

Anti-Virus Comparative



Performance Test

Impact of Security Software on System Performance

Language: English

September 2017

Last Revision: 17th October 2017

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 in this test:

Adaware Antivirus Pro 12.2	F-Secure SAFE 17.0
Avast Free Antivirus 17.7	Kaspersky Internet Security 18.0
AVG Free Antivirus 17.7	McAfee Internet Security 20.2
AVIRA Antivirus Pro 15.0	Microsoft Windows Defender 4.11
Bitdefender Internet Security 22.0	Panda Free Antivirus 18.3
BullGuard Internet Security 18.0	Seqrite Endpoint Security 17.0
CrowdStrike Falcon Prevent 3.4	Symantec Norton Security 22.11
Emsisoft Anti-Malware 2017.8	Tencent PC Manager 12.3 (English)
eScan Corporate 360 14.0	Trend Micro Internet Security 12.0
ESET Internet Security 11.0	VIPRE Advanced Security 10.1
Fortinet FortiClient 5.6 (with FortiGate)	

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 10 64-Bit system**:

- File copying
- Archiving / unarchiving
- Installing / uninstalling applications
- Launching applications
- Downloading files
- Browsing Websites
- PC Mark 10 Professional Testing Suite

Test methods

The tests were performed on a Lenovo E560 machine with an Intel Core i5-6200U CPU, 8GB of RAM and SSD hard disks. The performance tests were done on a clean Windows 10 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.

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 reverted to the previously created system image and rebooted six times. We simulated various file operations that a computer user would execute: copying¹ 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 this year's performance test, we implemented a new, more automated testing framework. This allows us to increase the number of test iterations, from which we compute aggregated values. We believe that increasing the number of iterations increases our statistical precision. This is especially true for performance testing, as some noise is always present on real machines.

We also used a third-party, industry-recognized performance testing suite (PC Mark 10 Professional) to measure the system impact during real-world product usage. We used the predefined *PCMark 10 Extended* test. 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.

¹ We use around 4GB 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, you should use a minimum of 4GB of RAM. If you use Windows XP, Vista, 8 or 8.1, switch to Windows 10 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. 2015 may not protect you as well as the newer version would, even though you may still be able to update the signatures. Please 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:**
 - 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. Consider buying solid-state drives (SSDs).
 - 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).
 - Remove unneeded entries/shortcuts from the Start-Up folder in the All Programs menu.
 - 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: The content of several popular websites is fetched via *wget* from a local server.

Browsing Websites: popular websites are opened with Google Chrome. The time to completely load and display the website was measured. We only measure the time to navigate to the website when an instance of the browser is already started.

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 Slow, 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.

Slow	Mediocre	Fast	Very Fast
The mean value of the products in this cluster builds a clearly slower fourth cluster in the given subcategory	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		Downloading files	Browsing Websites
	On first run	On subse- quent runs			On first run	On subse- quent runs		
Adaware								
Avast								
AVG								
Avira								
Bitdefender								
BullGuard								
CrowdStrike								
Emsisoft								
eScan								
ESET								
Fortinet								
F-Secure								
Kaspersky Lab								
McAfee								
Microsoft								
Panda								
Seqrite								
Symantec								
Tencent								
Trend Micro								
VIPRE								

Key: Slow mediocre fast very fast

PC Mark Tests

In order to provide an industry-recognized performance test, we used the PC Mark 10 Professional Edition² testing suite. Users using PC Mark 10 benchmark³ 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, 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 website⁴.

“No security software” is tested on a baseline⁵ system without any security software installed, which scores 100 points in the PC Mark 10 Home benchmark.

	PC Mark Score
<i>Baseline</i>	<i>100.0</i>
Seqrite	99.5
ESET	99.2
F-Secure	99.0
AVIRA	98.5
CrowdStrike	
VIPRE	98.4
Fortinet	98.3
Bitdefender	97.8
McAfee	97.7
Panda	
BullGuard	97.1
Emsisoft	97.0
Kaspersky Lab	96.9
Symantec	96.3
Avast	96.1
AVG	
eScan	
Trend Micro	95.4
Microsoft	94.6
Tencent	93.0
Adaware	92.8

² For more information, see <https://www.futuremark.com/benchmarks/pcmark>

³ PCMark® is a registered trademark of Futuremark Corporation.

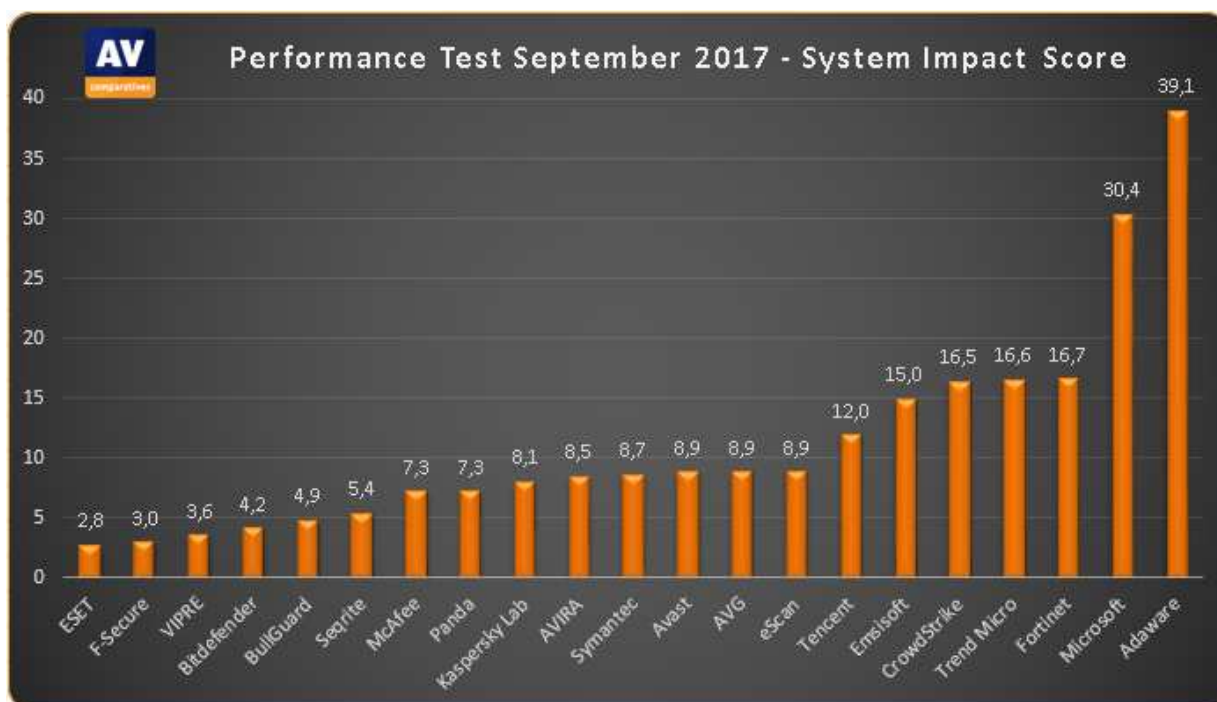
⁴ http://s3.amazonaws.com/download-aws.futuremark.com/PCMark_10_Technical_Guide.pdf (PDF)

⁵ Baseline system: Intel Core i5-6200U machine with 8GB RAM and SSD drive

Summarized results



Users should weight the various subtests according to their needs. We applied a scoring system 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, “mediocre” gets 5 points and “slow” gets 0 points. This leads to the following results:

	AV-C Score	PC Mark Score	TOTAL	Impact Score
ESET	88	99.2	187.2	2.8
F-Secure	88	99.0	187.0	3.0
VIPRE	88	98.4	186.4	3.6
Bitdefender	88	97.8	185.8	4.2
BullGuard	88	97.1	185.1	4.9
Seqrite	85	99.5	184.5	5.4
McAfee, Panda	85	97.7	182.7	7.3
Kaspersky Lab	85	96.9	181.9	8.1
AVIRA	83	98.5	181.5	8.5
Symantec	85	96.3	181.3	8.7
Avast, AVG, eScan	85	96.1	181.1	8.9
Tencent	85	93.0	178.0	12.0
Emsisoft	78	97.0	175.0	15.0
CrowdStrike	75	98.5	173.5	16.5
Trend Micro	78	95.4	173.4	16.6
Fortinet	75	98.3	173.3	16.7
Microsoft	63	96.6	159.6	30.4
Adaware	55	95.9	150.9	39.1



Award levels reached in this test

The following award levels are for the results reached in this performance test report. 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 [Malware Protection](#) tests on our website.

AWARDS	PRODUCTS ⁶
	<ul style="list-style-type: none"> ✓ ESET ✓ F-Secure ✓ VIPRE ✓ Bitdefender ✓ BullGuard ✓ Seqrite ✓ McAfee ✓ Panda ✓ Kaspersky Lab ✓ AVIRA ✓ Symantec ✓ Avast ✓ AVG ✓ eScan
	<ul style="list-style-type: none"> ✓ Tencent ✓ Emsisoft ✓ CrowdStrike ✓ Trend Micro ✓ Fortinet
	<ul style="list-style-type: none"> ✓ Microsoft ✓ Adaware

⁶ 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 © 2017 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 (October 2017)