PASSMARK® SOFTWARE

# Consumer Internet Security Products Performance Benchmarks (Oct 2011)

## ESET vs. 10 Competitors


**Document:** Consumer Internet Security Products – Performance Benchmarks (Oct 2011)
**Authors:** C. Richards, I. Robinson, D. Wren
**Company:** PassMark Software


**Date:** 11 October 2011
**Edition:** Edition 2
**File:** ESet_vs_10_Competitors_InternetSecuritySuites-Oct2011.docx

# Table of Contents

**TABLE OF CONTENTS** ..... **2**
**REVISION HISTORY** ..... **3**
**REFERENCES** ..... **3**
**EXECUTIVE SUMMARY** ..... **4**
**RANKING** ..... **5**
INTERNET SECURITY SOFTWARE ..... 5
**TASK DESCRIPTION** ..... **6**
HARDWARE ENVIRONMENTS ..... 6
PRODUCTS AND VERSIONS TESTED ..... 6
**PERFORMANCE BENCHMARK RESULTS** ..... **7**
**DISCLAIMER AND DISCLOSURE** ..... **12**
DISCLAIMER OF LIABILITY ..... 12
DISCLOSURE ..... 12
TRADEMARKS ..... 12
**CONTACT DETAILS** ..... **12**
**APPENDIX A – METHODOLOGY DESCRIPTION** ..... **13**

# Revision History

| Rev | Revision History | Date |
|---|---|---|
| Edition 1 | Initial version of this report, includes new test, new test methods and new results for all products listed in report. | 13 September 2011 |
| Edition 2 | Updated to include McAfee Internet Security 2012. | 11 October 2011 |

# References

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

# Executive Summary

PassMark Software® conducted objective performance testing on eleven (11) Internet Security software products on Windows 7 Ultimate Edition (64-bit) between July 2011 and October 2011. This report presents our results and findings as a result of performance benchmark testing conducted for these consumer internet security products.

Subsequent editions of this report will include new products released as they are made available. For more details on which versions were tested, please see the section *"Products and Versions"*.

Testing was performed on all products using fourteen (14) performance metrics[1]. These performance metrics are as follows:

- Boot Time;
- Average Scan Time;
- Subsequent Scan Time (before Restart);
- User Interface Launch Time;
- Memory Usage during System Idle;
- Peak Memory Usage (during Update and Scan);
- Internet Explorer Launch Time;
- Installation Size;
- Installation Time;
- New Registry Keys Added;
- Installation of Third Party Applications;
- Network Throughput;
- File Format Conversion; and
- File Write, Open and Close.

[1] PassMark Software produces benchmark reports for numerous software vendors. The list of products and benchmarks used is at the discretion of the vendor and so may not be directly comparable between future or past reports.

# Ranking

PassMark Software assigned every product a score depending on its ranking in each metric compared to other products in the same category.

## Internet Security Software

In the following table the highest possible score attainable is 154 in a hypothetical situation where a product has attained first place in all 14 metrics.

Internet Security products have been ranked by their overall scores:

| Product Name | Overall Score |
|---|---|
| ESET Smart Security 5 | 116 |
| Avira Premium Security Suite | 105 |
| Norton Internet Security 2012 | 103 |
| Kaspersky Internet Security 2012 | 98 |
| AVG Internet Security 2011 | 80 |
| F-Secure Internet Security 2011 | 80 |
| McAfee Internet Security 2012 | 78 |
| Trend Micro Titanium Internet Security 2011 | 73 |
| BitDefender Internet Security 2011 | 66 |
| G Data Internet Security 2012 | 62 |
| Panda Internet Security 2012 | 62 |

# Task Description

PassMark Software has conducted performance benchmark testing and subjective comparative analysis on eleven (11) consumer internet security software products.

## Hardware Environments

The following hardware platforms were used in conducting our comparative analysis and performance tests, and are intended to represent a typical client machine deployment:

### Client Machine Specification

**Operating System:** Windows 7 Ultimate x64 (Service Pack 1)
**CPU:** Intel Core i5 750 Quad Core @ 2.67GHz
**Motherboard:** Gigabyte P55-UD3R Motherboard
**RAM:** 4 GB DDR3
**HDD:** Western Digital 500GB 7200RPM (WD5000AAKX)

### Server Machine Specification

**Operating System:** Windows Server 2008 R2 64-bit (Service Pack 1)
**CPU:** Phenom X4 @ 3.00GHz
**Motherboard:** A-Bit A-N78HD
**RAM:** 2 GB DDR2
**HDD:** Western Digital 500GB 7200RPM (WD5000AAKX)

## Products and Versions Tested

| Manufacturer | Product Name | Release Year | Product Version | Date Tested |
|---|---|---|---|---|
| AVG Technologies | AVG Internet Security 2011 | 2011 | Current 10.0.1390 | Jul 2011 |
| Avira | Avira Premium Security Suite | 2011 | Current 10.2.0.659 | Jul 2011 |
| BitDefender | BitDefender Internet Security 2011 | 2010 | Current 14.0.30.357 | Aug 2011 |
| ESET LLC | ESET Smart Security 5 | 2011 | Current 5.0.90.0 | Jul 2011 |
| F-Secure Corporation | F-Secure Internet Security 2011 | 2010 | Current 10.51.106 | Jul 2011 |
| G Data Software AG | G Data Internet Security 2011 | 2011 | Current 22.0.2.25 | Jul 2011 |
| Kaspersky Labs | Kaspersky Internet Security 2011 | 2011 | Current 12.0.0.374 | Jul 2011 |
| McAfee | McAfee Internet Security 2011 | 2011 | Current 5.0.259.0 | Oct 2011 |
| Panda Security | Panda Internet Security 2011 | 2011 | Current 17.00.00 | Jul 2011 |
| Symantec Corporation | Norton Internet Security 2012 | 2011 | Current 19.1.0.21 | Sep 2011 |
| Trend Micro Inc | Trend Micro Titanium Internet Security 2011 | 2010 | Current 3.1.1109 | Aug 2011 |

# Performance Benchmark Results

The following performance categories have been selected as 'real-life' metrics which may impact heavily on system performance and responsiveness. These benchmarks allow the comparison of the level of impact that internet security software products may have on client machines. Products with good performance will have less impact on client machine activities, workflow and productivity.

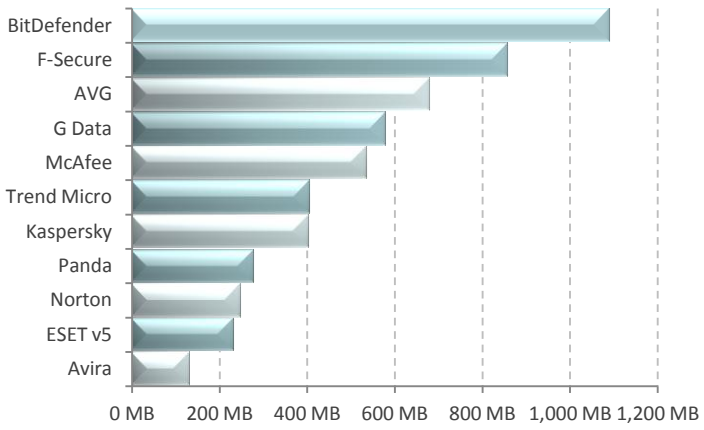
More detailed description of the methodology used can be found in **Appendix A – Performance Methodology**.

## Installation Size

***Protect your system without filling up disk space***

In offering new features and functionality to users, internet 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 users.

*This metric measures the total additional disk space consumed by the client after installation and a manual update. Our final result is measured in megabytes (MB).*

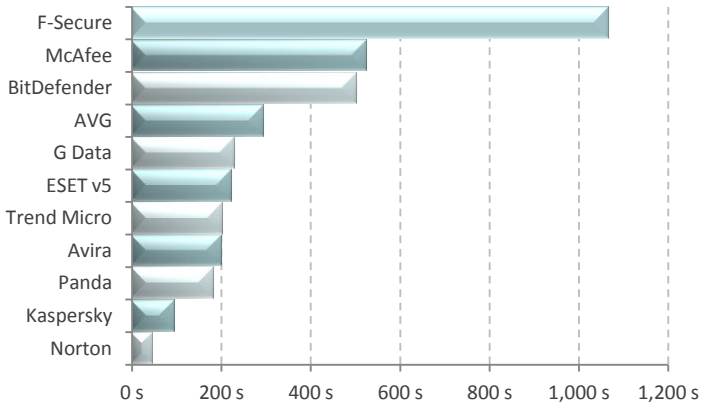



## Installation Time

*Spend less time waiting for product install*

The speed and ease of the installation process will strongly influence the user's first impression of the internet security software.

*The following chart compares the minimum installation time it takes for Internet 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.*

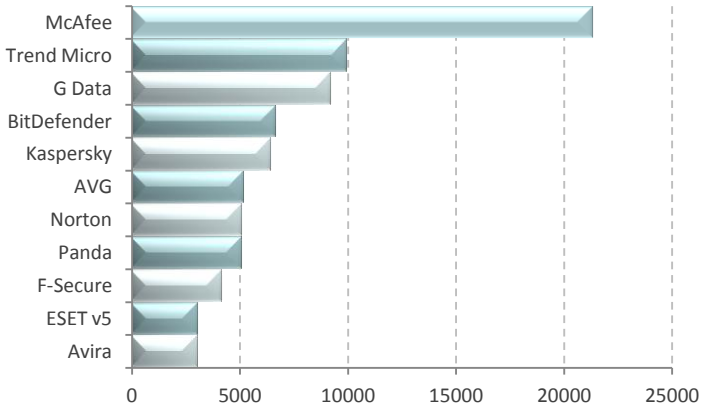



## Registry Key Count

***Improve system performance***

A large registry increases a machine's use of resources. This may negatively impact system performance, especially on much older machines.

*The following chart compares the amount of Registry Keys created during product installation for each Internet Security product tested. Products with lower key counts are considered better performing products in this category.*

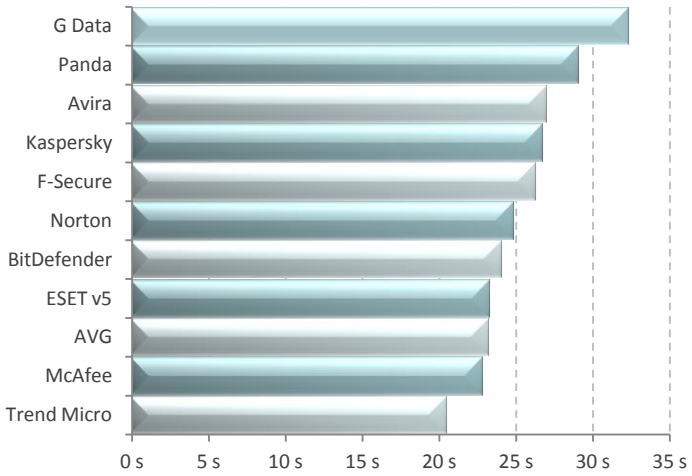


## Boot Time

***Spend less time waiting for your system to start***

Many internet security software suites create start up tasks and processes, causing machine boot times to take significantly longer. End users can do little but wait for their machine to become responsive. Better performing products will have less of an impact on boot time.

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

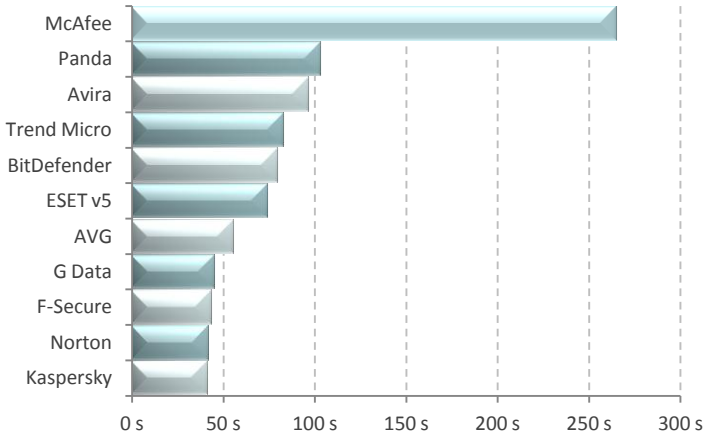



## Average scan time

***Reduce the time taken to scan your system***

Many internet security software suites have ways of remembering safe files that have been previously been scanned since product installation, reducing the time it takes to rescan them. This metric measured the average amount of time required to run and initial scan and then run a subsequent scan on a set of clean files, with a restart occurring after the previous scan to remove file caching effects. Our sample file set comprised of files that would typically be found on end-user machines, such as media files, system files and Microsoft Office documents. The initial scan time while forming part of the average is not included in this report.

*The following chart compares the average time taken to scan a set of 8052 files (totalling 5.4 GB) for each Internet Security product tested. This time is calculated by averaging the initial scan time with 5 subsequent scans performed with a restart since the previous scan. Products with lower scan times are considered better performing products in this category.*

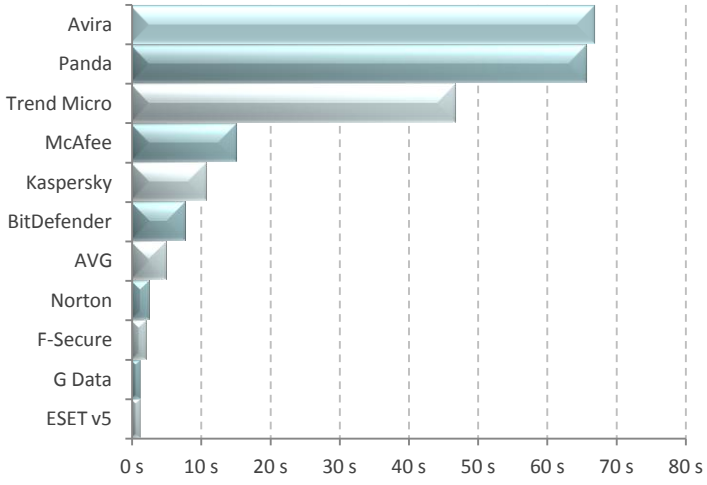



## Subsequent Scan time (before restart)

***Reduce the time taken to scan your system***

Many internet security software suites will remember safe files that have been previously scanned, and their behaviour in rescanning these files can be affected by whether the system has been restarted since the previous scan. This, along with file caching effects, will in general, give a quicker scan time for a scan that has been run with no restart since the previous scan on that same set of files.

*The following chart compares the average time taken to scan a set of 8052 files (totalling 5.4 GB) for each Internet Security product tested. This time is calculated by averaging 5 subsequent scans performed without a restart since the previous scan. Products with lower scan times are considered better performing products in this category.*

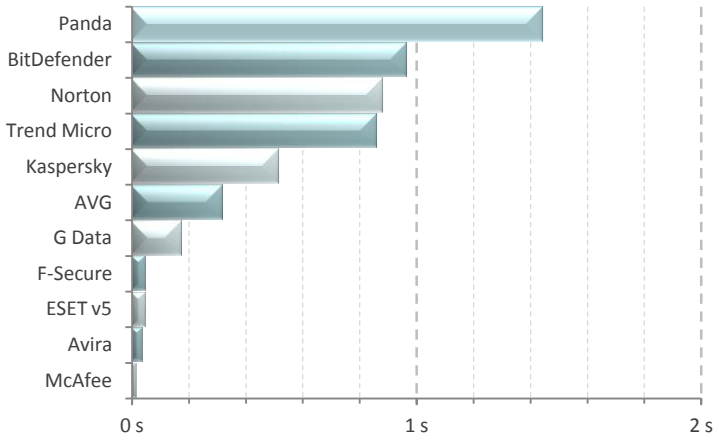


## UI Launch Time

*Spend less time waiting for product launch*

This metric provides an objective indication as to how responsive an internet security product appears to the user, by measuring the amount of time it takes for the user interface of the internet security software to launch from Windows.

*The following chart compares the average time taken to launch a product's user interface. Products with lower launch times are considered better performing products in this category.*

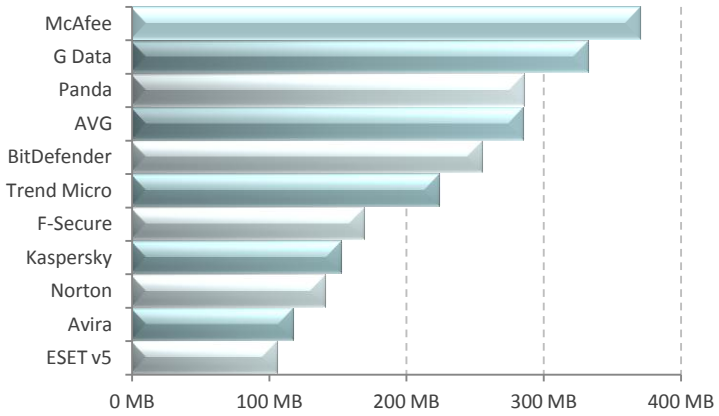



## Memory Usage during System Idle

*Have more system resources to perform tasks*

The amount of memory used while the machine is idle provides a good indication of the amount of system resources being consumed by the internet security software.

*The following chart compares the average amount of RAM in use by an Internet 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.*

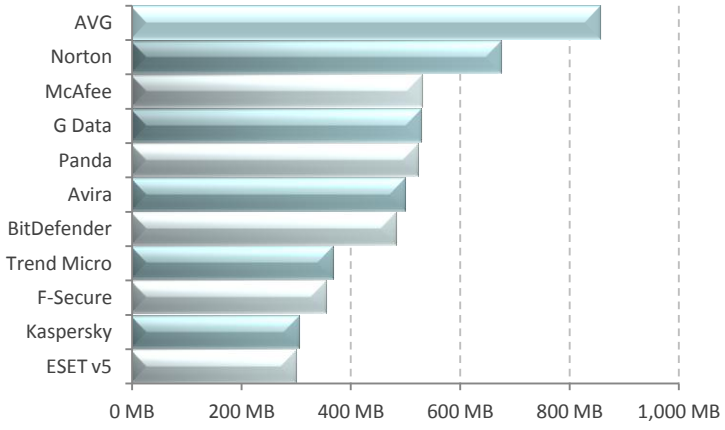



## Peak Memory Usage

*Reduce the memory footprint of your product*

The amount of memory used while the machine is performing an update and scan provides a good indication of the amount of system resources being consumed by the internet security software. Better performing products occupy less memory while the machine is performing an update and scan operation.

*The following chart compares the average amount of RAM in use by an Internet Security product during an update and scan operation. This average is taken from a sample of 25 memory snapshots taken at roughly 60 seconds apart. Products with lower RAM usage are considered better performing products in this category.*

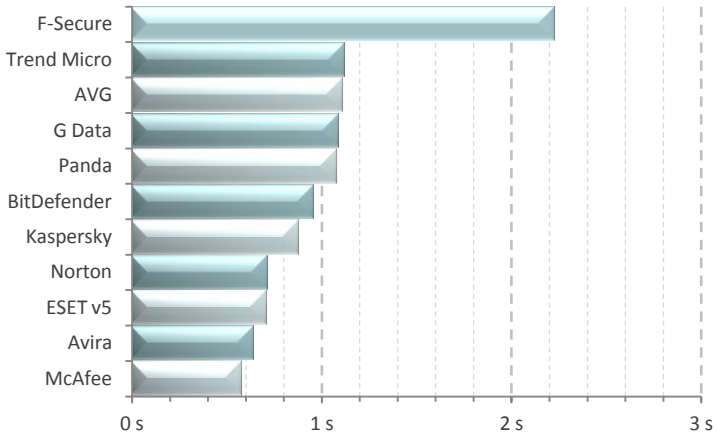


## Internet Explorer 8 Launch Time

*Spend less time waiting for IE8 to launch*

This metric is one of many methods to objectively measure how much an internet security product impacts on the responsiveness of the system. This metric measures the amount of time it takes to launch the user interface of Internet Explorer 8. To allow for caching effects by the operating system, both the initial launch time and the subsequent launch times were measured.

*The following chart compares the average launch times of Internet Explorer after rebooting the machine for each Internet Security product we tested. Products with lower launch times are considered better performing products in this category.*

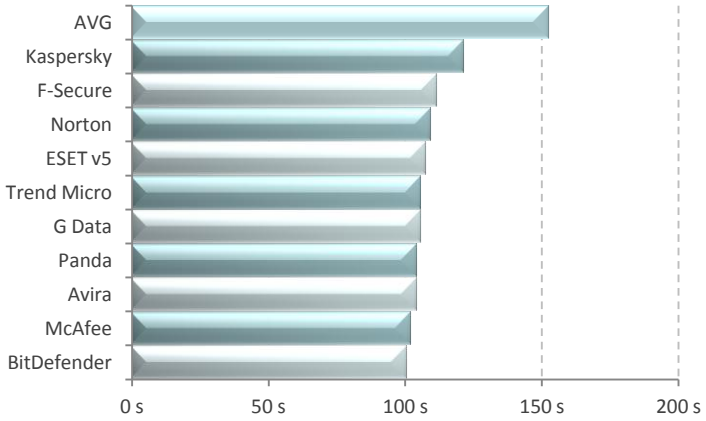



## Installing Third Party Applications

*Spend less time waiting for application install*

The installation speed of third party applications may be impacted by antivirus behaviour such as heuristics or real time malware scanning.

*The following chart compares the average time taken to install a third party application for each Internet Security product tested. Products with lower times are considered better performing products in this category.*

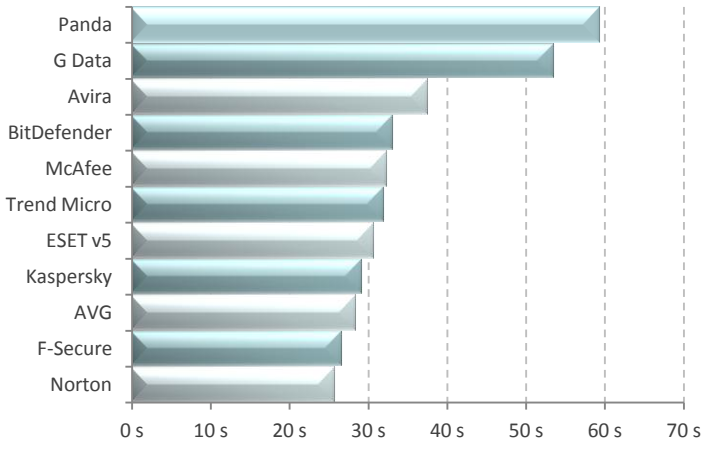



## Network Throughput

*Minimize impact on internet downloads*

This 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.

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

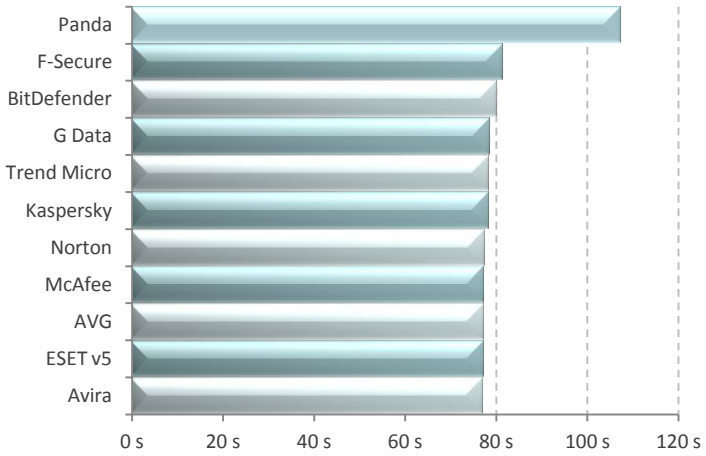


## File Format Conversion

*Convert files faster*

This test measures the amount of time taken to convert an MP3 file to a WAV and subsequently, convert the same MP3 file to a WMA format.

*The following chart compares the average time it takes for a sample file to be converted from one file format to another (MP3⇢ WMA, MP3⇢ WAV) for each Internet Security product tested. Products with lower times are considered better performing products in this category.*



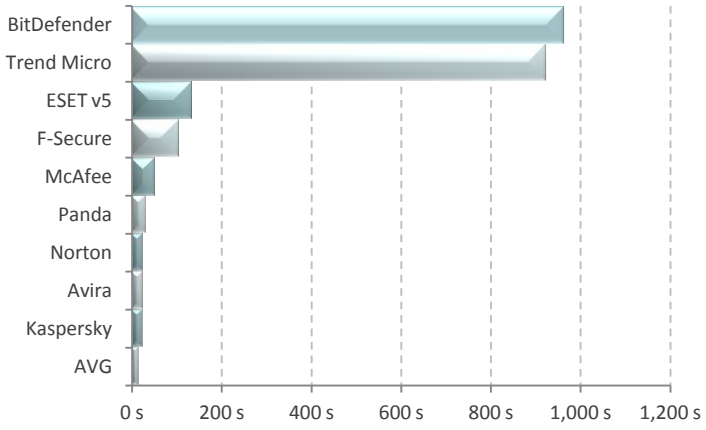

## File Write, Open and Close

*Minimize time taken to open files*

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.

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

*Note: G Data product excluded as the result was off the scale of the chart.*



# Disclaimer and Disclosure

This report covers selected Internet Security products that were available at the time of testing. Version numbers of software reviewed within this document are provided in the "Products and Versions Tested" 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

The production of this report was funded by ESET LLC. The list of products tested and the metrics included in the report were selected by ESET LLC. As such they may not be comparable to future or past reports.

## Trademarks



# Contact Details

**PassMark Software Pty Ltd**
Suite 202, Level 2
35 Buckingham St.
Surry Hills, 2010
Sydney, Australia
**Phone** + 61 (2) 9690 0444
**Fax** + 61 (2) 9690 0445
**Web** www.passmark.com

# Appendix A – Methodology Description

## Windows 7 Image Creation

A Windows 7 Ultimate edition machine was built and ***Norton Ghost*** was used to create a "clean" baseline image prior to testing. Our aim is to create a clean baseline image with the smallest possible footprint and reduce the possibility of variation caused by external operating system factors.

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

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

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

## Benchmark 1 – Boot Time

**Summary**

This metric measures the amount of time taken for the machine to boot into the operating system.

**Methodology**

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

The boot process is first optimized with xbootmgr.exe using the command "xbootmgr.exe -trace boot –prepSystem –resultPath d:\bootlogs\temp" which prepares the system for the test over six optimization boots. The boot traces obtained from the optimization process are discarded.

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

Finally, a post-processing tool will be used to parse the boot traces and obtain the BootTimeViaPostBoot value. This value reflects the amount of time it takes the system to complete all (and only) boot time processes. Our final result will be an average of five boot traces. There is a .bat file in d:\bootlogs by name parse.bat to run the post-processing tool.

## Benchmarks 2 and 3 – Scan Time before Reboot, and Scan Time after Reboot

**Summary** Measure on demand scan times of a file set.

**Methodology:** PassMark Software will perform 11 scans of the sample file set. An initial scan of the file set, some scans without a restart of the machine, and some scans with a restart. The time taken to scan the files is taken from an antivirus product's scan logs, or where logs are not available, manually with a stopwatch. Scans will be launched by right clicking on the folder to be scanned.
The process will be
Step 1: Initial scan after installation
Step 2: Immediately repeat scan without a reboot.
Step 3: Reboot (with interleaving with other tests needing reboot)
Step 4: Repeat scan after reboot has finished and machine idle
Step 5: Goto step 2, repeat loop 5 times for 11 runs in total.

**Final Result:** Two results will be reported. (The initial scan time is excluded from the report).
1) The subsequent scan time, before restart (5 samples per product)
2) The average of the initial and subsequent scan times, after restart (5 samples per product)

## Benchmark 4 – Memory Usage during System Idle

**Summary:** A command-line utility called *sysinfoAvg.exe*, will be used to measure the amount of overall of system memory usage during an idle period.

**Methodology:** As with previous tests performed for ESET, PassMark will use *sysinfoAvg.exe* to take snapshots of the overall system memory usage every minute for ten minutes, starting at boot.

**Final Result:** The final result is calculated as an average of the "working set" size for 10 samples.

## Benchmark 5 – Peak Memory Usage (during Update and Scan)

**Summary:** Measure the product's peak memory usage using an update and a scan.

**Methodology:** Once again, *sysinfoAvg.exe* will be used to measure the overall system memory usage every minute for 25 minutes while an update and a full scan of the C:\ drive is run. i.e. a total of 25 samples will be taken. If both the update and the scan finish before the 25 minutes has ended, then no further values will be taken, assuming that memory usage during idle time is less than when the software is active.

**Final Result:** The final result will be the peak value of the 25 samples.

## Benchmark 6 – Internet Explorer 8 Launch Time

**Summary:** The time required to open IE will be measured.

**Methodology:** The average launch time of the Internet Explorer interface will be taken using *AppTimer*. This test is practically identical to the User Interface launch time test. For each product tested, we will obtain a total of fifteen samples from five sets of three Internet Explorer launches, with a reboot before each set to clear caching effects by the operating system. When compiling the results the first of each set will be separated out so that there will be a set of values for the initial launch after reboot and a set for subsequent launches. For this test, we will use ***Internet Explorer 8*** (Version 8.0.7601.17514) as our test browser.

**Final Result:** We will average the subsequent launch times to obtain an average subsequent launch time. Our final result for this test will be an average of the subsequent launch average and the initial launch time.

## Benchmark 7 – User Interface Launch Time

**Summary:** The time required to open the main window of the AV/IS product will be measured.

**Methodology:** The average launch time of the AV/IS product user interface will be taken using *AppTimer*. For each product tested, we will obtain a total of fifteen samples from five sets of three AV/IS product user interface launches, with a reboot before each set to clear caching effects by the operating system. When compiling the results the first of each set will be separated out so that there is a set of values for the initial launch after reboot and a set for subsequent launches.

**Final Result:** We will average the subsequent launch times to obtain an average subsequent launch time. Our final result for this test will be an average of the subsequent launch average and the initial launch time.

## Benchmark 8 – Installation Time

**Summary:** This test measures the minimum Installation Time a product requires to be fully functional and ready for use by the end user.

**Methodology:** 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 will be copied to the Desktop before initializing installation. Each step of the installation process will be manually timed with a stopwatch and recorded in as much detail as possible. Where input is required by the end user, the stopwatch will be 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 are declined or skipped. Where it was not possible to skip a scan, the time to scan will be 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 will also be installed (e.g. website link checking software as part of an Internet Security Product).

Installation time includes the time taken by the product installer to download components required in the installation. This may include mandatory updates (e.g. Microsoft Security Essentials) or the delivery of the application itself from a download manager (e.g. McAfee Internet Security, BitDefender Internet Security). We have noted in our results where a product has downloaded components for product installation.

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

## Benchmark 9 – Installation Size

**Summary:** Measure the amount of disk space used as a result of installing the product

**Methodology:** PassMark Software will use the *OSForensics* tool to measure the amount of disk space consumed by the installation of internet security software. *OSForensics* is a new version of OSCheck (which was used in past years) which can capture and compare signatures of disks, folders and files. The comparison of signatures in OSForensics displays a list of newly created, modified and deleted files.

OSForensics will be used similarly to OSCheck in last year's testing. An initial disk signature will be taken prior to installation. After installation, the security software will be manually updated to ensure that the software is fully functional. After the update, the test machine will be restarted to clear temporary files, and a subsequent disk signature is taken.

**Final Result:** The final result for the installation size test will be the total size of additional files, and additional space taken as a result of modification of existing files (i.e. files that were larger after software installation). That is, the total size of added files plus modified files will be added to give the final result.

The final result for the installation package size will be the size of the package on disk.

## Benchmark 10 – Registry Key Count

**Summary:** This test measures the amount of keys and values added to registry during the installation of the product

**Methodology:** The test will be conducted using the OSForensics tool, an application which conducts a count of all new, modified, and deleted keys, errors and values under HKEY_LOCAL_MACHINE and HKEY_USERS.

Two registry key counts signatures will be taken, one prior to installation and a second immediately following a reboot after installation.

**Final Result:** To obtain our result, we will take the total number of new registry keys.

## Benchmark 11 – Third Party Program Installation

**Summary:** This test will measure the amount of time taken to install and uninstall three (3) third-party applications.

**Methodology:** Similar to last year's testing, PassMark Software will perform five runs of this test with a machine restart between each run. The test will be executed as part of a batch script, and the time taken to install and uninstall each third party product will be measured and recorded by *CommandTimer.exe*. The 3rd party products need to be scripted so that they can be installed automatically and silently.

**Final Result:** The final result is calculated as an average of five samples.

## Benchmark 12 – Network Throughput

**Summary:** This benchmark measured how much time was required to download a sample set of binary files of various sizes using wget.

**Methodology:** This benchmark will measure how much time will be 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 2008 and IIS 7. CommandTimer.exe will be used in conjunction with GNU Wget (version 1.10.1) to time and conduct the download test.

The complete sample set of files will be 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].

**Final Result:** This test will be conducted five times to obtain the average time to download this sample of files, with the test machine rebooted between each sample to remove potential caching effects.

## Benchmark 13 – File Format Conversion (MP3 → WAV, MP3 → WMA)

**Summary:** Measure the conversion time of MP3 files to WAV and WMA format.

**Methodology:** This test will measure the amount of time taken to convert five MP3 files to WAV then WMA format. The previous year's test converted only one MP3 file. Similar to last year's testing, PassMark Software will perform five runs of this test with a machine restart between each run. The time taken to convert each audio file to each format will be measured and recorded by *CommandTimer.exe*.

**Final Result:** The final result is calculated as an average of five samples.

## Benchmark 14 – File write, open and close

**Summary:** Measure the time required to open and close files on the disk

**Methodology:** 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 will be 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

**Final Result:** The final result is calculated as an average of five samples.