Anti-Virus Comparative

Performance test (AV Products)

Impact of Anti-Virus Software on System Performance

Language: English
April 2013
Last Revision: 6th May 2013

www.av-comparatives.org

Table of Contents

Introduction

We want to make clear that the results in this report are intended to give only an indication of the impact on system performance (mainly by the real-time/on-access components) of the various Anti-Virus products in these specific tests. Users are encouraged to try out the software on their own PC's and form an opinion based on their own observations.

Tested products

The following products were evaluated (with default settings) in this test[1]:

- avast! Free Antivirus 8.0
- AVG Anti-Virus 2013
- AVIRA Antivirus Premium 2013
- Bitdefender Antivirus Plus 2013
- BullGuard Antivirus 2013
- Emsisoft Anti-Malware 7.0
- eScan Anti-Virus 14.0
- ESET NOD32 Antivirus 6.0
- Fortinet FortiClient Lite 4.3.5
- F-Secure Anti-Virus 2013
- G DATA AntiVirus 2014
- Kaspersky Anti-Virus 2013
- Kingsoft Anti-Virus 2013.SP2.5
- McAfee AntiVirus Plus 2013
- Microsoft Security Essentials 4.2
- Panda Cloud Antivirus Free 2.1.1
- Qihoo 360 Antivirus 4.0
- Sophos Anti-Virus 10.2
- Symantec Norton Anti-Virus 2013[2]
- ThreatTrack Vipre Antivirus 2013
- Trend Micro Titanium Antivirus Plus 2013

Please note that the results in this report apply only to the products/versions listed above (e.g. 64-Bit versions, product version, etc.). Also, keep in mind that different vendors offer different (and differing quantities of) features in their products.

The following activities/tests were performed under an up-to-date Windows 7 Professional SP1 64-Bit:

- File copying
- Archiving / Unarchiving
- Encoding / Transcoding
- Installing / Uninstalling applications
- Launching applications
- Downloading files
- PC Mark 7 Professional Testing Suite

We updated the test-sets and procedures for performance testing (e.g. by updating the test files, testing times/cycles and automation scripts), as well as the used hardware.

[1] We used the latest available product versions available at time of testing (end of April 2013).
[2] We added Symantec Norton in this test, even if they did not apply for being included into our test-series. A magazine has covered the expenses for testing additionally Symantec.

Test methods

The tests were performed on a machine with Intel Core i5-3330 CPU and 4GB of RAM. The performance tests were done on a clean and fully updated Microsoft Windows 7 Professional SP1 64-Bit system (English) and then with the installed Anti-Virus software (with default settings). The tests have been done with an active internet connection to simulate 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 used 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. We simulated various file operations that a computer user would execute: copying[3] different types of clean files from one place to another, archiving and unarchiving files, installing and uninstalling applications, encoding and transcoding[4] audio and video files, downloading files, launching applications, etc. We also used a third-party industry recognized performance testing suite (PC Mark 7 Professional) to measure the system impact during real-world product usage. Readers are invited to evaluate the various products themselves, to see how they impact on their systems (such as 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 Anti-Virus products are loading their services very late (even minutes later) at boot (users may notice that after some time that the system loaded, the system gets very slow for some moments), so the system looks like loading very fast, but it just loads its services later and makes the system also insecure/vulnerable. As we do not want to support such activities, we still do not measure boot times.

To support our concerns, we sporadically check in performance tests if the products are loading all their protection modules before e.g. malware in the start-up folder is executed. Several products failed this test, except AVG, Bitdefender, eScan, Kingsoft, Microsoft and Sophos. Those were the only products that detected and blocked the malware before its execution after system start-up (by loading itself at an early stage); in all other cases, first the malware was successfully executed and only later detected by the AV products, when it was already too late.

---

[3] We used around 3GB of data consisting of various file types and sizes (pictures, movies, audio files, various MS Office documents, PDF files, applications/executables, Microsoft Windows 7 system files, archives, etc.).

[4] Converting MP3 files to WAV, MP3 to WMA and AVI to MP4

Side 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 have usually 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 and 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 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 provides 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 the main factor 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 XP, Windows 7 or Windows 8, you should use a minimum of 2GB of RAM. If you use Vista, switch to Windows 7 or Windows 8. 64-Bit systems are preferable, as especially software that is optimized for such systems will run faster.
  - Make sure you have only ONE Anti-Virus program with real-time protection. If your new PC came with a trial Anti-Virus program, remove this before installing a different AV program.

- **Keep all your software up-to-date**: Using an Anti-Virus version from e.g. 2010 does 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**:
  - If your hard disk is almost full, your system performance will suffer accordingly. Leave at least 20% of your disk space free and move your movies and other infrequently accessed files to another (external) disk. If money is not an issue, 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 Autostart/start-up folder in the program menu
  - if your PC is already messed up by residual files and registry entries left over by hundreds of applications you installed and uninstalled after trying them out over the past years, reinstall a clean operating system and install only software you really need (fewer software installations, fewer potential vulnerabilities and conflicts, and so on) and use e.g. an image/backup tool in order to ensure that you do not have to reinstall everything manually in future.

- **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.

- **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 are not rescanned again for a while (or more) or are whitelisted. This increases the speed considerably (esp. after some time the PC was used), but also adds some little potential risk, as not all files are scanned anymore. It is up to the user to decide what to prefer. We suggest performing regularly a full-system scan (to be sure that all files are at least currently found as clean and to further optimize the fingerprinting).

- **Be patient:** a delay of a few additional seconds due to Anti-Virus is not necessarily a big deal. However, if even with the suggestions above the performance of your PC still annoys you, for instance, after you have installed the Anti-Virus 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 do not scan all kind 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 widespread at 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.

Encoding/transcoding

Music files are often stored and converted on home systems, and converting such files takes system resources. Due that, many home users may be interested to know if their Anti-Virus product imposes a slowdown while converting multimedia files from one format to another. We encoded and transcoded some multimedia files with FFmpeg and HandBrakeCLI.

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

Office document files (Word, Excel, PowerPoint) and PDF files are very common. We opened some large document files in Microsoft Office (and closed it) and some large PDF files in Adobe Acrobat Reader (and closed it). The time taken for the viewer or editor application to launch and afterwards 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 features 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 Anti-Virus products have, compared to the other tested Anti-Virus products. The reported data just give an indication and are not necessarily applicable in all circumstances, as too many factors can play an additional part.

As we noticed that delivering percentages get easily misinterpreted by users (as well as misused by marketing departments or the press) and percentages would need adjustments when other hardware specifications are being used, we grouped the percentage results by clustering them. The impact within those categories does not statistically differ, also considering error measurements. The testers defined the categories by consulting statistical methods like hierarchical clustering and taking into consideration what would be noticed from user's perspective or compared to the impact of the other security products. As the single performance results (page 9) are built using clusters, if some products are faster/slower than others this reflects in the results. Due to that, the results cannot be directly compared with results from previous tests, as they can only be compared within the test. This means that it would be wrong to state that a product got slower (in some areas) compared to last year, while it would be correct to state that a product was (within the test) slower than those in the higher category. We give this time the mean values (the percentages refer to a system without AV) of the clusters as an indication only:

	slow	mediocre	fast	very fast
File copying (first run)	-	The mean value of this cluster is over +100%	The mean value of this cluster is under +100%	The mean value of this cluster is under +50%
File copying (subsequent runs)	-	-	The mean value of this cluster is over +35%	The mean value of this cluster is under +35%
Archiving/unarchiving	-	-	The mean value of this cluster is over +10%	The mean value of this cluster is under +10%
Installing/uninstalling	-	The mean value of this cluster is over +80%	The mean value of this cluster is under +80%	The mean value of this cluster is under +40%
Encoding/transcoding	-	-	-	The mean value of this cluster is under 2%
Open Office documents (on first run)	-	The mean value of this cluster is over +120%	The mean value of this cluster is under +120%	The mean value of this cluster is under +60%
Open Office documents (on subsequent runs)	-	-	The mean value of this cluster is over +35%	The mean value of this cluster is under +35%
Open PDF (on first run)	-	The mean value of this cluster is over +60%	The mean value of this cluster is under +60%	The mean value of this cluster is under +20%
Open PDF (on subsequent runs)	-	-	The mean value of this cluster is over +10%	The mean value of this cluster is under +10%
Downloading files	-	The mean value of this cluster is over +120%	The mean value of this cluster is under +120%	The mean value of this cluster is under +60%

Overview of single AV-C performance scores

Vendor	File copying		Archiving/ unarchiving	Installing/ uninstalling applications	Encoding/ transcoding	Launching applications				Downloading files
						Open Office documents		Open PDF		
	On first run	On subsequent runs				On first run	On subsequent runs	On first run	On subsequent runs	
Avast										
AVG										
AVIRA										
Bitdefender										
BullGuard										
Emsisoft										
eScan										
ESET										
Fortinet										
F-Secure										
G DATA										
Kaspersky										
Kingsoft										
McAfee										
Microsoft										
Panda										
Qihoo										
Sophos										
Symantec										
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 7 Professional Edition[5] testing suite. Users using PC Mark 7 should take care to minimize all external factors which could affect the testing suite and follow strictly at least the considerations/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 website[6].

"Without AV" is tested on a baseline[7] system without AV, which scores 100 points in the PC Mark test.

	PC Mark points
without AV	100
F-Secure	99,6
Kaspersky	
Sophos	
ESET	99,4
Microsoft	
Avira	98,9
Avast	98,7
Panda	
Symantec	
AVG	97,9
Bitdefender	97,6
Emsisoft	
Fortinet	
McAfee	
Qihoo	
Vipre	97,3
G DATA	96,8
Trend Micro	
BullGuard	96,3
eScan	92,5
Kingsoft	91,4

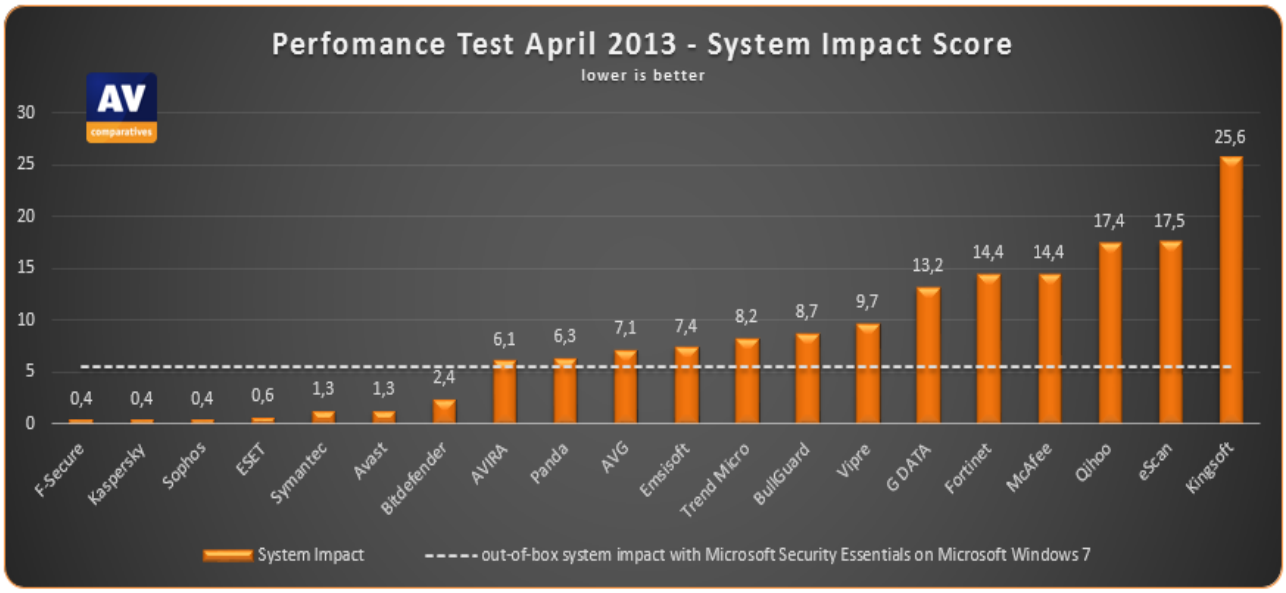
[5] For more information, see http://www.pcmark.com/benchmarks/pcmark7/
[6] http://www.pcmark.com/benchmarks/pcmark7/whitepaper/whitepaper.pdf (PDF)
[7] Baseline system: Intel Core i5-3330 machine with 4GB RAM

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.

For "file copying", we took the mean values, as well as for "launching applications" (on subsequent runs). Like in previous performance reports, "very fast" gets 15 points, "fast" gets 10 points, "mediocre" gets 5 points and "slow" gets zero points. This leads to the following results:

	AV-C Score	PC Mark Score	TOTAL	Impact Score
F-Secure, Kaspersky, Sophos	90	99,6	**189,6**	0,4
ESET	90	99,4	**189,4**	0,6
Avast, Symantec	90	98,7	**188,7**	1,3
Bitdefender	90	97,6	**187,6**	2,4
Microsoft	85	99,4	**184,4**	5,6
AVIRA	85	98,9	**183,9**	6,1
Panda	85	98,7	**183,7**	6,3
AVG	85	97,9	**182,9**	7,1
Emsisoft	85	97,6	**182,6**	7,4
Trend Micro	85	96,8	**181,8**	8,2
BullGuard	85	96,3	**181,3**	8,7
Vipre	83	97,3	**180,3**	9,7
G DATA	80	96,8	**176,8**	13,2
Fortinet, McAfee	78	97,6	**175,6**	14,4
Qihoo	75	97,6	**172,6**	17,4
eScan	80	92,5	**172,5**	17,5
Kingsoft	73	91,4	**164,4**	25,6



Award levels reached in this test

The following award levels are for the results reached in this performance test report[8]. Please note that the performance test only tells you how much impact an Anti-Virus product may have on a system compared to other Anti-Virus products (please read the note on page 8); it does not tell anything about the effectiveness of the protection a product provides.

AWARDS	PRODUCTS[9]
	✓ F-Secure ✓ Kaspersky ✓ Sophos ✓ ESET ✓ Avast ✓ Symantec ✓ Bitdefender
	✓ AVIRA ✓ Panda ✓ AVG ✓ Emsisoft ✓ Trend Micro ✓ BullGuard ✓ Vipre
	✓ G DATA ✓ Fortinet ✓ McAfee ✓ Qihoo ✓ eScan
	✓ Kingsoft

The above awards have been given based on our assessment of the overall impact results with default settings under Microsoft Windows 7 Professional SP1 64 Bit.

[8] Microsoft security products are no longer included in the awards page as they are tested out-of-competition.
[9] We suggest considering products with the same award to be as light as the other products with same award.

Copyright and Disclaimer

AV-Comparatives e.V. (May 2013)