Anti-Virus Comparative

Performance test

Impact of Anti-Virus Software on System Performance

Date: October 2008

Last revision: 18th November 2008

Website: http://www.av-comparatives.org

1. Introduction

Many readers have asked AV-Comparatives in the past to conduct a test which looks at the impact of Anti-Virus software on system performance. This request has been rejected by us up to now, as in our opinion there are too many circumstances which can influence system performance, and therefore an objective measurement which is applicable in general is impossible.
Nevertheless, AV-Comparatives thought about how such a test could be done and finally agreed to do one by creating, using, modifying and/or improving existing test methods/scripts. At the same time, however, we want to make clear that the results in this report are intended to give just an indication of the impact on system performance (mainly by the real-time/on-access components) of the various Anti-Virus products. Users are encouraged to try out the software on their own PC and build an opinion based on their own observations.
As with all new tests we introduce, it should be considered as a preliminary approach. We will further optimize the performance test methodologies in the next round.

2. Tested products

This report builds on the test of August 2008 (http://www.av-comparatives.org/seiten/ergebnisse/report19.pdf) and therefore the same products/versions[1] were used:
avast! Professional Edition 4.8
AVG Anti-Virus 8.0
AVIRA AntiVir Premium 8.1
BitDefender Antivirus 2008
eScan Anti-Virus 9.0
ESET NOD32 Anti-Virus 3.0
F-Secure Anti-Virus 2009
G DATA AntiVirusKit (AVK) 2009
Kaspersky Anti-Virus 2009
McAfee VirusScan Plus 12.1
Microsoft OneCare 2.5
Norman Antivirus & Anti-Spyware 7.1
Sophos[2] Endpoint Protection 7.5.1
Symantec Norton Anti-Virus 2009
TrustPort[3] Antivirus Workstation 2.8
VBA32[4] Scanner for Windows 3.12.8.2

You can find the exact version numbers etc. in the afore-mentioned report. Newer/up-to-date products will be used in the next performance test report next year.
Please note that the results in this report apply only to the products/versions listed above and should not be assumed to be comparable to (for example) the versions provided by the above listed vendors as part of a product suite.
Also, keep in mind that different vendors offer different (and differing quantities of) features in their products.

[1] some products already improved their performance in the meantime – this will be seen in the next report
[2] Sophos is an enterprise product.
[3] TrustPort was tested with only two engines (AVG, Norman)
[4] excessive heuristic and thorough mode were not enabled in VBA32

3. Test methods

The tests have been performed on identical Intel Core 2 Duo 8400 machines with 2GB of RAM. The performance tests were first done on a clean Windows XP Professional SP3 system (English) and then with the installed Anti-Virus software (with default settings and also with most paranoid settings).
All hard disks were defragmented before starting the various tests, and care was taken to minimize any other factor which could influence the measurements and/or comparability of the systems (network, temperature, etc.).
All tests were repeated 20 times to get average values. Please do not take the percentages as absolutes, as in such tests fluctuations are to be expected (and will vary based on which files are used).
After introducing the sets and utilities needed for the performance tests, we run a full system scan so that optimizing processes included in the Anti-Virus packages could take place.

The tests were split into two parts:

a) We simulate various file operations that a computer user would execute: copying[5] different types of clean files from one place to another, archiving and unarchiving[6] Office 2003 files, encoding and transcoding[7] audio and video files, etc.
b) We analyze the system boot up and shutdown of the PCs, to see what impact the Anti-Virus software has on it (i.e. what delays are introduced). We defined different ways of measuring performance in order to achieve this goal:
   i. The first test method consists of rebooting the machine and measuring how much time is taken from the moment where you click on reboot, until the system has booted up and the system reaches idle status.
   ii. In the second test method, the PC is first shut-down. Then the PC is started and we measure the time from start loading the OS until the Anti-Virus has been loaded and the system reaches idle status.

   The boot time values are the mean values of the two mean values returned by the two boot time test methods above. A third approach will be probably added in the next round.

The overall impact value is taken as the average value of the summarized percentages of the different aspects measured. If you are not using some aspects we have tested (such as encoding), you can use the single results for comparison.
Readers are invited to evaluate the various products themselves so as to see how the various products impact on their systems (such as, for example software conflicts and/or user preferences and so on, as well as different system configurations that may lead to varying results).

---

[5] we split this process into 200-300MB data of various file categories (pictures, movies, music, various MS Office 2003 documents [mainly Word, Excel, Powerpoint and some Access files], various MS Office 2007 documents [mainly Word, Excel, Powerpoint and some Visio files], PDF files, applications/executables, Windows XP system files, archives, etc.), but on this occasion we list in this report only the total mean value of the subsets average percentages. Most of the nine categories constitute around 10% of the set; movies only 5%, while PDF files and archives around 15%, as they are in our opinion more often copied than e.g. movies. The set size was about 2,5GB data / ~7000 files. We will try to better weight the category sizes in the next round.
[6] with the open source program 7-Zip (http://www.7-zip.org)
[7] Converting many and various MP3 files to WAV, MP3 to WMA, AVI to MPG and MPG to AVI

4. Side notes and comments

The on-access/real-time scanner component of Anti-Virus software checks as a background process 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.

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

The boot time test is one of the most controversial tests in terms of measurement. It is very difficult to know exactly when the boot process has finished. When the Windows-Shell is loaded, this doesn't mean that the boot process is already finished. There are several programs, such as Anti-Virus software, which may start later in the process. So, to meet this case, we define the time the boot process is finished as being when all services have been started and the CPU is idle.

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

In our opinion, Anti-Virus vendors should deliver a fast product which uses by default high protection settings which does not slow down the system significantly. Some products gain better performance by using lower settings than other ones. Examples of products which run with most secure settings by default are products by McAfee, Microsoft, ESET, Norman. Also Avast, Symantec, Kaspersky, AVG and VBA32 run with a good balance of protection settings and performance, as it can be seen when comparing the results with default settings and highest settings.

As some products install themselves with less effective default settings on slow PCs, we display the results for both settings and remind you that settings may depend according to the hardware on which the software is used, also.

Anyway, while this report looks at how much impact various Anti-Virus products have on system performance, it is not always just the Anti-Virus software which is 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.

4.1 A few common problems we observed on some user PC's:

- **Old hardware**: If a PC already runs at snail's pace because it uses ten-year-old hardware, using modern (Anti-Virus) software may make it unusable.

  - If possible, buy a new PC which meets the minimum recommended requirements of the software you want to use.

  - Adding more RAM (RAM is very cheap nowadays) does not hurt. If you use Windows XP, you should use a minimum of 2GB of RAM. If you use Vista, use at least 3GB.

- **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.

  - 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

  - Use (e.g.) CCleaner[8] and ATFCleaner[9] to remove unneeded and temporary files from your disk on a regular basis.

  - 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
    - an image/backup[10] tool in order to ensure that you do not have to reinstall everything manually in future and
    - a sandbox[11] in which you can try out new software without installing it to your system.

- **Defragment your hard disks regularly!** A fragmented hard disk can have a very big impact on system performance as well as increasing considerably the time needed to boot/start up the system.

- **Slow down due to a malware infection**: Try out some online-scanners[12] supplied by other Anti-Virus vendors to cross-check whether your PC may be compromised.

[8] http://www.ccleaner.com
[9] http://www.atribune.org
[10] e.g. Acronis TrueImage Home (http://www.acronis.com)
[11] e.g. Sandboxie (http://www.sandboxie.com)

- **Keep all your software up-to-date**: Using an Anti-Virus version from 2003 does not really protect you as well as the newer version would, even though you may still be able to update the signatures. 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 other application improvements may also have been introduced.

- **Be patient:** a delay of a few additional seconds due an Anti-Virus is not necessarily a big deal. But if even with the suggestions above your PC still needs a considerably longer time to boot up, for instance, after you have installed the Anti-Virus you should consider trying out another Anti-Virus product. (If you notice a slow-down after having used the Anti-Virus for a long time already, there are probably other factors behind the slowdown.). Do not reduce your security by disabling essential protection features, just in the hope of gaining a slightly faster PC.

- Experienced users may also try the following:
  - Optimize the boot up settings in the BIOS configuration
  - Disable unneeded services, registry start-ups[13] and drivers with MSCONFIG

If you are not sure about how to use/apply the above suggestions, ask a knowledgeable friend or ask in a forum of your choice. AV-Comparatives is not in a position to provide support or take any responsibility for problems that may arise if you are unable to apply the above-mentioned tips correctly.

[12] various online scanners are listed on http://wiki.castlecops.com/Online_antivirus_scans for example
[13] a nice utility is Autoruns, available at http://live.sysinternals.com/autoruns.exe

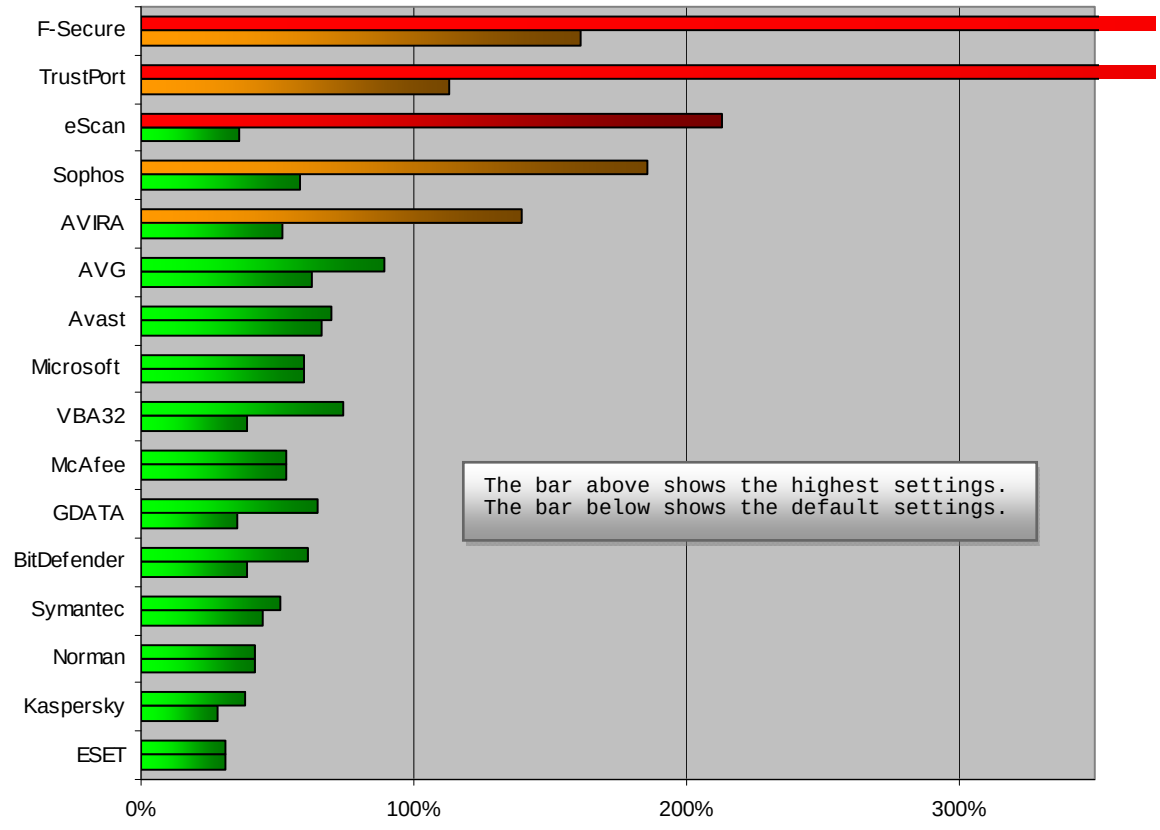
5. Test results

Those 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. Do not take any of these numbers as being universally applicable or absolute.
The ordering in the tables[14] and graphs[15] is sorted by the mean value of highest[16] and default settings. Lower is better.

5.1 File copying:

	Default settings	Highest settings
ESET	+31%	+31%
Kaspersky	+28%	+38%
Norman	+42%	+42%
Symantec	+45%	+51%
BitDefender	+39%	+61%
GDATA	+35%	+65%
McAfee	+53%	+53%
VBA32	+39%	+74%
Microsoft	+60%	+60%
Avast	+66%	+70%
AVG	+63%	+89%
AVIRA	+52%	+140%
Sophos	+58%	+186%
eScan	+36%	+213%
TrustPort	+113%	over +500%
F-Secure	+161%	over +500%

Note: F-Secure and TrustPort use several engines, which may be one reason why they are slower than the other (single-engine) products.



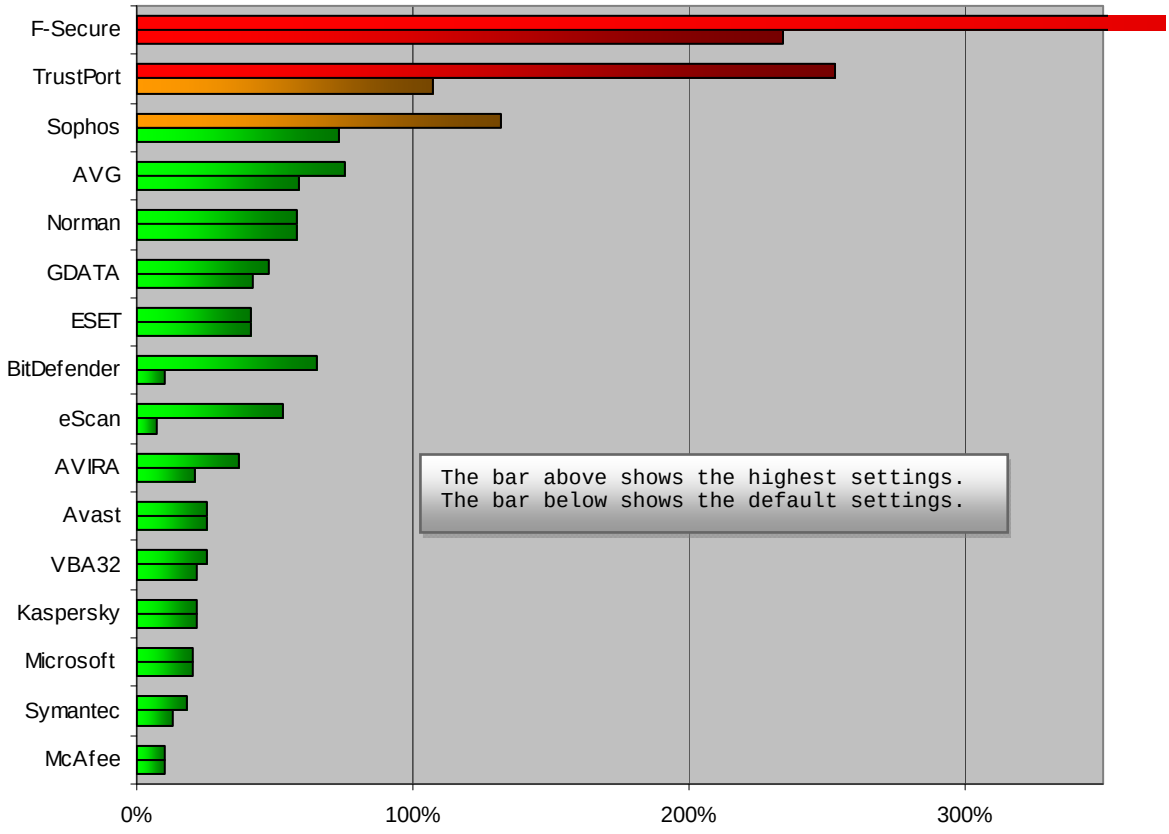
[14] the measurement is ranked by the additional delay to a system compared to the same system with installed Anti-Virus Software; the unprotected system has 0% delay. The graph shows how much delay is added. If copying some clean files takes e.g. 30 seconds, +100% delay means it would take 60 seconds.
[15] the bar colours just indicate what we consider acceptable values, and so on.
[16] because with default settings it could be that a scanner does not even scan the files used in the test

5.2 Archiving and unarchiving:

Several MS Office 2003 files were archived and unarchived by the open source software 7-Zip.

	Default settings	Highest settings
McAfee	+10%	+10%
Symantec	+13%	+18%
Microsoft	+20%	+20%
Kaspersky	+22%	+22%
VBA32	+22%	+25%
Avast	+25%	+25%
AVIRA	+21%	+37%
eScan	+7%	+53%
BitDefender	+10%	+65%
ESET	+41%	+41%
GDATA	+42%	+48%
Norman	+58%	+58%
AVG	+59%	+75%
Sophos	+73%	+132%
TrustPort	+107%	+253%
F-Secure	+234%	over +500%

Note: F-Secure and TrustPort use several engines, which may be one reason why they are slower than the other (single-engine) products.

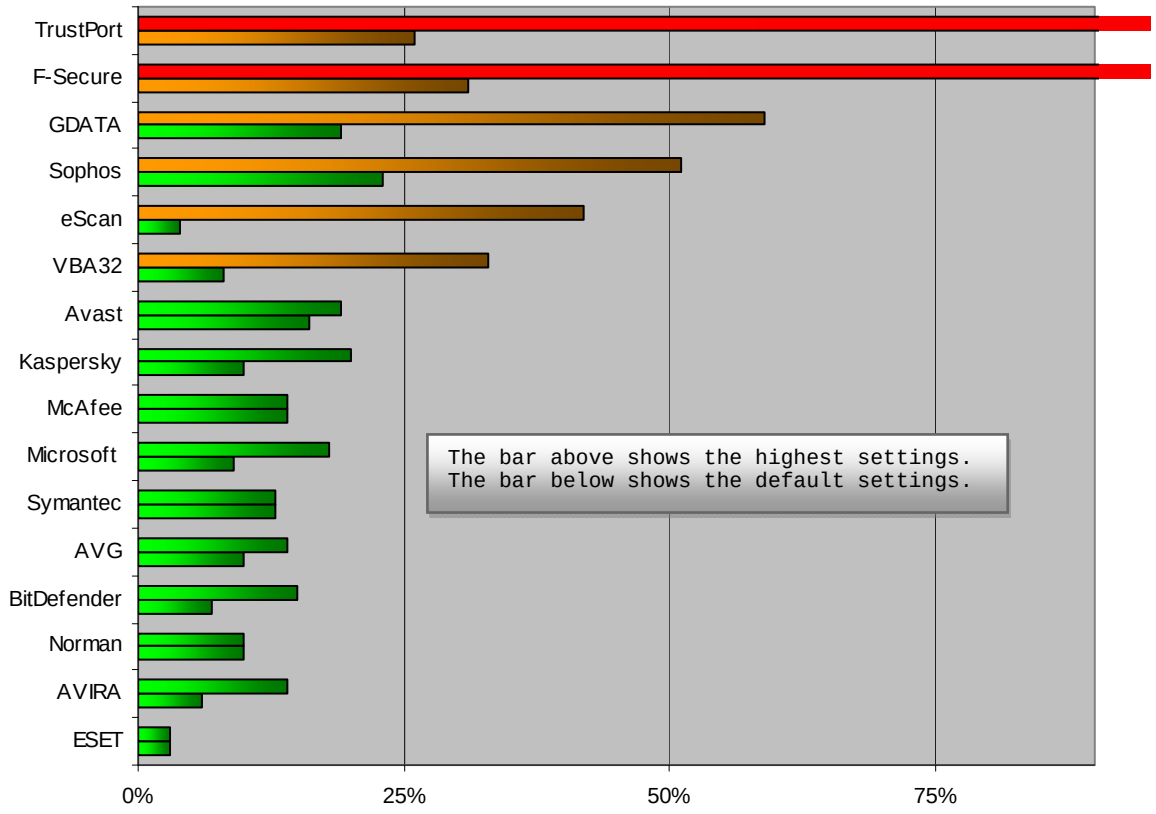


5.3 Encoding/transcoding:

Music and Video-Files were encoded and transcoded with FFmpeg.

	Default settings	Highest settings
ESET	+3%	+3%
AVIRA	+6%	+14%
Norman	+10%	+10%
BitDefender	+7%	+15%
AVG	+10%	+14%
Symantec	+13%	+13%
Microsoft	+9%	+18%
McAfee	+14%	+14%
Kaspersky	+10%	+20%
Avast	+16%	+19%
VBA32	+8%	+33%
eScan	+4%	+42%
Sophos	+23%	+51%
GDATA	+19%	+59%
TrustPort	+26%	over +200%
F-Secure	+31%	over +200%

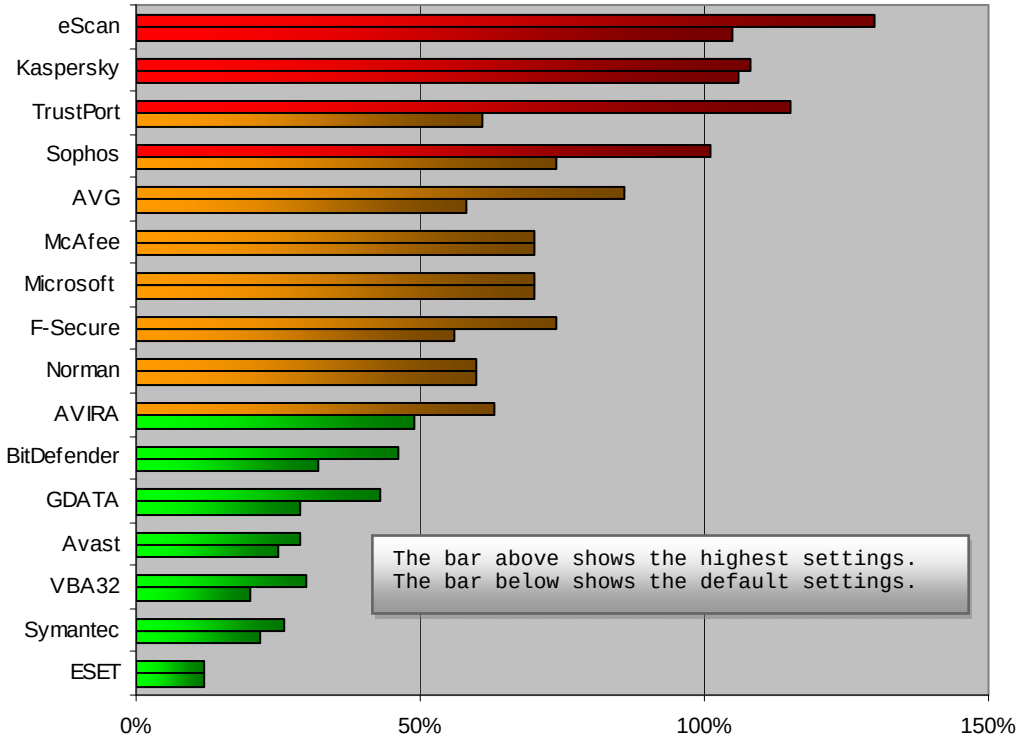
Note: F-Secure and TrustPort use several engines, which may be one reason why they are slower than the other (single-engine) products.



5.4 Boot Time test:

The boot-time test is highly controversial. While the other tests (like file copy/access - something users do while using the computer) are continuous tests, the boot test measures something (boot up / shutdown) which is done usually only once at day.

	Default settings	Highest settings
ESET	+12%	+12%
Symantec	+22%	+26%
VBA32	+20%	+30%
Avast	+25%	+29%
GDATA	+29%	+43%
BitDefender	+32%	+46%
AVIRA	+49%	+63%
Norman	+60%	+60%
F-Secure	+56%	+74%
Microsoft	+70%	+70%
McAfee	+70%	+70%
AVG	+58%	+86%
Sophos	+74%	+101%
TrustPort	+61%	+115%
Kaspersky	+106%	+108%
eScan	+105%	+130%



Kaspersky, AVG, Norman and Sophos will overall not reach the Advanced+ award mainly due the scores (compared to other products) in the boot test, as in this first report we do not weight the results. Those products earned anyway the Advanced award, as they are fast scanners according to the other subtests (but boot time could be improved further). Furthermore, some Anti-Virus products (like AVG, Kaspersky, etc.) use a maximum of the OS task scheduling capabilities, so they start their own processes when the CPU is idle - there might be a process with low priority that would immediately get into background and let other (anti-virus) processes run (which is measured in the boot time count, even if the PC could be considered as usable). Next time we will take care of this behaviour, to reflect even better real-world experience.

5.5 Overall impact:

In this first test we will not use different weights for the various subtests. The numbers below are just mean values over the four subtests. Users should weight the various subtests according to their needs. In our opinion the file copying test is much more important than the boot time test, the archiving/unarchiving test or the encoding/transcoding test (especially for users who do not encode/transcode audio/video files).

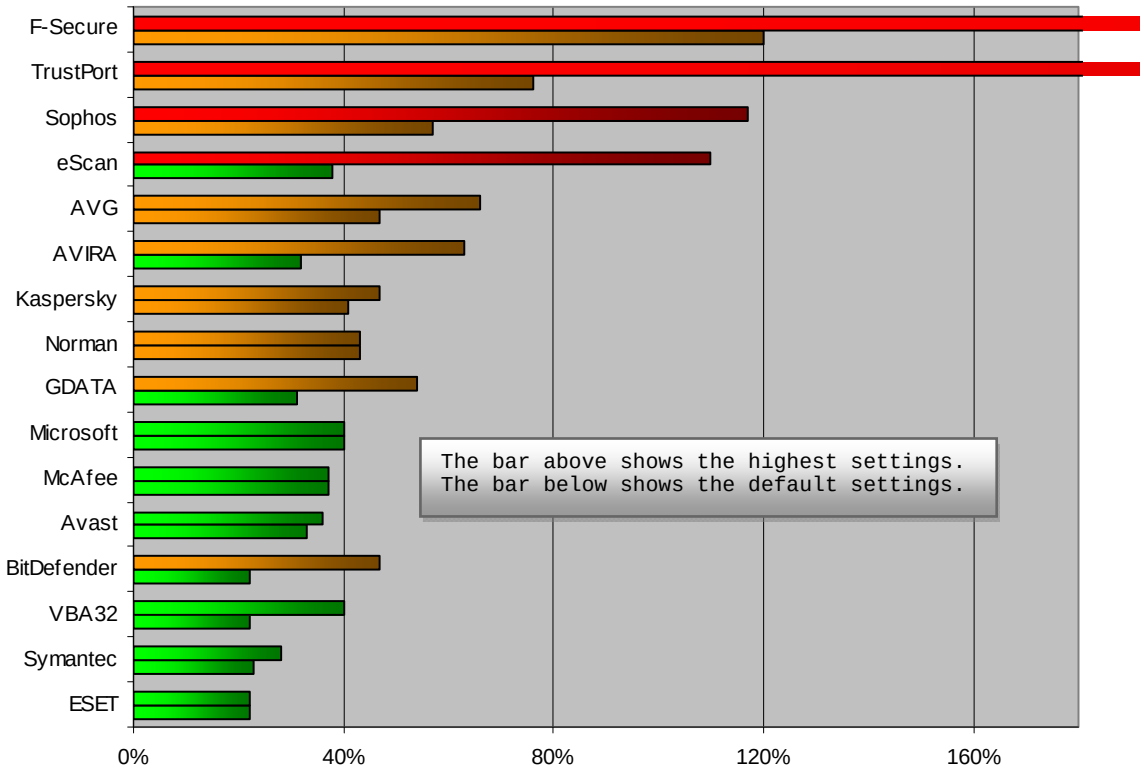
	Default settings	Highest settings
ESET	+22% (very fast)	+22% (very fast)
Symantec	+23% (very fast)	+28% (very fast)
VBA32	+22% (very fast)	+40% (very fast)
BitDefender	+22% (very fast)	+47% (fast)
Avast	+33% (very fast)	+36% (very fast)
McAfee	+37% (very fast)	+37% (very fast)
Microsoft	+40% (very fast)	+40% (very fast)
GDATA	+31% (very fast)	+54% (fast)
Norman	+43% (fast)	+43% (fast)
Kaspersky	+42% (fast)	+47% (fast)
AVIRA	+32% (very fast)	+63% (fast)
AVG	+47% (fast)	+66% (fast)
eScan	+38% (very fast)	+110% (mediocre)
Sophos	+57% (fast)	+117% (mediocre)
TrustPort	+76% (fast)	over +300% (very slow)
F-Secure	+120% (mediocre)	over +300% (very slow)

Note: F-Secure and TrustPort use several engines, which may be one reason why they are slower than the other (single-engine) products.

We applied the labels according to the structure below:

0-40% very fast
41-80% fast
81-120% mediocre
121-160% slow
over 160% very slow

Considering that some products used optimization processes, the given labels are in our opinion generous and were therefore applied strictly.



6. Certification levels reached in this test

We provide a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). The following certification levels are for the results reached in this performance test report. Please note that the performance test only tells you how much impact an Anti-Virus may have on a system compared to other Anti-Virus products: it does not tell you anything about the effectiveness of the protection a product provides. To determine, for example, how the detection rates of the various Anti-Virus products are, please refer to our other tests, available at www.av-comparatives.org

CERTIFICATION LEVELS	PRODUCTS
	**ESET** **Symantec** **VBA32** **Avast** **McAfee** **Microsoft** **BitDefender** **GDATA** **AVIRA**
	**Norman** **Kaspersky** **AVG** **eScan** **Sophos**
	**TrustPort** **F-Secure**[17]

The above awards have been given based on the labels (*very fast*, *fast*, *mediocre*, *slow and very slow*) of the overall impact assessment results, taking into account the labels given to the default (basically) and highest settings.

If you want to stay informed about new tests of AV-Comparatives, please register to subscribe to our newsletter.

[17] F-Secure sent us an updated scanner after running this test. With the new scanner F-Secure's overall performance (with default settings) was rated as “Very Fast” with an overhead of +34%. This update will be available to all users in the beginning of 2009.

7. Copyright and Disclaimer

AV-Comparatives e.V. (October 2008)