

Anti-Virus Comparative



Performance Test

Impact of Security Software on System Performance

Language: English

May 2015

Last Revision: 30th June 2015

www.av-comparatives.org

Table of Contents



1. Introduction	3
2. Tested products	3
3. Test methods	4
4. Notes and comments	5
5. Test cases	7
6. Test results	7
7. Award levels reached in this test	11
8. Copyright and Disclaimer	12

Introduction

We want to make clear that the results in this report are intended only to give an indication of the impact on system performance (mainly by the real-time/on-access components) of the security products in these specific tests. Users are encouraged to try out the software on their own PC's and see how it performs on their own systems.

Tested products

The following products for 64-bit systems were evaluated (with default settings) in this test¹:

Avast Free Antivirus 2015	F-Secure Internet Security 2015
AVG Internet Security 2015	Kaspersky Internet Security 2015
AVIRA Antivirus Pro 15.0	Lavasoft Ad-Aware Free Antivirus+ 11.6
Baidu Antivirus 5.4 (English)	McAfee Internet Security 2015
Bitdefender Internet Security 2015	Panda Free Antivirus 15.1
BullGuard Internet Security 15.1	Quick Heal Total Security 16.0
Emsisoft Anti-Malware 10.0	Sophos Endpoint Protection 10.3
eScan Internet Security Suite 14.0	Tencent PC Manager 10.4 (English)
ESET Smart Security 8.0	ThreatTrack Vipre Internet Security 2015
Fortinet FortiClient 5.2 (with FortiGate)	Trend Micro Internet Security 2015

For the benefit of readers who are familiar with performance tests done in previous years, we should point out that this test includes both “Antivirus” and “Internet Security” products – both referred to as *security products*. We have tested the product that each manufacturer submits for the protection tests in the Main Test Series. Please note that the results in this report apply only to the specific product versions listed above (i.e. to the exact version numbers and to 64-bit systems). Also, keep in mind that different vendors offer different (and differing numbers of) features in their products.

The following activities/tests were performed under an up-to-date Windows 8.1 64-Bit system:

- File copying
- Archiving / unarchiving
- Installing / uninstalling applications
- Launching applications
- Downloading files
- PC Mark 8 Professional Testing Suite

This year we have not considered encoding/transcoding, as we feel this is no longer relevant.

¹ We used the latest product versions available at time of testing (May 2015). Additionally, Microsoft Windows Defender integrated in Windows 8.1 has also been evaluated.

Test methods

The tests were performed on an HP 350 G1 machine with an Intel Core i5-4210U CPU, 4GB of RAM and SATA II hard disks. The performance tests were done on a clean and fully updated Windows 8.1 64-Bit system (English) and then with the installed security software (with default settings). The tests were done with an active Internet connection to allow for the real-world impact of cloud services/features.

The hard disks were defragmented before starting the various tests, and care was taken to minimize other factors that could influence the measurements and/or comparability of the systems. Optimizing processes/fingerprinting used by the products were also considered – this means that the results represent the impact on a system which has already been operated by the user for a while. The tests were repeated several times (with and without fingerprinting) in order to get mean values and filter out measurement errors. After each run, the workstation was defragmented and rebooted six times. We simulated various file operations that a computer user would execute: copying² different types of clean files from one place to another, archiving and unarchiving files, downloading files from the Internet and launching applications (opening documents). For the subtests, we have this year replaced WinAutomation with an industry-recognized performance assessment tool, namely Windows Assessment and Deployment Toolkit (Windows ADK) 6.3.9600.17029 with the Windows Performance Toolkit (WPT). This toolkit is widely used in the industry to measure the performance of computer systems. By using this tool, we enable vendors to more easily replicate the results and find out what in the product causes the impact on performance. In order to prevent vendors optimising their products for our test, we have implemented our own test drivers for the ADK. These also enable us to measure the performance impact of individual sub-tests without these influencing each other.

We also used a third-party, industry-recognized performance testing suite (PC Mark 8 Professional) to measure the system impact during real-world product usage. Readers are invited to evaluate the various products themselves, to see what impact they have on their systems (due to e.g. software conflicts and/or user preferences, as well as different system configurations that may lead to varying results).

Security products need to load on systems at an early stage to provide security from the very beginning – this load has some impact on the time needed for a system to start up. Measuring boot times accurately is challenging. The most significant issue is to define exactly when the system is fully started, as many operating environments may continue to perform start-up activities for some time after the system appears responsive to the user. It is also important to consider when the protection provided by the security solution being tested is fully active, as this could be a useful measure of boot completion as far as the security solution is concerned. Some security products load their services very late at boot (or even minutes later). Users may notice that some time after the system has loaded, it will become very slow for a little while; thus, it initially looks as though the system has loaded very quickly, but in fact the security product just loads its services belatedly, leaving the system more vulnerable. As we find this misleading, we still do not publish boot times in our reports.

² We use around 3GB of data consisting of various file types and sizes (pictures, movies, audio files, MS Office documents, PDF documents, applications/executables, Windows operating system files, archives, etc.).

Notes and comments

The on-access/real-time scanner component of anti-virus software runs as a background process to check all files that are accessed, in order to protect the system continuously against malware threats. For example, on-access scanners scan files as soon as they are accessed, while (e.g.) behaviour-blockers add a different layer of protection and monitor what the file does when it is already executed/running. The services and processes that run in the background to do these tasks also require and use system resources. Suite products usually have a higher impact on system performance than anti-virus-only products, as more services/features are included and running in the background.

Security products need to be active deep in the system in order to protect it, e.g. to scan processes and so on that are already active during the system start-up, to identify rootkits and other malware. Those procedures add some extra time and thus a delay in system boot/start up.

If a product takes up too many system resources, users get annoyed and may either disable or uninstall some essential protective features (and thus considerably compromise the security of their system) or may switch to security software that is less resource-hungry. Therefore, it is important not only that anti-virus software provide high detection rates and good protection against malware, but also that it does not degrade system performance or trouble users.

While this report looks at how much impact various Internet security products have on system performance, it is not always the security software that is principally responsible for a slow system. Other factors also play a role, and if users follow some simple rules, system performance can be improved noticeably. The next sections address some of the other factors that may play a part.

A few common problems observed on some user PCs:

- **Old hardware:** If a PC already runs at a snail's pace because it has ten-year-old hardware, using modern (security) software may make it unusable.
 - If possible, buy a new PC that at least meets the minimum recommended requirements of the software you want to use. Multi-Core processors are preferable.
 - Adding more RAM does not hurt. If you use Windows 7 or Windows 8, you should use a minimum of 4GB of RAM. If you use Windows XP or Vista, switch to Windows 8.1 64-Bit.
 - Make sure you have only ONE security program with real-time protection. If your new PC came with a trial security suite, remove this before installing a different protection program.
- **Keep all your software up-to-date:** Using an anti-virus version from e.g. 2013 may not protect you as well as the newer version would, even though you may still be able to update the signatures. Please visit <http://update.microsoft.com> regularly and keep your operating system up-to-date by installing the recommended patches. Any software can have vulnerabilities and bugs, so keep all the software installed on your PC up-to-date: this will not only protect you against many exploits and vulnerabilities, but also give you any other application improvements that have been introduced.

- **Clean up the content of your hard disk:**
 - o If your hard disk is almost full, your system performance will suffer accordingly. Leave at least 20% of your disk space free and transfer your movies and other infrequently accessed files to another (external) disk. If money is not an issue, consider buying solid-state drives (SSDs).
 - o Uninstall unneeded software. Often, the slowdown that users notice after installing an anti-virus product is due to other software on the PC running in the background (that is, due to software conflicts or heavy file access by other programs, each access requiring anti-virus scanning).
 - o Remove unneeded entries/shortcuts from the Start-Up folder in the All Programs menu.
 - o If your PC is already cluttered with residual files and registry entries left over by hundreds of applications you installed and uninstalled after trying them out, reinstall a clean operating system and install only software you really need (fewer software installations means fewer potential vulnerabilities and conflicts, and so on) and use e.g. an image/backup tool in order to return to a clean system without reinstalling everything.
- **Defragment your hard disks regularly:** A fragmented hard disk can have a very big impact on system performance as well as considerably increasing the time needed to boot up the system. A minimum of 15% free space on a hard disk is necessary for effective defragmentation. Please note that defragmentation is not necessary with a solid-state drive (SSD) and can reduce its lifetime.
- **Fingerprinting/Optimization:** most anti-virus products use various technologies to decrease their impact on system performance. Fingerprinting is such a technology, where already scanned files do not get rescanned for some time or (more rarely) or are whitelisted. This increases the speed considerably (especially after a longer period of PC usage), but also adds some potential risk, as not all files are scanned anymore. It is up to the user to decide what to do. We suggest regularly performing a full-system scan (to be sure that all files are at least currently found to be clean, and to further optimize the fingerprinting).
- **Be patient:** a delay of a few additional seconds due to security software is not necessarily a big deal. However, if even with the suggestions above the performance of your PC still annoys you, you should consider trying out another anti-virus product. If you only notice a slow-down after using the anti-virus for a long time, there are probably other factors behind the slowdown. Never reduce your security by disabling essential protection features, just in the hope of gaining a slightly faster PC!

Test cases

File copying: Some anti-virus products ignore some types of files by design/default (e.g. based on their file extensions), or use fingerprinting technologies, which may skip already scanned files in order to increase the speed (see comments on page 6). We copied a set of various common file types from one physical hard disk to another physical hard disk.

Archiving and unarchiving: Archives are commonly used for file storage, and the impact of anti-virus software on the time taken to create new archives or to unarchive files from existing archives may be of interest for most users. We archived a set of different file types that are commonly found on home and office workstations. The results already consider the fingerprinting/optimization technologies of the anti-virus products, as most users usually make archives of files they have on their disk.

Installing/uninstalling applications: We installed several popular applications with the silent install mode, then uninstalled them and measured how long it took. We did not consider fingerprinting, because usually an application is installed only once.

Launching applications: Microsoft Office (Word, Excel, PowerPoint) and PDF documents are very common. We opened and then later closed various documents in Microsoft Office and in Adobe Acrobat Reader. The time taken for the viewer or editor application to launch, and afterwards to close, was measured. Although we list the results for the first opening and the subsequent openings, we consider the subsequent openings more important, as normally this operation is done several times by users, and optimization of the anti-virus products take place, minimizing their impact on the systems.

Downloading files: Large files are downloaded from a local server with a GUI-less browser that allows sending HTTP requests in the background. Additionally, the content of several popular websites are fetched via *wget*, also from a local server.

Test results

These specific test results show the impact on system performance that a security product has, compared to the other tested security products. The reported data just gives an indication and is not necessarily applicable in all circumstances, as too many factors can play an additional part. The testers defined the categories Mediocre, Fast and Very Fast by consulting statistical methods and taking into consideration what would be noticed from the user's perspective, or compared to the impact of the other security products. If some products are faster/slower than others in a single subtest, this is reflected in the results.

Mediocre	Fast	Very Fast
The mean value of the products in this cluster builds a third cluster in the given subcategory	The mean value of the products in this group is higher than the average of all scores in the given subcategory	The mean value of the products in this group is lower than the average of all scores in the given subcategory

Overview of single AV-C performance scores

Vendor	File copying		Archiving/ unarchiving	Installing/ uninstalling applications	Launching applications (opening documents and PDF files)		Downloading files
	On first run	On subsequent runs			On first run	On subsequent runs	
Avast							
AVG							
Avira							
Baidu							
Bitdefender							
BullGuard							
Emsisoft							
eScan							
ESET							
Fortinet							
F-Secure							
Kaspersky Lab							
Lavasoft							
McAfee							
Microsoft							
Panda							
Quick Heal							
Sophos							
Tencent							
Trend Micro							
ThreatTrack							

Key:

mediocre

fast

very fast

PC Mark Tests

In order to provide an industry-recognized performance test, we used the PC Mark 8 Professional Edition³ testing suite. Users using PC Mark 8 benchmark⁴ should take care to minimize all external factors that could affect the testing suite, and strictly follow at least the suggestions documented inside the PC Mark manual, in order to get consistent and valid/useful results. Furthermore, the tests should be repeated several times to verify them. For more information about the various consumer scenarios tests included in PC Mark, please read the whitepaper on their website⁵.

“No security software” is tested on a baseline⁶ system with Windows Defender disabled⁷, which scores 100 points in the PC Mark 8 Work benchmark.

	PC Mark 8 Points
<i>No security software</i>	100
Avast	97.9
Emsisoft	97.8
Kaspersky Lab	97.7
Bitdefender	97.6
ESET	
McAfee	
AVG	97.5
F-Secure	
Avira	97.4
Sophos	
Tencent	
BullGuard	97.2
Baidu	97.1
eScan	
Panda	97.0
Fortinet	96.7
Trend Micro	
Lavasoft	96.3
Quick Heal	
ThreatTrack	

³ For more information, see <http://www.futuremark.com/benchmarks/pcmark8>

⁴ PCMark® is a registered trademark of Futuremark Corporation.

⁵ <http://www.futuremark.com/downloads/pcmark8-technical-guide.pdf> (PDF)

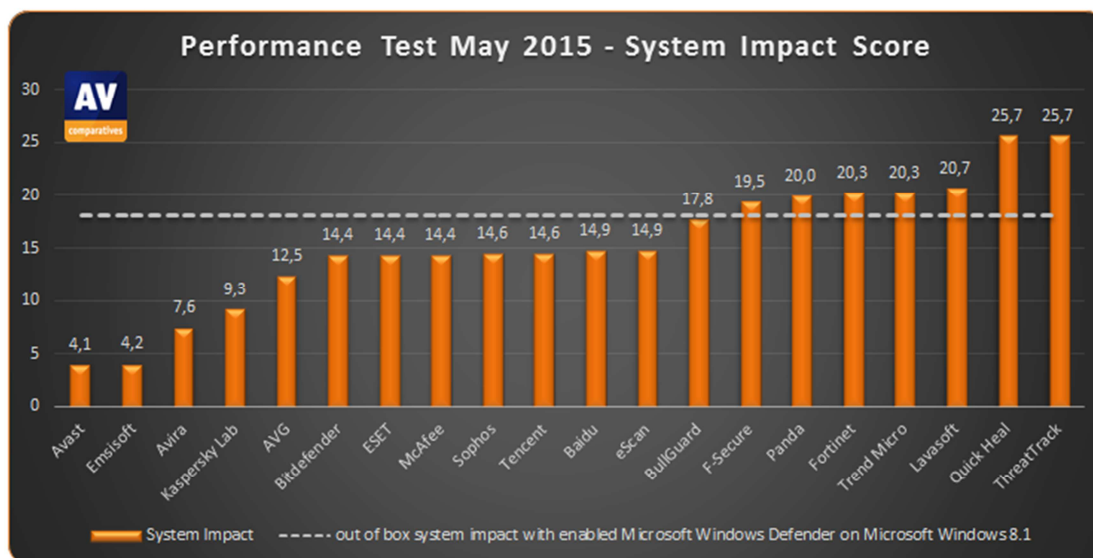
⁶ Baseline system: Intel Core i5-4210U machine with 4GB RAM

⁷ The PC Mark score with active Windows Defender would be 96,9.

Summarized results

Users should weight the various subtests according to their needs. We applied a scoring system in order to sum up the various results. Please note that for the File Copying and Launching Applications subtests, we noted separately the results for the first run and for subsequent runs. For the AV-C score, we took the rounded mean values of first and subsequent runs for File Copying, whilst for Launching Applications we considered only the subsequent runs. “Very fast” gets 15 points, “fast” gets 10 points and “mediocre” gets 5 points. This leads to the following results:

	AV-C Score	PC Mark Score	TOTAL	Impact Score
Avast	73	97.9	170.9	4.1
Emsisoft	73	97.8	170.8	4.2
Avira	70	97.4	167.4	7.6
Kaspersky Lab	68	97.7	165.7	9.3
AVG	65	97.5	162.5	12.5
Bitdefender	63	97.6	160.6	14.4
ESET	63	97.6	160.6	14.4
McAfee	63	97.6	160.6	14.4
Sophos	63	97.4	160.4	14.6
Tencent	63	97.4	160.4	14.6
Baidu	63	97.1	160.1	14.9
eScan	63	97.1	160.1	14.9
BullGuard	60	97.2	157.2	17.8
F-Secure	58	97.5	155.5	19.5
Panda	58	97.0	155.0	20.0
Fortinet	58	96.7	154.7	20.3
Trend Micro	58	96.7	154.7	20.3
Lavasoftware	58	96.3	154.3	20.7
Quick Heal	53	96.3	149.3	25.7
ThreatTrack	53	96.3	149.3	25.7



The out-of-box system impact score with enabled Windows Defender on Microsoft Windows 8.1 is 18.1.

Award levels reached in this test

The following award levels are for the results reached in this performance test report⁸. Please note that the performance test only tells you how much impact a security product may have on a system compared to other security products (please read the note on page 8); it does not say anything about the effectiveness of the protection a product provides, so please have also a look at the results of recent [Real-World Protection](#) and [File Detection](#) tests on our website.

AWARDS	PRODUCTS ⁹
	<ul style="list-style-type: none"> ✓ Avast ✓ Emsisoft ✓ Avira ✓ Kaspersky Lab ✓ AVG ✓ Bitdefender ✓ ESET ✓ McAfee ✓ Sophos ✓ Tencent ✓ Baidu ✓ eScan
	<ul style="list-style-type: none"> ✓ BullGuard ✓ F-Secure ✓ Panda ✓ Fortinet ✓ Trend Micro ✓ Lavasoft
	<ul style="list-style-type: none"> ✓ Quick Heal ✓ ThreatTrack
	-

The above awards have been given based on our assessment of the overall impact results with default settings under Windows 8.1 64-Bit.

⁸ Microsoft Windows Defender was tested out-of-competition and is therefore not included in the awards page.

⁹ We suggest considering products with the same award to be as light as the other products with same award.

Copyright and Disclaimer

This publication is Copyright © 2015 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted if the explicit written agreement of the management board of AV-Comparatives is given prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as a result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but no representative of AV-Comparatives can be held liable for the accuracy of the test results. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

AV-Comparatives (June 2015)