Anti-Virus Comparative
No. 23, August 2009

On-demand Detection of Malicious Software

includes false alarm and on-demand scanning speed test

Language: English
August 2009
Last Revision: 2009-09-19

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Professional Edition 4.8
- AVG Anti-Virus 8.5
- AVIRA AntiVir Premium 9.0
- BitDefender Anti-Virus 2010
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 4.0
- F-Secure Anti-Virus 2010
- G DATA AntiVirus 2010
- Kaspersky Anti-Virus 2010
- Kingsoft AntiVirus 9
- McAfee VirusScan Plus 2009
- Microsoft Live OneCare 2.5
- Norman Antivirus & Anti-Spyware 7.10
- Sophos Anti-Virus 7.6
- Symantec Norton Anti-Virus 2010
- Trustport Antivirus 2009

Conditions for participation and test methodology

The conditions for participation in our tests are listed in the methodology document at http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf. Before proceeding with this report, readers are advised to first read the above-mentioned document.

Products included in our tests constitute already some very good anti-virus software with relatively high on-demand detection rates, as this is one of the requirements needed to be included in our tests. The participation is usually limited to not more than 18 well-known and worldwide used quality Anti-Virus products with relatively high detection rates, which vendors agreed to get tested and included in this public report.

Tested Product Versions

The Malware sets, system sets and the products were updated and frozen on the 10th August 2009. The following 16 up-to-date products[1] were included in this public test:

- avast! Professional Edition 4.8.1348
- AVG Anti-Virus 8.5.406
- AVIRA AntiVir Premium 9.0.0.446
- BitDefender Anti-Virus 13.0.13.254
- eScan Anti-Virus 10.0.997.491
- ESET NOD32 Antivirus 4.0.437.0
- F-Secure Anti-Virus 10.00.246
- G DATA AntiVirus 20.0.4.9
- Kaspersky Anti-Virus 9.0.0.463
- Kingsoft AntiVirus 2009.08.05.16
- McAfee VirusScan Plus 13.11.102
- Microsoft Live OneCare 2.5.2900.28
- Norman Antivirus & Anti-Spyware 7.10.02
- Sophos Anti-Virus 7.6.10
- Symantec Norton Anti-Virus 17.0.0.136
- Trustport Antivirus 2.8.0.3017

Some products may offer additional features e.g. to provide additional protection against malware during its execution (if not detected in advance on-access or on-demand).

Please try the products on your own system before making a purchase decision based on these tests. There are also some other program features and important factors (e.g. price, ease of use/management, compatibility, graphical user interface, language, HIPS / behaviour blocker functions, etc.) to consider.

Although extremely important, the detection rate of a product is only one aspect of a complete Anti-Virus product. AV-Comparatives will publish in the next months the results of its full product / dynamic test, as well as other test reports which cover different aspects/features of the products.

[1] The August test allows the submission of RTM-versions if the (same) final version is going to be released before the report is published. Beta versions are not accepted.

Comments

As almost all products run nowadays in real life with highest protection settings by default or switch automatically to highest settings in case of a detected infection, we tested all products with highest settings (except Sophos and F-Secure).

Below are some notes about the used settings (scan of all files etc. is always enabled) and some technologies which need to be explained:

AVG, BitDefender, eScan, ESET, Kingsoft, Microsoft, Norman:
Runs with highest settings by default.

avast:
Runs (in case of an infection) by default automatically with highest settings.

G DATA:
Runs (depending from hardware) with highest settings by default.

AVIRA, Kaspersky, Symantec, TrustPort:
Asked to get tested with all extended categories enabled and with heuristic set to high/advanced. Due to that, we recommend users to consider also setting the heuristics to high/advanced, as those products do not use their highest settings by default.

F-Secure, Sophos:
Asked to get tested and awarded based on its default settings (without deep heuristic / suspicious detections). Due that, we suggest users to consider to also do not set the settings to high (except in case of an existing infection).

McAfee:
Uses an in-the-cloud technology (Artemis / Active Protection) which is enabled by default and working while an Internet connection is available. Artemis was tested at the same time as other products were updated so it did not have any time advantage over other products. For informational purposes, we noted also the results without the in-the-cloud technology (offline).

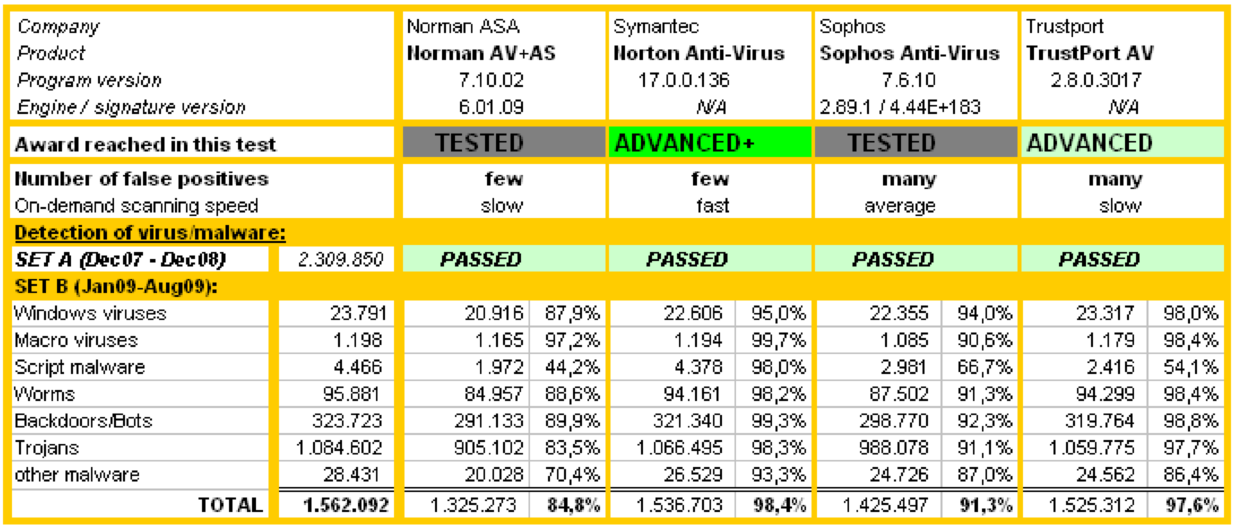
Test Results

Below are the test results tables containing the detection rate details of the various products.

Company		AVIRA		Alwil Software		AVG Technologies		BitDefender	
Product		**AntiVir Premium**		**avast! Professional**		**AVG Anti-Virus**		**BitDefender AV**	
Program version		9.0.0.446		4.8.1348		8.5.406		13.0.13.254	
Engine / signature version		8.02.00.248/7.01.05.93		090810-0		270.13.49/2294		N/A	
Award reached in this test		ADVANCED		ADVANCED+		ADVANCED		ADVANCED+	
Number of false positives		**many**		**few**		**few**		**few**	
On-demand scanning speed		fast		fast		slow		average	
Detection of virus/malware:									
SET A (Dec07 - Dec08)	*2.309.850*	***PASSED***		***PASSED***		***PASSED***		***PASSED***	
SET B (Jan09-Aug09):									
Windows viruses	23.791	23.698	99,6%	23.337	98,1%	22.700	95,4%	23.451	98,6%
Macro viruses	1.198	1.198	100%	1.188	99,2%	1.097	91,6%	1.176	98,2%
Script malware	4.466	4.410	98,7%	4.402	98,6%	2.063	46,2%	4.243	95,0%
Worms	95.881	95.350	99,4%	94.784	98,9%	92.016	96,0%	94.268	98,3%
Backdoors/Bots	323.723	322.389	99,6%	317.811	98,2%	309.579	95,6%	318.584	98,4%
Trojans	1.084.602	1.077.548	99,3%	1.062.424	98,0%	1.018.389	93,9%	1.058.782	97,6%
other malware	28.431	28.134	99,0%	27.669	97,3%	23.179	81,5%	27.579	97,0%
TOTAL	**1.562.092**	1.552.727	**99,4%**	1.531.615	**98,0%**	1.469.023	**94,0%**	1.528.083	**97,8%**

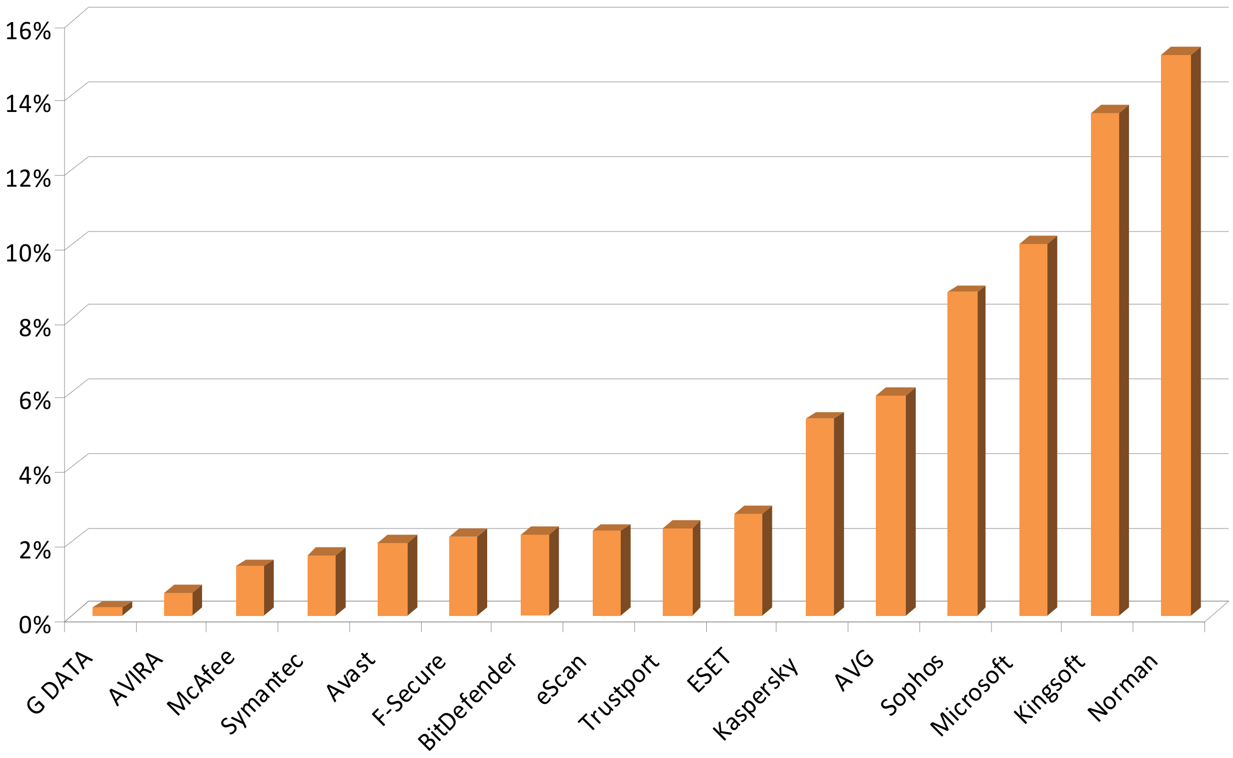
Company		MicroWorld		F-Secure		G DATA Security		Kaspersky Labs	
Product		**eScan ISS**		**F-Secure Anti-Virus**		**G DATA AntiVirus**		**Kaspersky AV**	
Program version		10.0.997.491		10.00.246		20.0.4.9		9.0.0.463	
Engine / signature version		N/A		9.10.15261		N/A		N/A	
Award reached in this test		ADVANCED+		ADVANCED+		ADVANCED+		ADVANCED	
Number of false positives		**few**		**few**		**few**		**few**	
On-demand scanning speed		slow		slow		average		average	
Detection of virus/malware:									
SET A (Dec07 - Dec08)	*2.309.850*	***PASSED***		***PASSED***		***PASSED***		***PASSED***	
SET B (Jan09-Aug09):									
Windows viruses	23.791	23.446	98,5%	23.460	98,6%	23.778	99,9%	22.890	96,2%
Macro viruses	1.198	1.176	98,2%	1.176	98,2%	1.198	100%	1.176	98,2%
Script malware	4.466	4.243	95,0%	4.245	95,1%	4.458	99,8%	4.094	91,7%
Worms	95.881	94.210	98,3%	94.380	98,4%	95.753	99,9%	93.724	97,8%
Backdoors/Bots	323.723	318.329	98,3%	319.042	98,6%	323.272	99,9%	312.236	96,5%
Trojans	1.084.602	1.057.669	97,5%	1.058.927	97,6%	1.082.183	99,8%	1.018.970	93,9%
other malware	28.431	27.567	97,0%	27.593	97,1%	28.409	99,9%	26.094	91,8%
TOTAL	**1.562.092**	1.526.640	**97,7%**	1.528.823	**97,9%**	1.559.051	**99,8%**	1.479.184	**94,7%**

Company		Kingsoft		McAfee		Microsoft		ESET	
Product		**Kingsoft AntiVirus**		**McAfee VirusScan+**		**Microsoft OneCare**		**NOD32 Antivirus**	
Program version		2009.11.6.63		13.11.102		2.5.2900.28		4.0.437.0	
Engine / signature version		*2009.8.10.12*		5400.1158 / 5705		1.63.1207.0		4323.1230	
Award reached in this test		TESTED		ADVANCED		STANDARD		ADVANCED+	
Number of false positives		**many**		**many**		**few**		**few**	
On-demand scanning speed		fast		average		slow		average	
Detection of virus/malware:									
SET A (Dec07 - Dec08)	*2.309.850*	***PASSED***		***PASSED***		***PASSED***		***PASSED***	
SET B (Jan09-Aug09):									
Windows viruses	23.791	19.725	82,9%	23.185	97,5%	21.919	92,1%	22.493	94,5%
Macro viruses	1.198	85	7,1%	1.198	100%	1.189	99,2%	1.198	100%
Script malware	4.466	1.295	29,0%	3.482	78,0%	3.721	83,3%	4.278	95,8%
Worms	95.881	85.588	89,3%	94.322	98,4%	91.190	95,1%	94.128	98,2%
Backdoors/Bots	323.723	291.986	90,2%	321.161	99,2%	299.285	92,5%	316.786	97,9%
Trojans	1.084.602	930.761	85,8%	1.072.925	98,9%	962.996	88,8%	1.053.237	97,1%
other malware	28.431	20.237	71,2%	25.144	88,4%	24.945	87,7%	26.888	94,6%
TOTAL	**1.562.092**	1.349.677	**86,4%**	1.541.417	**98,7%**	1.405.245	**90,0%**	1.519.008	**97,2%**



Company *Product* *Program version* *Engine / signature version*		Norman ASA **Norman AV+AS** 7.10.02 6.01.09		Symantec **Norton Anti-Virus** 17.0.0.136 N/A		Sophos **Sophos Anti-Virus** 7.6.10 2.89.1 / 4.44E+183		Trustport **TrustPort AV** 2.8.0.3017 N/A	
Award reached in this test		TESTED		ADVANCED+		TESTED		ADVANCED	
Number of false positives On-demand scanning speed		**few** slow		**few** fast		**many** average		**many** slow	
Detection of virus/malware:									
SET A (Dec07 - Dec08)	*2.309.850*	***PASSED***		***PASSED***		***PASSED***		***PASSED***	
SET B (Jan09-Aug09):									
Windows viruses	23.791	20.916	87,9%	22.606	95,0%	22.355	94,0%	23.317	98,0%
Macro viruses	1.198	1.165	97,2%	1.194	99,7%	1.085	90,6%	1.179	98,4%
Script malware	4.466	1.972	44,2%	4.378	98,0%	2.981	66,7%	2.416	54,1%
Worms	95.881	84.957	88,6%	94.161	98,2%	87.502	91,3%	94.299	98,4%
Backdoors/Bots	323.723	291.133	89,9%	321.340	99,3%	298.770	92,3%	319.764	98,8%
Trojans	1.084.602	905.102	83,5%	1.066.495	98,3%	988.078	91,1%	1.059.775	97,7%
other malware	28.431	20.028	70,4%	26.529	93,3%	24.726	87,0%	24.562	86,4%
TOTAL	**1.562.092**	1.325.273	**84,8%**	1.536.703	**98,4%**	1.425.497	**91,3%**	1.525.312	**97,6%**

Graph of missed samples (lower is better)



The results of our on-demand tests are usually applicable also for the on-access scanner (if configured the same way), but not for on-execution protection technologies (like HIPS, behaviour blockers, etc.).

A good detection rate is still one of the most important, deterministic and reliable features of an antivirus product. Additionally, most products provide at least some kind of HIPS, behaviour-based or other functionalities to block (or at least warn about the possibility of) malicious actions e.g. during the execution of malware, when all other on-access and on-demand detection/protection mechanism failed.

Please do not miss the second part of the report (it will be published in a few months) containing the retrospective test, which evaluates how well products are at detecting new/unknown malware. Further test reports (cleaning test, performance test, PUA detection test, dynamic test, etc.) covering other aspects of the various products will be released soon on our website.

Even if we deliver various tests and show different aspects of Anti-Virus software, users are advised to evaluate the software by themselves and build their own opinion about them. Test data or reviews just provide guidance to some aspects that users cannot evaluate by themselves. We suggest and encourage readers to research also other independent test results provided by various well-known and established independent testing organizations, in order to get a better overview about the detection and protection capabilities of the various products over different test scenarios and various test-sets.

The awards on page 13 are given according to the table below:

	Detection Rates			
	<87%	**87 - 93%**	**93 - 97%**	**97 - 100%**
Few (0-15 FP's)	**tested**	**STANDARD**	**ADVANCED**	**ADVANCED+**
Many (16-100 FP's)	**tested**	**tested**	**STANDARD**	**ADVANCED**

Summary results

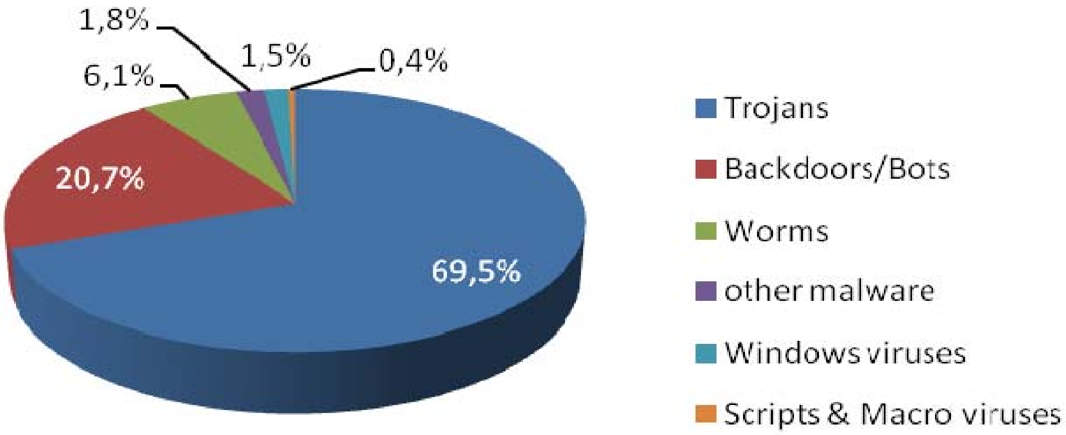
The test-set is split in two parts. The percentages below refer to SET B, which contains only malware from the last 7 months. SET A is usually covered very well (>97%) by all the tested products and contains malware from December 2007 to December 2008.

Please consider also the false alarm rates when looking at the below detection rates!

Total detection rates[2]:

1.	G DATA	99.8%
2.	AVIRA	99.4%
3.	McAfee[3]	98.7%
4.	Symantec	98.4%
5.	Avast	98.0%
6.	F-Secure	97.9%
7.	Bitdefender	97.8%
8.	eScan	97.7%
9.	Trustport	97.6%
10.	ESET	97.2%
11.	Kaspersky	94.7%
12.	AVG	94.0%
13.	Sophos	91.3%
14.	Microsoft	90.0%
15.	Kingsoft	86.4%
16.	Norman	84.8%

SET B contains nearly 1.6 million malware samples. The used malware test-set consists of:



[2] We estimate the remaining error margin to be around 0.2%

[3] McAfee VirusScan Plus 2009 and above comes with the "in-the-cloud" Artemis technology turned on by default. For corporate users or home users using older McAfee products without “Active Protection” - as well as all other users - it may be important to know what the baseline minimum detection rate of McAfee would be, should the Internet connection be not available. **The McAfee detection rate without Internet connection was 92.6%.**

False positive/alarm test

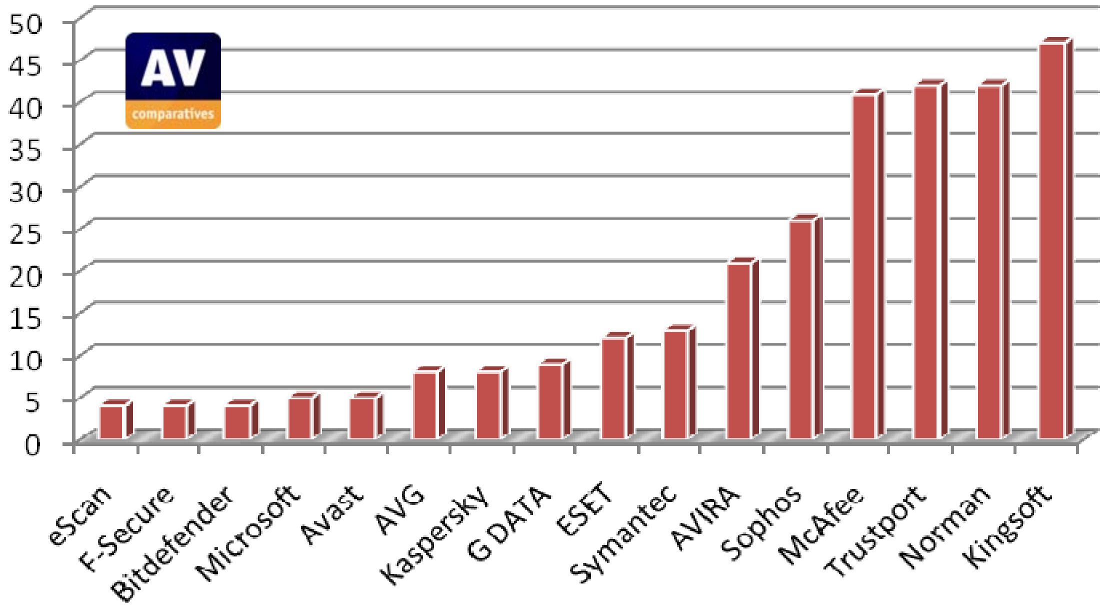
In order to better evaluate the quality of the detection capabilities of anti-virus products, we provide also a false alarm test. False alarms can sometimes cause as much troubles as a real infection. Please consider the false alarm rate when looking at the detection rates, as a product which is prone to cause false alarms achieves higher scores easier.

False Positive Results

Number of false alarms found in our full set of clean files (lower is better):

1.	Bitdefender, eScan, F-Secure	4	
2.	Microsoft, Avast	5	
3.	AVG, Kaspersky	8	few FP's
4.	G DATA	9	
5.	ESET	12	
6.	Symantec	13	
7.	AVIRA	21	
8.	Sophos	26	
9.	McAfee[4]	41	many FP's
10.	Trustport, Norman	42	
11.	Kingsoft	47	

The graph below shows the number of false alarms found in our set of clean files by the tested Anti-Virus products.



The details about the discovered false alarms can be seen in a separate report available at: http://www.av-comparatives.org/images/stories/test/fp/avc_report23_fp.pdf

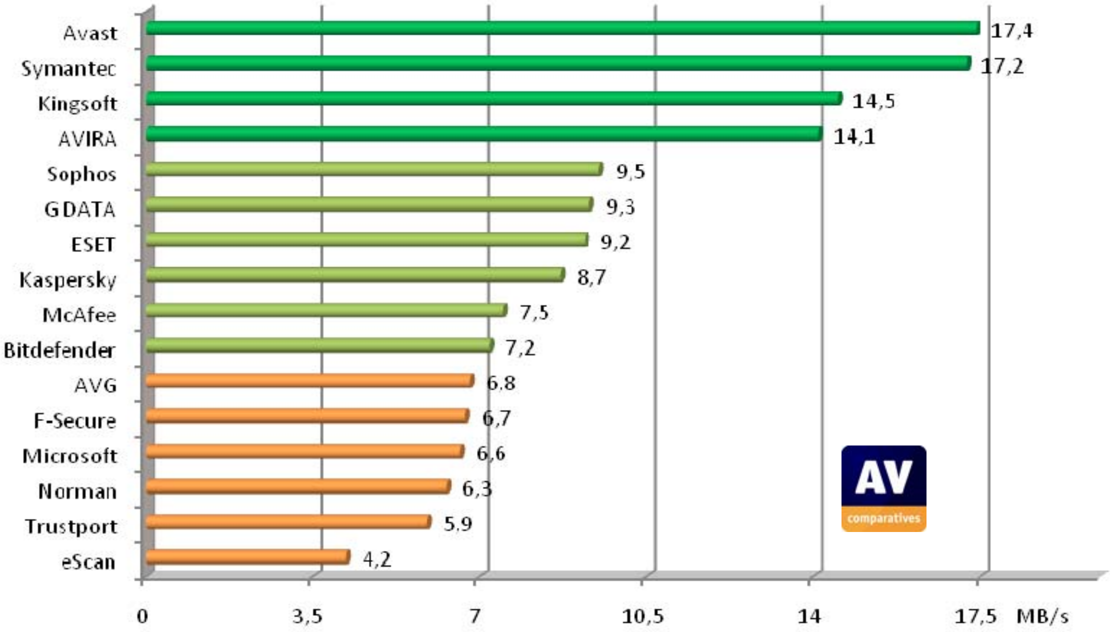
[4] McAfee without in-the-cloud had 26 false alarms.

Scanning Speed Test

Anti-Virus products have different scanning speeds due to various reasons. It has to be taken in account how reliable the detection rate of an Anti-Virus is; if the Anti-Virus product uses code emulation, if it is able to detect difficult polymorphic viruses, if it does a deep heuristic scan analysis and active rootkit scan, how deep and thorough the unpacking and unarchiving support is, additional security scans, etc.

Most products have technologies to decrease scan times on subsequent scans by skipping previously scanned files. As we want to know the scan speed (when files are really scanned for malware) and not the skipping files speed, those technologies are not taken into account here. In our opinion some products should inform the users more clearly about the performance-optimized scans and then let the users decide if they prefer a short performance-optimized scan (which does not re-check all files, with potential risk of overlooking infected files) or a full-security scan.

The following graph shows the throughput rate in MB/sec (higher is faster) of the various Anti-Virus products when scanning (on-demand) with highest settings our whole set of clean files (used for the false alarm testing). The scanning throughput rate will vary based on the set of clean files[5], the settings and the hardware used.



The average scanning throughput rate (scanning speed) is calculated by the size of the clean-set in MB's divided by the time needed to finish the scan in seconds. The scanning throughput rate of this test cannot be compared with future tests or with other tests, as it varies from the set of files, hardware used etc.

The scanning speed tests were done under Windows XP SP3, on identical Intel Core 2 Duo E8300/2.83GHz, 2GB RAM and SATA II disks.

[5] to know how fast various products would be on *your* PC at scanning *your* files, we advise you to try the products yourself

Award levels reached in this test

AV-Comparatives provides a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). As this report contains also the raw detection rates and not only the awards, users that do not care about false alarms can rely on that score alone if they want to.

AWARDS (based on detection rates and false alarms)	**PRODUCTS** (in no specific order)[6]
AV comparatives ADVANCED+ ★★★ ON DEMAND DETECTION TEST AUG 09	✓ G DATA ✓ Symantec ✓ Avast ✓ F-Secure ✓ BitDefender ✓ eScan ✓ ESET
AV comparatives ADVANCED ★★ ON DEMAND DETECTION TEST AUG 09	✓ AVIRA* ✓ McAfee* ✓ TrustPort* ✓ Kaspersky ✓ AVG
AV comparatives STANDARD ★ ON DEMAND DETECTION TEST AUG 09	✓ Microsoft
AV comparatives TESTED ON DEMAND DETECTION TEST AUG 09	✓ Sophos* ✓ Kingsoft ✓ Norman

*: those products got lower awards due false alarms

The Awards are not only based on detection rates - also False Positives found in our set of clean files are considered. A product that is successful at detecting a high percentage of malware but suffers from false alarms may not be necessarily better than a product which detects less malware but which generates less FP's.

[6] We suggest to consider products with same the award to be as good as the other products with same award.

Copyright and Disclaimer

AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss, which might occur as 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 a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. 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 e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (September 2009)