Anti-Virus Comparative
No. 25, February 2010

On-demand Detection of Malicious Software

includes false alarm and on-demand scanning speed test

Language: English
February 2010
Last Revision: 17th March 2010

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Free Antivirus 5.0
- AVG Anti-Virus 9.0
- AVIRA AntiVir Premium 9.0
- BitDefender Antivirus 2010
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 4.0
- F-Secure Anti-Virus 2010
- G DATA AntiVirus 2010
- K7 TotalSecurity 10.0
- Kaspersky Anti-Virus 2010
- Kingsoft AntiVirus 2010
- McAfee AntiVirus Plus 2010
- Microsoft Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 7.30
- Panda Antivirus Pro 2010
- PC Tools Spyware Doctor with AV 7.0
- Sophos Anti-Virus 9.0
- Symantec Norton Anti-Virus 2010
- Trend Micro AntiVirus plus AntiSpyware 2010
- Trustport Antivirus 2010

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.

The participation is limited to not more than 20 well-known and worldwide used quality Anti-Virus products, which vendors agreed to get tested and included in the public test-series of 2010.

Tested Product Versions

The Malware sets have been frozen the 3rd February 2010. The system sets and the products were updated and frozen on the 10th February 2010. The following 20 up-to-date products were included in this public test:

- avast! Free[1] Antivirus 5.0.396
- AVG Anti-Virus 9.0.733
- AVIRA AntiVir Premium 9.0.0.457
- BitDefender Anti-Virus 13.0.19.347
- eScan Anti-Virus 10.0.1058.644
- ESET NOD32 Antivirus 4.0.474.0
- F-Secure Anti-Virus 10.12.108
- G DATA AntiVirus 20.2.4.1
- K7 TotalSecurity 10.0.0025
- Kaspersky Anti-Virus 9.0.0.736 (a.b)
- Kingsoft AntiVirus 2010.2.10.1
- McAfee AntiVirus Plus 14.0.306
- Microsoft Security Essentials 1.0.1611.0
- Norman Antivirus & Anti-Spyware 7.30
- Panda Antivirus Pro 9.01.00
- PC Tools Spyware Doctor with Antivirus 7.0.0.514
- Sophos Anti-Virus 9.0.3
- Symantec Norton Anti-Virus 17.5.0.127
- Trend Micro AntiVirus plus AntiSpyware 17.50.1366.0
- Trustport[2] Antivirus 5.0.0.4087

K7, Panda, PC Tools and Trend Micro are new participants of the 2010 test-series.

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, URL filter/reputation services, support, etc.) to consider. 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).

Although extremely important, the detection rate of a product is only one aspect of a complete Anti-Virus product. AV-Comparatives provides also a whole product / dynamic test, as well as other test reports which cover different aspects/features of the products.

[1] Alwil Software decided to participate in the tests with their free product version.
[2] Based on two engines (AVG and Bitdefender).

Comments

Almost all products run nowadays by default with highest protection settings (at least either at the entry points, during whole computer on-demand scans or scheduled scans) or switch automatically to highest settings in case of a detected infection. Due that, in order to get comparable results, we tested all products with highest settings, if not explicitly advised otherwise by the vendors (as we will use same settings over all tests, the reason is usually that their highest settings either cause too many false alarms, have a too high impact on system performance, or the settings are planned to be changed/removed by the vendor in near future). To avoid some frequent questions, below are some notes about the used settings (scan of all files etc. is always enabled) of some products:

AVIRA, Kaspersky, Symantec, TrustPort: asked to get tested with heuristic set to high/advanced. Due to that, we recommend users to consider also setting the heuristics to high/advanced.

F-Secure, Sophos: asked to get tested and awarded based on their default settings (i.e. without using their advanced heuristics / suspicious detections setting).

AVG, AVIRA: asked to do not enable/consider the informational warnings of packers as detections. Due that, we did not count them as detections (neither on the malware set, nor on the clean set).

AV-Comparatives prefers to test with default settings. As most products run with highest settings by default (or switch to highest automatically when malware is found, making it impossible to test against various malware with "default" settings), in order to get comparable results we set also the few remaining products to highest settings (or leave them to lower settings) in accordance with the respective vendors. We hope that all vendors will find the appropriate balance of detection/false alarms/system impact and will provide highest security already by default and remove paranoid settings inside the user interface which are too high to be ever of any benefit for normal users.

What's new in this test

You will notice that this time the test-set is smaller than previous times. This is because we are now trying to include in the test-set mainly prevalent real-world malware being still around (within last eight months). To build the test-set we consulted (but as it was a first try, we did not exclusively rely on) metadata and telemetry data collected and shared within AV industry, as well as querying various clouds afterwards and requesting data of the most-common user-submitted malware. Malware we see on user PC's are automatically considered as important. Nevertheless, as with every first attempt, we noticed that not all sources are yet able to provide reliable prevalence data, so we had to clean up some sets afterwards. This will improve in future, as the industry is currently working on optimizing their data sharing processes.

Anyway, considering that the used test-set will probably get smaller and focus mainly on threats that should be detected and should be easier to spot, we expect products to score higher. This is the reason why we may increase next time the marks to get higher awards. Next time also the marks for FPs to get "ADVANCED+" may be set stricter.

What's also new and interesting is the prevalence information we try to give inside the detailed false alarm report (see link on page 10).

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! Free Antivirus**		**AVG Anti-Virus**		**BitDefender AV**	
Program version		9.0.0.457		5.0.396		9.0.733		13.0.19.347	
Engine / signature version		8.02.01.160/7.10.04.23		100210-0		271.1.1/2679		*N/A*	
Award reached in this test		ADVANCED+		ADVANCED+		ADVANCED		ADVANCED+	
Number of false positives		**few**		**few**		**few**		**very few**	
On-demand scanning speed		fast		fast		average		slow	
Windows viruses	19.396	19.322	99,6%	19.148	98,7%	18.916	97,5%	19.233	99,2%
Macro viruses	1.617	1.610	99,6%	1.605	99,3%	1.583	97,9%	1.564	96,7%
Script malware	3.585	3.283	91,6%	3.424	95,5%	2.152	60,0%	3.196	89,1%
Worms	116.446	116.210	99,8%	115.469	99,2%	113.856	97,8%	115.612	99,3%
Backdoors/Bots	129.883	129.224	99,5%	126.120	97,1%	122.951	94,7%	126.081	97,1%
Trojans	939.654	933.161	99,3%	912.612	97,1%	883.623	94,0%	915.332	97,4%
other malware	14.151	13.111	92,7%	13.172	93,1%	10.644	75,2%	13.553	95,8%
TOTAL	**1.224.732**	1.215.921	**99,3%**	1.191.550	**97,3%**	1.153.725	**94,2%**	1.194.571	**97,5%**

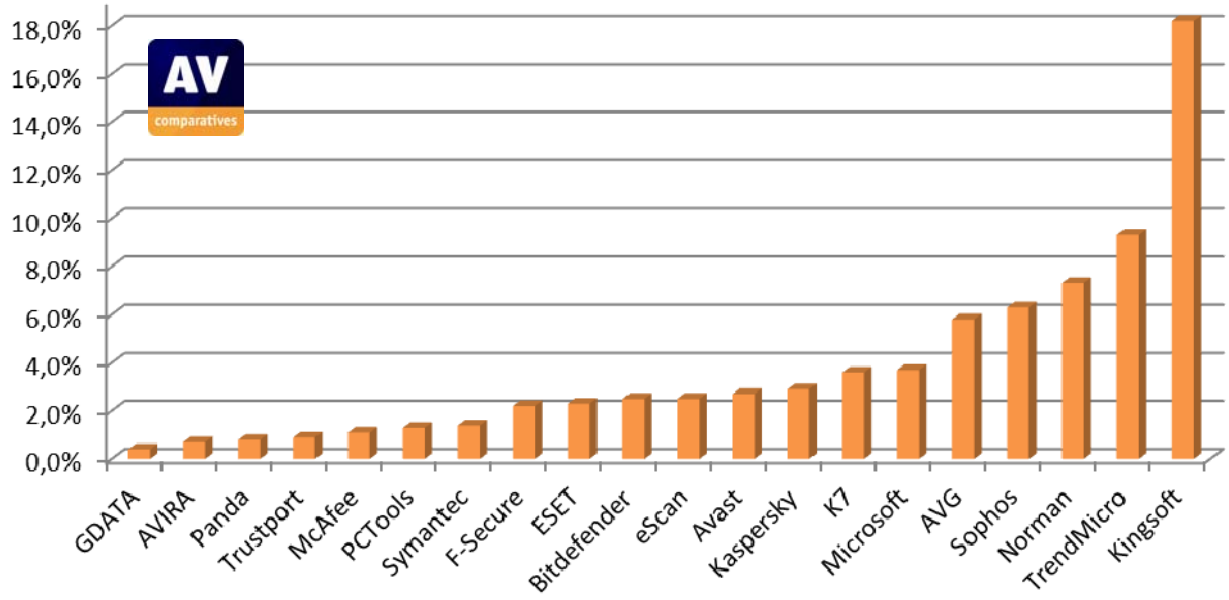
Company		MicroWorld		F-Secure		G DATA Security		K7 Computing	
Product		**eScan Anti-Virus**		**F-Secure Anti-Virus**		**G DATA AntiVirus**		**K7 TotalSecurity**	
Program version		10.0.1058.644		10.12.108		20.2.4.1		10.0.0025	
Engine / signature version		*N/A*		9.20.15437		*N/A*		9.38.0891	
Award reached in this test		ADVANCED+		ADVANCED+		ADVANCED+		STANDARD	
Number of false positives		**very few**		**very few**		**few**		**very many**	
On-demand scanning speed		slow		slow		average		average	
Windows viruses	19.396	19.233	99,2%	19.284	99,4%	19.363	99,8%	17.840	92,0%
Macro viruses	1.617	1.564	96,7%	1.564	96,7%	1.617	100%	1.598	98,8%
Script malware	3.585	3.196	89,1%	3.199	89,2%	3.575	99,7%	1.519	42,4%
Worms	116.446	115.612	99,3%	115.678	99,3%	116.294	99,9%	114.680	98,5%
Backdoors/Bots	129.883	126.079	97,1%	126.401	97,3%	129.290	99,5%	126.382	97,3%
Trojans	939.654	915.330	97,4%	917.468	97,6%	935.203	99,5%	909.035	96,7%
other malware	14.151	13.553	95,8%	13.575	95,9%	14.029	99,1%	9.427	66,6%
TOTAL	**1.224.732**	1.194.567	**97,5%**	1.197.169	**97,7%**	1.219.371	**99,6%**	1.180.481	**96,4%**

Company		Kaspersky Labs		Kingsoft		McAfee		ESET	
Product		**Kaspersky AV**		**Kingsoft AntiVirus**		**McAfee AntiVirus +**		**NOD32 Antivirus**	
Program version		9.0.0.736 (a.b)		2010.02.10.01		14.0.306		4.0.474.0	
Engine / signature version		*N/A*		*N/A*		5400.1158 / 5888		4854.1261	
Award reached in this test		ADVANCED+		TESTED		ADVANCED		ADVANCED+	
Number of false positives		**few**		**many**		**many**		**very few**	
On-demand scanning speed		average		average		slow		average	
Windows viruses	19.396	18.127	93,5%	15.796	81,4%	19.336	99,7%	19.135	98,7%
Macro viruses	1.617	1.617	100%	1.524	94,2%	1.617	100%	1.615	99,9%
Script malware	3.585	3.257	90,9%	632	17,6%	2.400	66,9%	2.972	82,9%
Worms	116.446	115.619	99,3%	97.539	83,8%	115.905	99,5%	115.821	99,5%
Backdoors/Bots	129.883	126.132	97,1%	99.965	77,0%	128.319	98,8%	126.931	97,7%
Trojans	939.654	910.585	96,9%	778.478	82,8%	931.514	99,1%	916.549	97,5%
other malware	14.151	13.535	95,6%	7.924	56,0%	12.329	87,1%	12.988	91,8%
TOTAL	**1.224.732**	1.188.872	**97,1%**	1.001.858	**81,8%**	1.211.420	**98,9%**	1.196.011	**97,7%**

Company		Norman ASA		Symantec		Panda Security		Microsoft	
Product		**Norman AV+AS**		**Norton Anti-Virus**		**Panda Antivirus Pro**		**Security Essentials**	
Program version		7.30		17.5.0.127		9.01.00		1.0.1611.0	
Engine / signature version		6.04.03		120210d		*N/A*		1.75.617.0	
Award reached in this test		TESTED		ADVANCED+		ADVANCED		ADVANCED	
Number of false positives		**many**		**few**		**many**		**very few**	
On-demand scanning speed		slow		fast		fast		slow	
Windows viruses	19.396	17.990	92,8%	18.844	97,2%	19.288	99,4%	18.288	94,3%
Macro viruses	1.617	1.597	98,8%	1.612	99,7%	1.339	82,8%	1.611	99,6%
Script malware	3.585	2.283	63,7%	3.222	89,9%	1.462	40,8%	2.766	77,2%
Worms	116.446	112.958	97,0%	115.890	99,5%	116.082	99,7%	115.283	99,0%
Backdoors/Bots	129.883	119.276	91,8%	127.532	98,2%	129.824	100,0%	125.643	96,7%
Trojans	939.654	870.424	92,6%	926.445	98,6%	937.570	99,8%	903.838	96,2%
other malware	14.151	10.647	75,2%	13.847	97,9%	9.611	67,9%	12.319	87,1%
TOTAL	**1.224.732**	1.135.175	**92,7%**	1.207.392	**98,6%**	1.215.176	**99,2%**	1.179.748	**96,3%**

Company		Sophos		PC Tools		Trend Micro		Trustport	
Product		**Sophos Anti-Virus**		**SpywareDoctor+AV**		**Trend Micro AV+AS**		**TrustPort AV**	
Program version		9.0.3		7.0.0.514		17.50.1366.0000		5.0.0.4087	
Engine / signature version		3.4.2 / 4.50G+204		*N/A*		6.837.50		*N/A*	
Award reached in this test		ADVANCED		ADVANCED+		TESTED		ADVANCED+	
Number of false positives		**few**		**few**		**many**		**few**	
On-demand scanning speed		fast		average		average		slow	
Windows viruses	19.396	18.824	97,1%	18.938	97,6%	18.431	95,0%	19.343	99,7%
Macro viruses	1.617	1.603	99,1%	1.612	99,7%	1.604	99,2%	1.616	99,9%
Script malware	3.585	2.370	66,1%	3.226	90,0%	2.751	76,7%	3.264	91,0%
Worms	116.446	111.679	95,9%	115.904	99,5%	112.164	96,3%	116.204	99,8%
Backdoors/Bots	129.883	119.668	92,1%	127.744	98,4%	115.407	88,9%	128.922	99,3%
Trojans	939.654	880.523	93,7%	926.911	98,6%	849.330	90,4%	930.394	99,0%
other malware	14.151	12.317	87,0%	13.921	98,4%	11.061	78,2%	13.758	97,2%
TOTAL	**1.224.732**	1.146.984	**93,7%**	1.208.256	**98,7%**	1.110.748	**90,7%**	1.213.501	**99,1%**

Graph of missed samples (lower is better)



Percentages refer to the used test-set only. Even if it is just a subset of malware, due its size, it is important to look at the number of missed malware. For example, 0.3% means almost 3700 missed malware samples from the used test-set.

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 Anti-Virus 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.

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.

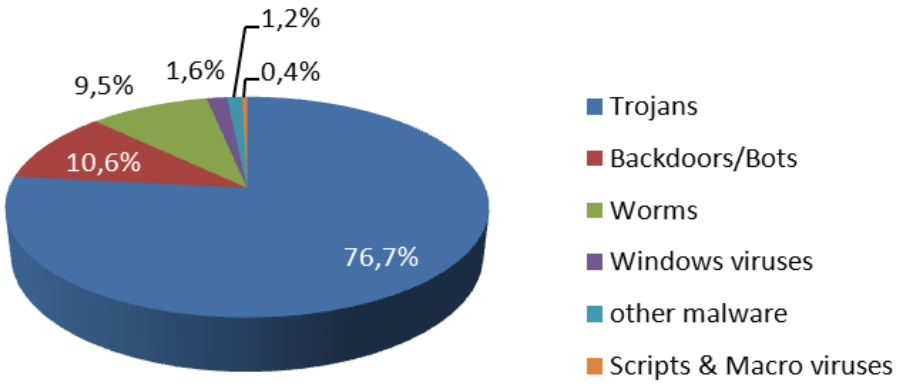
Summary results

Please consider also the false alarm rates when looking at the below detection rates[3]!

Total detection rates[4]:

1.	G DATA	99.6%
2.	AVIRA	99.3%
3.	Panda	99.2%
4.	Trustport	99.1%
5.	McAfee	98.9%
6.	PC Tools	98.7%
7.	Symantec	98.6%
8.	F-Secure	97.8%
9.	ESET	97.7%
10.	Bitdefender, eScan	97.5%
11.	Avast	97.3%
12.	Kaspersky	97.1%
13.	K7	96.4%
14.	Microsoft	96.3%
15.	AVG	94.2%
16.	Sophos	93.7%
17.	Norman	92.7%
18.	Trend Micro	90.7%
19.	Kingsoft	81.8%

The used test-set contains about 1.2 million malware samples and consists of:



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

[4] Additional results: The McAfee detection rate with "very high" in-the-cloud sensitivity would have scored 99.0% and have "very many" false alarms.
Baseline minimum detection rates of some products when there is no Internet connection available (i.e. without their in-the-cloud technology): McAfee: 94.9% (19 FPs) , Panda: 73.3% (32 FPs), Trend Micro: 68.5% (22 FPs)

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. All discovered false alarms were reported and sent to the respective Anti-Virus vendors and have now been already fixed.

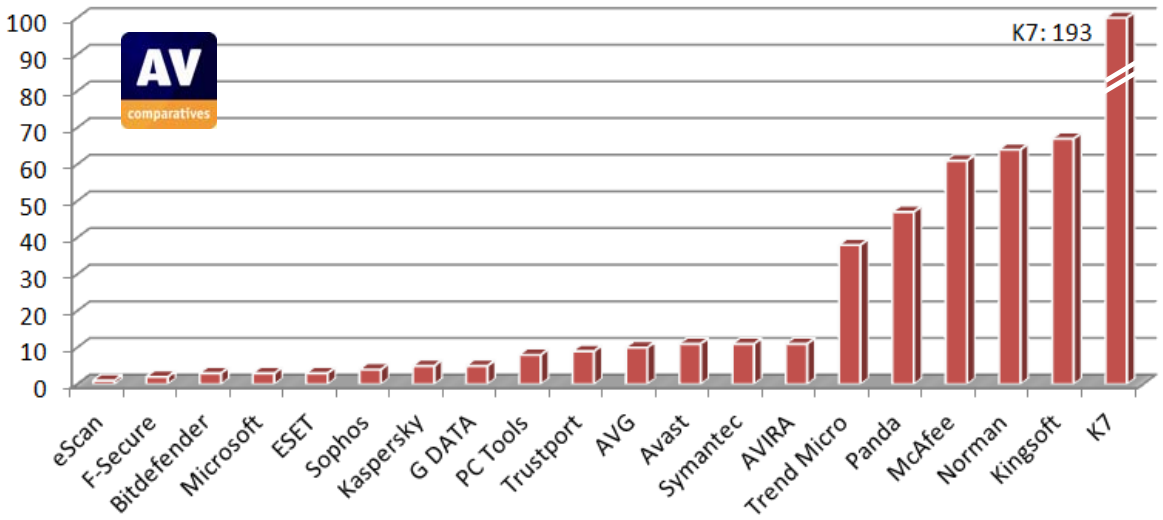
False Positive Results

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

1.	eScan	1	
2.	F-Secure	2	very few FP's
3.	Bitdefender, Microsoft, ESET	3	
4.	Sophos	4	
5.	Kaspersky, G DATA	5	
6.	PC Tools	8	few FP's
7.	Trustport	9	
8.	AVG	10	
9.	Avast, Symantec, AVIRA	11	
10.	Trend Micro	38	
11.	Panda	47	
12.	McAfee	61	many FP's
13.	Norman	64	
14.	Kingsoft	67	
15.	K7	193	very many FP's

The details about the discovered false alarms (including their prevalence) can be seen in a separate report available at:
http://www.av-comparatives.org/images/stories/test/fp/avc_report25_fp.pdf

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

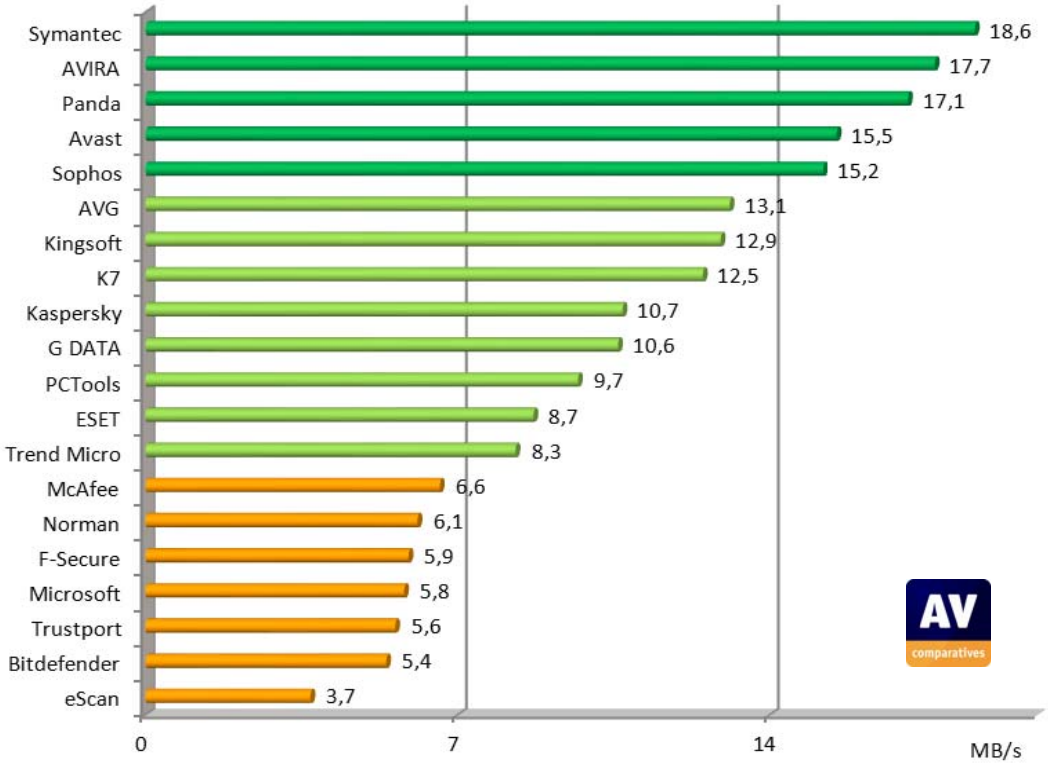


Scanning Speed Test

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, if it really scans all file types (or uses e.g. white lists in the cloud), 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 the 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 e.g. 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
	✓ G DATA ✓ AVIRA ✓ TrustPort ✓ PC Tools ✓ Symantec ✓ F-Secure ✓ ESET ✓ BitDefender ✓ eScan ✓ Avast ✓ Kaspersky
	✓ McAfee* ✓ Panda* ✓ Microsoft ✓ Sophos ✓ AVG
	✓ K7*
	✓ Norman* ✓ Trend Micro* ✓ Kingsoft

*: 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.

The awards were given according to the table below (may change next time):

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

Copyright and Disclaimer

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

AV-Comparatives e.V. (March 2010)