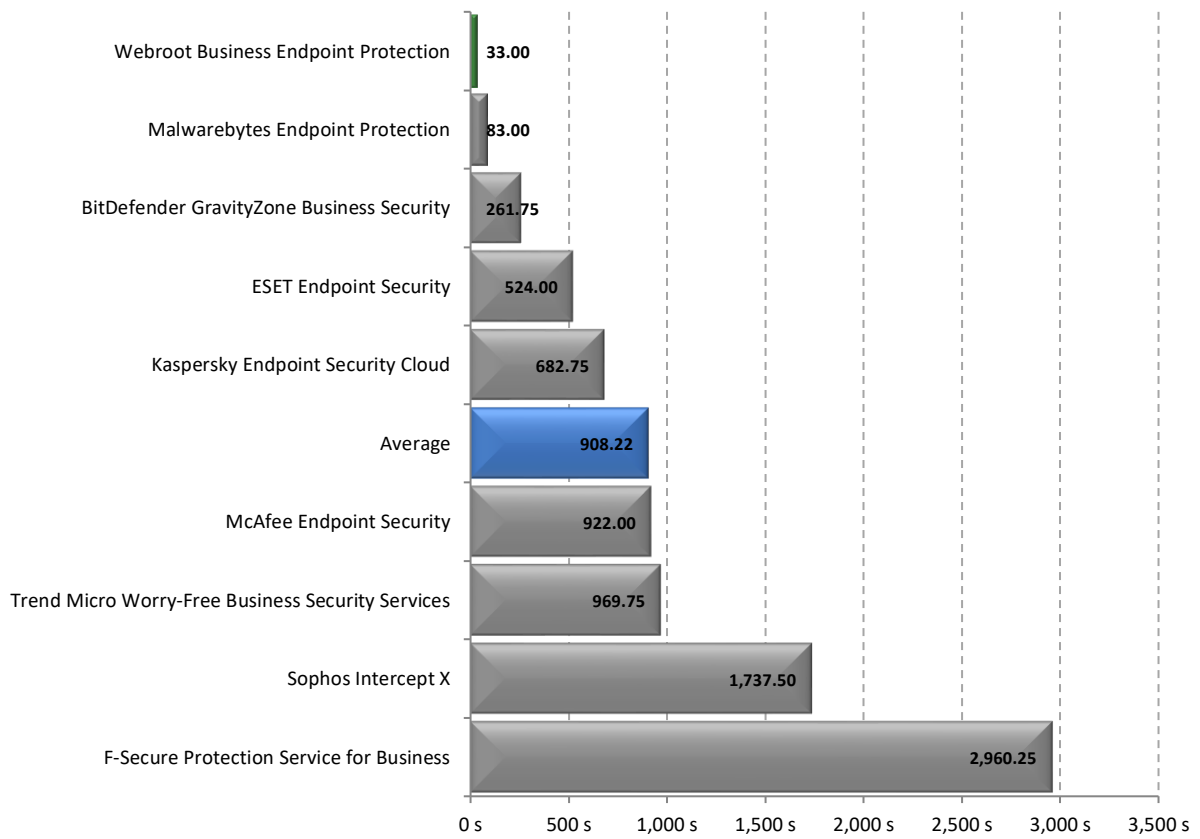
Benchmark 9 – On-Demand Scan Time

The following chart compares the average time taken to run an On-demand scan on the system for each security product tested.



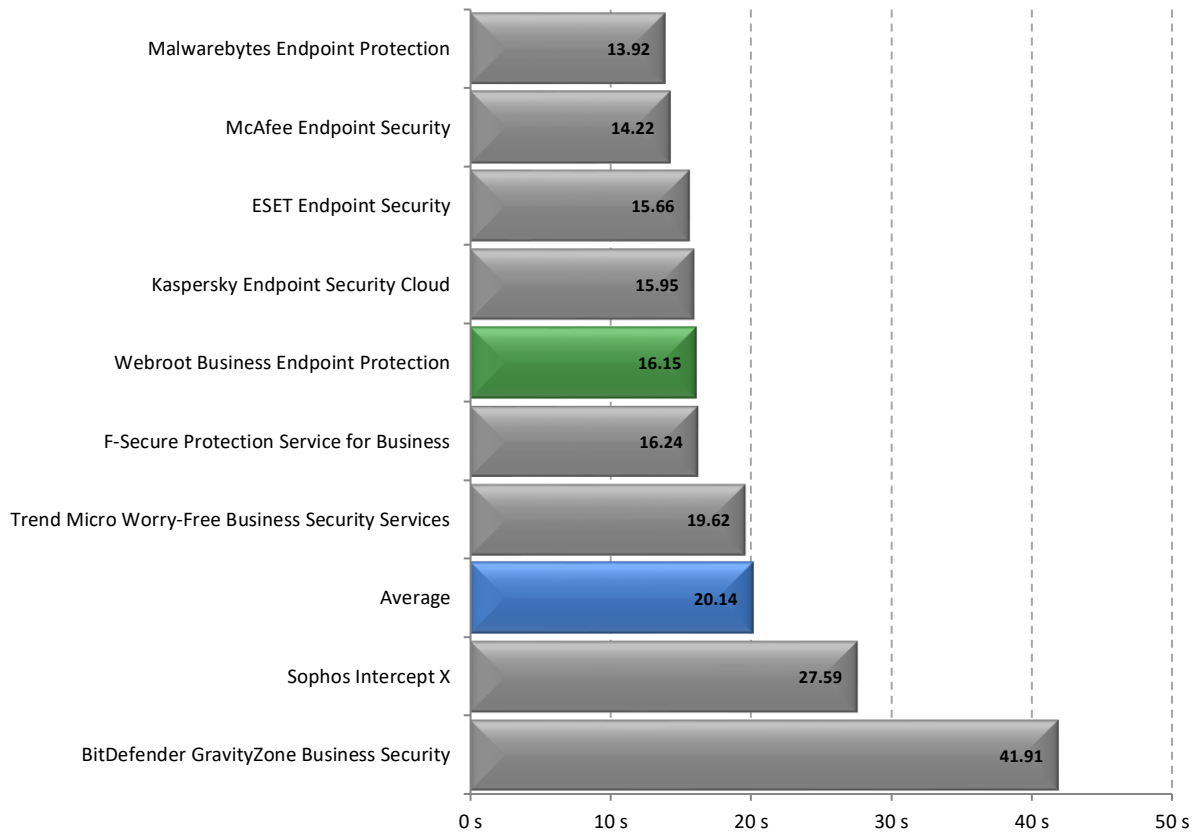
Benchmark 10 – Scheduled Scan Time

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



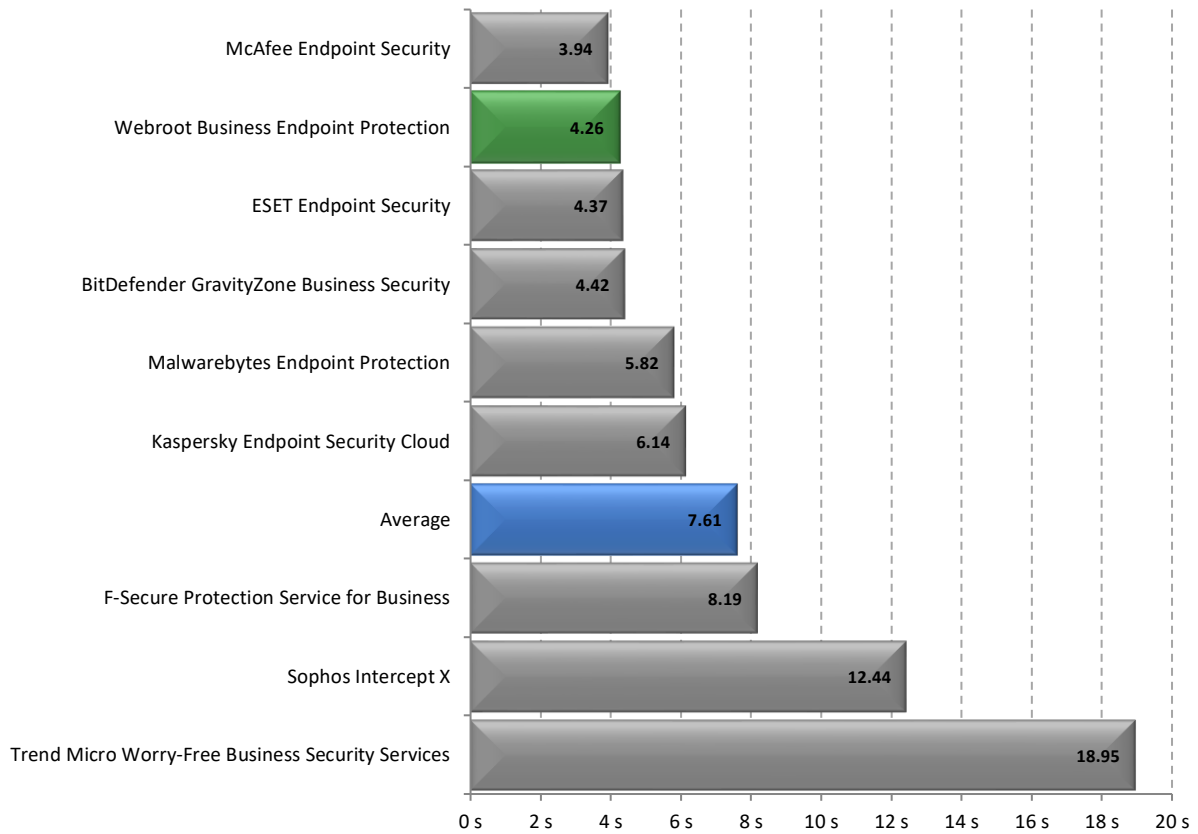
Benchmark 11 – Browse Time

The following chart compares the average time taken for Microsoft Edge 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.



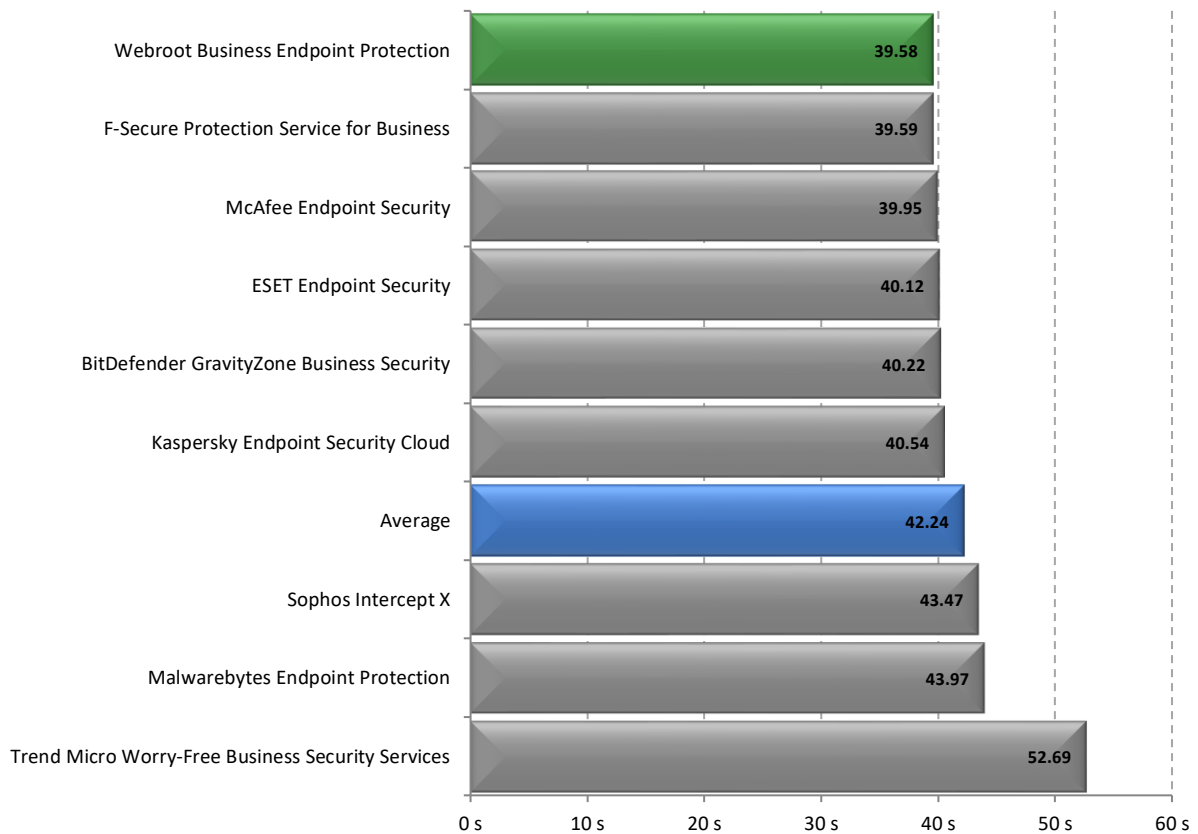
Benchmark 12 – File Copy, Move, and Delete

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.



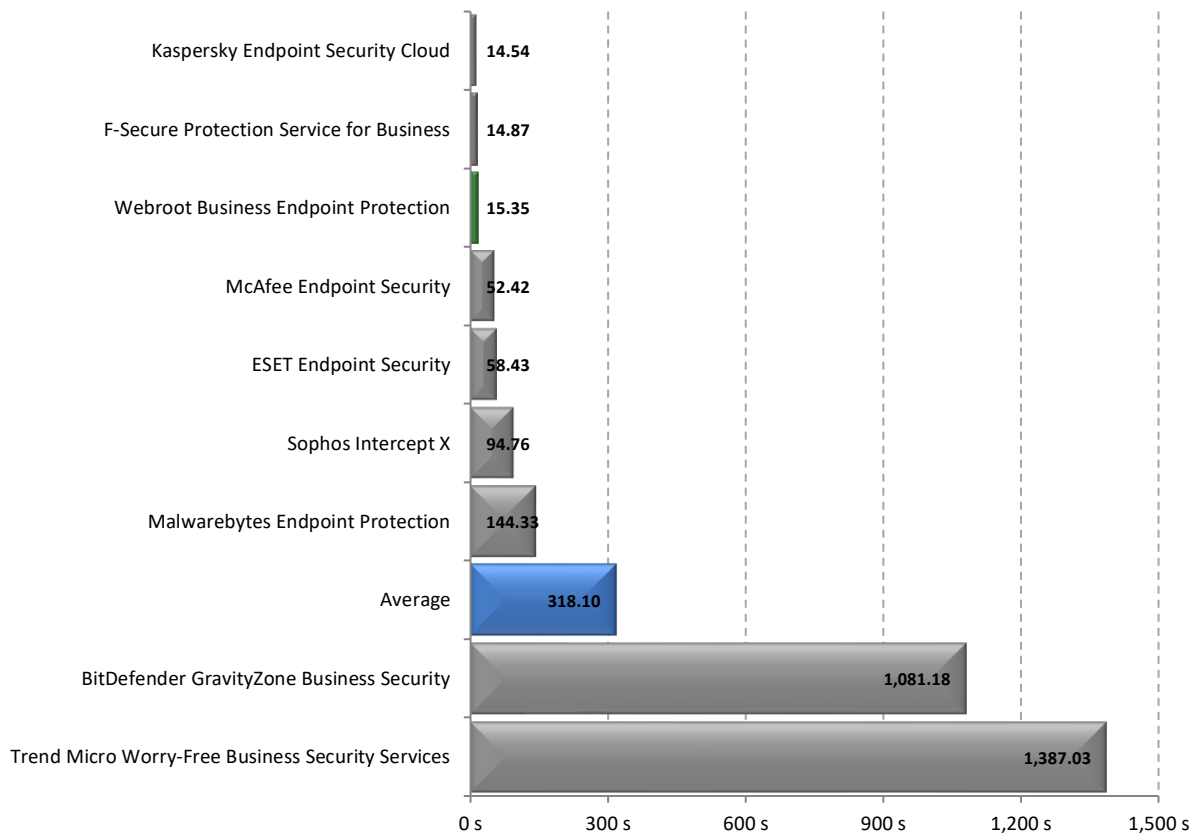
Benchmark 13 – File Compression and Decompression

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.



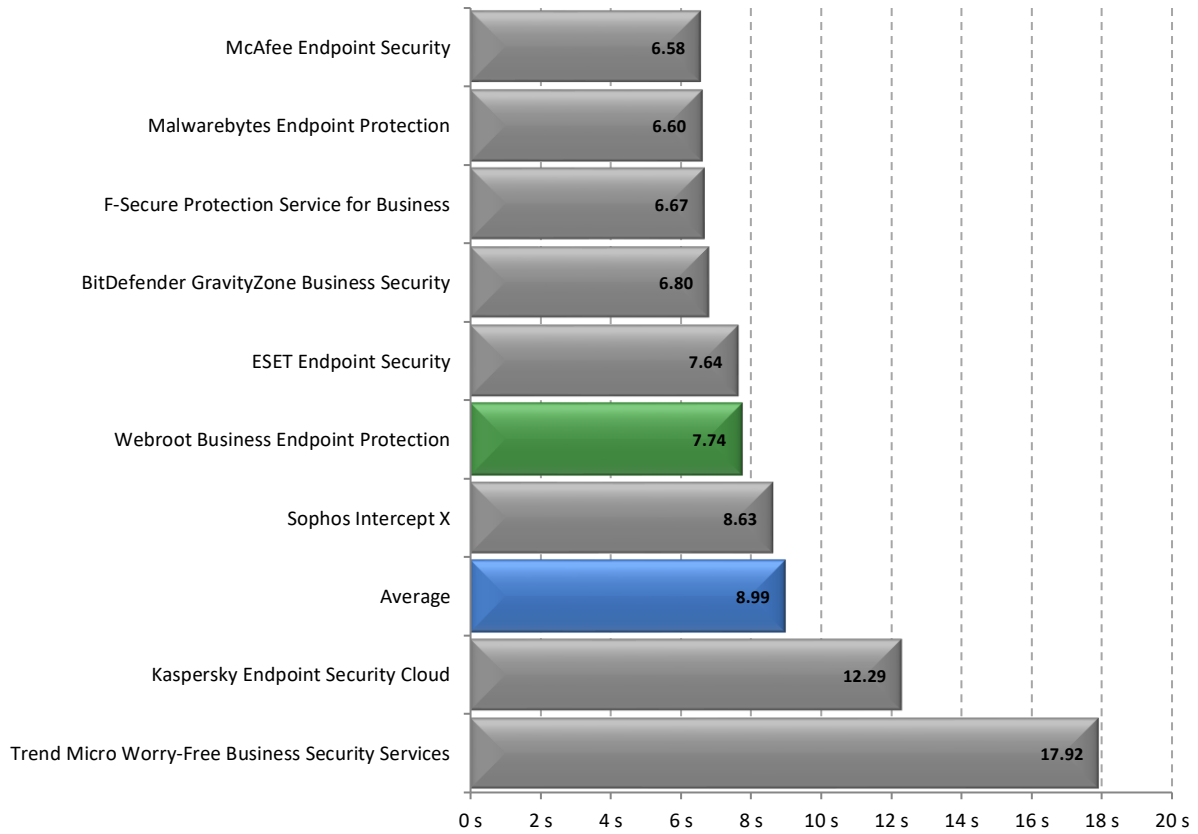
Benchmark 14 – File Write, Open, and Close

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 15 – 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 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 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

Level 5

63 Foveaux St.

Surry Hills, 2010

Sydney, Australia

Phone + 61 (2) 9690 0444

Fax + 61 (2) 9690 0445

Web <https://www.passmark.com>

Appendix 1 – Test Environment

Endpoint Machine

Model:	Lenovo H50W-50 i5
CPU:	Intel Core i5-4460 CPU @ 3.20GHz
Video Card:	NVIDIA GeForce GT 705
RAM:	8GB DDR3 RAM
SSD (Main Boot Drive):	Samsung SSD 850 PRO 512 GB
2nd Drive:	Samsung SSD 850 PRO 512 GB
3rd Drive:	Seagate HDD 1TB (7200RPM)
Network:	1Gbps (Connected via Gigabit Ethernet cable)
O/S:	Windows 10 Pro Version 2004

Web Server

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

Motherboard:	Intel S1200BTL Server
CPU:	Intel Xeon E3-1220v2 @ 3.10 GHz
Video Card:	Intel Integrated Graphics Card
RAM:	8GB (2 x 4GB) ECC RAM, 1333Mhz
Hard Drive:	SSD 128GB
Network:	1Gbps (Connected via Gigabit Ethernet cable)
O/S:	Windows Server 2012 Standard

Appendix 2 – Methodology Description

Windows 10 Image Creation

As with testing on Windows 10, *Macrium Reflect* 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 Pro**.
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 test) 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** we created initial and post-installation disk signatures for each product. These disk signatures recorded the number 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 run 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 – 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 On-Demand Scan Time test was being conducted. The final result was calculated as an average five sets of thirty CPU load samples.

Benchmark 6 – 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 7 – Memory Usage during Initial Scan

The **MemLog++** 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 **MemLog++** 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 **MemLog++** utility, enabling **MemLog++** to record memory usage for 120 seconds at 12 second intervals.

Benchmark 8 – Memory Usage during Scheduled Scan

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

A scheduled scan is configured on the target endpoint and once started, the **MemLog++** utility is launched, enabling **MemLog++** to record memory usage for 120 seconds at 12 second intervals.

Benchmark 9 – On-Demand Scan Time

On-Demand Scan Time is the time it took for each product to scan a set of sample files. The sample used was identical in all cases and contained a mixture of system files and Office files. In total there were 6166 files whose combined size was 982 MB. 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:

File Format	Number	Total Size
DLL	2589	490 MB
EXE	694	101 MB
SYS	332	23.3 MB
GIF	302	567 KB
DOC	281	64.2 MB
WMF	185	1.78 MB
PNG	149	1.93 MB
HTM/HTML	126	946 KB
CAT	111	7.25 MB
NLS	80	6.63 MB
JPG	70	1.09 MB
INI	59	1.76 MB
ICO	58	58.2 KB
MOF	43	6.12 MB
AX	39	4.48 MB
XLS	38	3.62 MB
CFG	36	141 KB
POT	36	2.37 MB
IME	35	5 MB
DRV	31	1.19 MB
TXT	31	366 KB
CHM	30	6.28 MB
OCX	30	6.12 MB
CPL	29	4.42 MB
MFL	29	2.62 MB
INF	26	1.54 MB
TLB	25	2.17 MB
DOT	24	1.55 MB
HLP	22	3.44 MB
IMD	20	18 MB
PY	20	79.2 KB
[NO EXTENSION]	19	3.29 MB
MSC	18	752 KB
VBS	18	838 KB
XML	18	574 KB
RTF	16	62.1 MB
ECF	15	15.6 KB
INC	15	27.3 KB
COM	14	282 KB
DAT	14	1.83 MB
LOG	14	4.53 MB
TSP	14	1.22 MB
XSL	14	44.3 KB
H	12	56.5 KB

File Format	Number	Total Size
FRA	3	880 KB
IQY	3	830 bytes
ISP	3	601 bytes
ITA	3	930 KB
MB	3	4.36 MB
MML	3	771 KB
MMW	3	946 KB
NLD	3	1.11 MB
RAR	3	1.91 MB
ROM	3	54.1 KB
SIG	3	19.8 KB
SVE	3	993 KB
TTF	3	580 KB
ACS	2	3.8 MB
C	2	28.5 KB
CMD	2	1.6 KB
LO_	2	128 KB
LXA	2	1.19 MB
MAP	2	3.72 KB
MDB	2	516 KB
MMF	2	1.92 KB
MSI	2	1.65 MB
NT	2	4.16 KB
OBE	2	13.9 KB
ODC	2	386 bytes
POL	2	488 bytes
RLL	2	112 KB
TAB	2	160 KB
TSK	2	2.25 KB
XLA	2	79 KB
ACL	1	37 KB
BMP	1	234 KB
BTR	1	1.25 MB
BUD	1	93 KB
CHK	1	8 KB
CHS	1	1.65 KB
CHT	1	1.65 KB
CNV	1	52 KB
CPI	1	124 KB
DATA	1	5.99 MB
DB	1	17.5 KB
DBL	1	2.13 KB
DHS	1	138 bytes
DICT	1	18 KB

TBL	13	606 KB
AW	12	2.59 MB
FAE	12	1.02 MB
JS	12	429 KB
SCR	12	2.5 MB
VSD	12	1.67 MB
ZIP	11	25.2 MB
[HIDDEN FILES]	11	-
PNF	10	1 MB
ACM	9	836 KB
ICM	9	192 KB
LEX	9	10.3 MB
PPT	9	4.46 MB
MANIFEST	8	5.96 KB
UCE	8	240 KB
ACG	7	780 KB
OLB	7	1.34 MB
WAV	7	5.03 MB
WIZ	7	1.11 MB
BIN	6	25 MB
GPD	6	112 KB
CNT	5	4.15 KB
DUN	5	2.46 KB
MPP	5	1.83 MB
PIP	5	12.5 KB
SAM	5	305 KB
ADM	4	1.64 MB
BAT	4	22.4 KB
CPX	4	6.46 KB
FON	4	61.3 KB
SCP	4	8.53 KB
SEP	4	6.79 KB
CSS	3	11.4 KB
DEU	3	1.45 MB
DTD	3	22.6 KB
ENU	3	999 KB
ESN	3	815 KB

DIZ	1	428 bytes
DLS	1	3.28 MB
DPC	1	414 bytes
ENG	1	751 bytes
GRA	1	182 KB
HOL	1	269 KB
HTC	1	28 KB
HXX	1	6.55 KB
ICS	1	375 bytes
IMG	1	66.2 KB
JPN	1	2.01 KB
KOR	1	2 KB
LOCAL	1	0 bytes
MOD	1	2.03 KB
MST	1	3.99 MB
NVU	1	2.74 KB
OPS	1	2.26 KB
PAT	1	42 bytes
PRF	1	6.62 KB
PRO	1	20.7 KB
RAM	1	64 bytes
RAT	1	3.09 KB
RSP	1	4.19 KB
SCF	1	75 bytes
SDB	1	1.03 MB
SDF	1	888 bytes
SLL	1	471 KB
SPD	1	1.6 MB
SQL	1	748 KB
SVG	1	77.5 KB
THA	1	697 bytes
TPL	1	10.5 KB
TRM	1	4 KB
VXD	1	81 bytes
WMA	1	2.5 MB
WMV	1	649 KB
WSC	1	39.5 KB
Total	6166	982 MB

This scan was run without launching the product's user interface, by right clicking the test folder and choosing the "Scan Now" option. 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.

In previous years of testing, we noticed many more products showing a substantial difference between the initial scan time (first scan) and subsequent scan times (scans 2 to 5). We believe this behavior is due to products themselves caching recently scanned files. As a result of this mechanism, we have averaged the four subsequent scan times to obtain an average subsequent scan time. Our final result for this test is an average of the subsequent scan average and the initial scan time.

Benchmark 10 – Scheduled Scan Time

This scan is configured as a full system scheduled scan from user interface or management console. The default 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. In the past, many products have shown a substantial difference between the initial scan time (first scan) and subsequent scan times (scans 2 to 5). We believe this behavior is due to products themselves caching recently scanned files. As a result of this mechanism, we have averaged the four subsequent scan times to obtain an average subsequent scan time. Our final result for this test is an average of the subsequent scan average and the initial scan time. Where this option is not available, the product is omitted from the metric, and given the lowest score for this metric.

Benchmark 11 – 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 108 '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 *Microsoft Edge* (version 89.0.774.57) 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 12 – 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. 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	Total Size
DOC	24	91.6 MB
DOCX	12	48.8 MB
PPT	9	126 MB
PPTX	9	74.4 MB
XLS	12	51.5 MB
XLSX	12	14.6 MB
PDF	219	323 MB
JPG	1045	135 MB
GIF	27	82.4 MB
PNG	5	483 KB
MOV	7	54.7 MB
RM	1	5.39 MB
AVI	24	130 MB

File Format	Number	Total Size
WMV	5	43.9 MB
MP3	84	356 MB
EXE	38	5.62 MB
DLL	208	56.6 MB
AX	2	36 KB
CPL	4	4.02 MB
CPX	4	8.56 KB
DRV	20	302 KB
ICO	2	210 KB
MSC	2	81.2 KB
NT	2	3.28 KB
ROM	4	71.4 KB
SRC	4	4.28 MB
SYS	4	88.12 KB
TLB	6	264 KB
TSK	2	2.24 KB
UCE	2	44.8 KB
Total	1800	1.57 GB

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 13 – File Compression and Decompression

This test measured the amount of time required to compress and decompress a sample set of files. *CommandTimer.exe* tool recorded the amount of time required for *7zip.exe* to compress the files into a *.zip and subsequently decompress the created *.zip file.

A breakdown of the file types and numbers in the sample dataset is as follows:

File Type	Number	Total Size
Document Files	78	97.9 MB
Image Files	1073	113 MB
Video Files	65	568 MB
Total	1216	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 14 – File Write, Open, and Close

This benchmark was derived from Oli Warner's File I/O test at <http://www.thepcspsy.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 15 – 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.

This data set contains 242 files. A breakdown of the file types is as follows:

File Type	Number	Total Size
Image Files	182	16.2 MB
Music Files	10	70.8 MB
Video Files	9	73.4 MB
PDF Files	36	56.8 MB
Compressed Archive Files	5	6.09 MB
Total	242	223.29 MB

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.