Anti-Virus Comparative

On-demand Detection of Malicious Software

includes false alarm and on-demand scanning speed test

Language: English
February 2011
Last Revision: 13th April 2011

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Free Antivirus 5.1
- AVG Anti-Virus Free Edition 10.0
- AVIRA AntiVir Personal 10.0
- BitDefender Antivirus Pro 2011
- eScan Anti-Virus 11.0
- ESET NOD32 Antivirus 4.2
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2011
- K7 TotalSecurity 10.0
- Kaspersky Anti-Virus 2011
- McAfee AntiVirus Plus 2011
- Microsoft Security Essentials 2.0
- Panda Antivirus Pro 2011
- PC Tools Spyware Doctor with AV 8.0
- Qihoo 360 Antivirus 1.1
- Sophos Anti-Virus 9.5
- Symantec Norton Anti-Virus 2011
- Trend Micro Titanium AntiVirus+ 2011
- Trustport Antivirus 2011
- Webroot AntiVirus with Spy Sweeper 7.0

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 Anti-Virus products, which vendors agreed to get tested and included in the public test-series of 2011.

Tested Product Versions

The Malware sets have been frozen the 10th February 2011. The system sets and the products were updated and frozen on the 22nd February 2011. The following 20 up-to-date products[1] were included in this public test:

- avast! Free Antivirus 5.1.889[2]
- AVG Anti-Virus Free Edition 10.0.1204
- AVIRA AntiVir Personal 10.0.0.611
- BitDefender Anti-Virus Pro 14.0.24.337
- eScan Anti-Virus 11.0.1139.855
- ESET NOD32 Antivirus 4.2.71.2
- F-Secure Anti-Virus 10.51.106
- G DATA AntiVirus 21.1.2.2
- K7 TotalSecurity 10.0.0051
- Kaspersky Anti-Virus 11.0.2.556
- McAfee AntiVirus Plus 14.5.130
- Microsoft Security Essentials 2.0.657.0
- Panda Antivirus Pro 10.00.00
- PC Tools Spyware Doctor with Antivirus 8.0.0.624
- Qihoo 360 Antivirus 1.1.0.1310
- Sophos Anti-Virus 9.5.5
- Symantec Norton Anti-Virus 18.5.0.125
- Trend Micro Titanium AntiVirus+ 2011
- Trustport Antivirus 11.0.0.4606
- Webroot AntiVirus with Spy Sweeper 7.0.6.38

Please try the products[3] 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] Avast, AVG and AVIRA wanted to participate in the tests with their free product version.
[2] Avast submitted version 5.1 for testing. The on-demand detection rate of Avast version 6.0 would be the same (confirmed also by Avast).
[3] Information about used additional third-party engines/signatures inside the products: **eScan**, **F-Secure** and **Qihoo 360** are based on the Bitdefender engine. **G DATA** is based on the Avast and Bitdefender engines. **PC Tools** is using the signatures of Symantec. **Trustport** is based on the AVG and Bitdefender engines. **Webroot** is based on the Sophos engine.

Comments

Nowadays, almost all products run with the highest protection settings by default (at least during on-demand / scheduled scans), some however may automatically switch to the highest settings once infection detections begin to occur. Due to this, and in order to ensure comparable results, we tested all products with the highest settings unless explicitly advised by the security vendors. The vendors may do this as they prefer the highest settings not to be used due to high number of False Alarms, or perhaps the highest settings will have a performance impact, or maybe they are planning to change/remove the setting in the near future. Below are some notes about the settings used (scan all files etc is always enabled), e.g.: where the settings are not set to the highest by default:

Avast, AVIRA, Kaspersky, Symantec: asked to get tested with heuristic set to high/advanced. For this reason, 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. So, 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 kindly ask vendors to provide stronger settings by default, i.e. set their default settings to highest levels of detection, esp. for scheduled scans or scans initiated by the user this would make more sense. We also kindly ask vendors to remove paranoid settings inside the user interface which are too high to be ever of any benefit for normal users. As some vendors decided to take part in our tests using the stronger settings (although they know that this will be applied and impact also other tests like false alarm test, performance test, etc.), it appears that the better option would be to go for the stronger settings by default and that is why we recommend users to consider to use those settings too.

Several products make use of cloud technologies, which require an active internet connection. Our test is performed using an active internet connection. Although we do not longer show the baseline detection rates without cloud and show instead only the results with active cloud, users should be aware that detection rates may in some few cases be lower if the scan is performed while offline. The cloud should be considered as an additional benefit/feature to increase detection rates (as well as response times and false alarm suppression) and not as a full replacement for local offline detections. Vendors should make sure that users are warned in case that the connectivity to the cloud gets lost e.g. during a scan, which may affect considerably the provided protection and make e.g. the initiated scan useless. We have seen that products which rely much on the cloud may perform better in detecting PE malware, while scoring lower in detecting malware in non-PE format, like present in the "other malware/viruses" category.

Telemetry data has been consulted to include malware samples which are/were hitting users in the last six months. Due the focus on prevalent and recent samples (majority is from last three months), the size of the test-set is smaller than in previous years.

Test Results

As nowadays Windows viruses, Macro viruses and scripts are only a small group compared to the prevalent number of Trojans, backdoors, worms, etc., those subgroups are no longer listed separately. They are now counted in the group "other malware/viruses", together with Rootkits, Exploits, etc.

Below are the test results tables containing the detection rate details of the various products over the used test-set.

Company *Product* *Program version*		Qihoo **360 Antivirus** 1.1.0.1310		AVIRA **AntiVir Personal** 10.0.0.611		Avast Software **avast! Free Antivirus** 5.1.889		AVG Technologies **AVG Free Anti-Virus** 10.0.1204	
Award reached in this test		STANDARD		ADVANCED+		ADVANCED		STANDARD	
Number of false positives On-demand scanning speed		**very many** average		**few** average		**many** fast		**few** average	
Worms	23.273	23.215	99,8%	23.094	99,2%	23.068	99,1%	22.581	97,0%
Backdoors/Bots	42.988	42.513	98,9%	42.539	99,0%	42.336	98,5%	39.786	92,6%
Trojans	319.560	313.190	98,0%	312.225	97,7%	314.355	98,4%	292.207	91,4%
other malware/viruses	17.722	16.179	91,3%	15.539	87,7%	17.135	96,7%	14.300	80,7%
TOTAL	**403.543**	395.097	**97,9%**	393.397	**97,5%**	396.894	**98,4%**	368.874	**91,4%**

Company *Product* *Program version*		BitDefender **BitDefender AV Pro** 14.0.24.337		MicroWorld **eScan Anti-Virus** 11.0.1139.855		F-Secure **F-Secure Anti-Virus** 10.51.106		G DATA Security **G DATA AntiVirus** 21.1.2.2	
Award reached in this test		ADVANCED+		ADVANCED+		ADVANCED+		ADVANCED	
Number of false positives On-demand scanning speed		**few** average		**few** average		**few** average		**many** average	
Worms	23.273	23.072	99,1%	23.072	99,1%	23.089	99,2%	23.261	99,9%
Backdoors/Bots	42.988	42.132	98,0%	42.132	98,0%	42.416	98,7%	42.896	99,8%
Trojans	319.560	312.359	97,7%	311.795	97,6%	313.915	98,2%	318.845	99,8%
other malware/viruses	17.722	16.153	91,1%	16.153	91,1%	16.279	91,9%	17.602	99,3%
TOTAL	**403.543**	393.716	**97,6%**	393.152	**97,4%**	395.699	**98,1%**	402.604	**99,8%**

Company *Product* *Program version*		K7 Computing **K7 TotalSecurity** 10.0.0051		Kaspersky Labs **Kaspersky AV** 11.0.2.556		McAfee **McAfee AntiVirus +** 14.5.130		ESET **NOD32 Antivirus** 4.2.71.2	
Award reached in this test		TESTED		ADVANCED+		ADVANCED+		ADVANCED	
Number of false positives On-demand scanning speed		**few** fast		**few** average		**none** average		**many** average	
Worms	23.273	21.711	93,3%	23.105	99,3%	23.013	98,9%	23.069	99,1%
Backdoors/Bots	42.988	36.733	85,4%	42.028	97,8%	42.441	98,7%	42.006	97,7%
Trojans	319.560	272.123	85,2%	308.880	96,7%	309.287	96,8%	312.111	97,7%
other malware/viruses	17.722	9.836	55,5%	17.250	97,3%	16.032	90,5%	16.082	90,7%
TOTAL	**403.543**	340.403	**84,4%**	391.263	**97,0%**	390.773	**96,8%**	393.268	**97,5%**

Company *Product* *Program version*		Symantec **Norton Anti-Virus** 18.5.0.125		Panda Security **Panda Antivirus Pro** 10.00.00		Microsoft **Security Essentials** 2.0.657.0		Sophos **Sophos Anti-Virus** 9.5.5	
Award reached in this test		ADVANCED		ADVANCED		ADVANCED		ADVANCED	
Number of false positives On-demand scanning speed		**few** average		**many** fast		**very few** slow		**few** average	
Worms	23.273	21.755	93,5%	23.122	99,4%	23.005	98,8%	22.328	95,9%
Backdoors/Bots	42.988	41.638	96,9%	42.966	99,9%	41.211	95,9%	37.822	88,0%
Trojans	319.560	307.215	96,1%	318.934	99,8%	308.242	96,5%	304.553	95,3%
other malware/viruses	17.722	14.748	83,2%	11.024	62,2%	14.115	79,6%	15.008	84,7%
TOTAL	**403.543**	385.356	**95,5%**	396.046	**98,1%**	386.573	**95,8%**	379.711	**94,1%**

Company *Product* *Program version*		PC Tools **SpywareDoctor+AV** 8.0.0.624		Trend Micro **Trend Micro TiAV+** 2011		Trustport **Trustport Antivirus** 11.0.0.4606		Webroot **Webroot AV+SS** 7.0.6.38	
Award reached in this test		STANDARD		STANDARD		ADVANCED+		TESTED	
Number of false positives On-demand scanning speed		**few** slow		**very many** average		**few** average		**many** fast	
Worms	23.273	21.599	92,8%	23.131	99,4%	23.233	99,8%	21.732	93,4%
Backdoors/Bots	42.988	40.545	94,3%	41.762	97,1%	42.675	99,3%	35.928	83,6%
Trojans	319.560	297.403	93,1%	300.564	94,1%	317.376	99,3%	272.565	85,3%
other malware/viruses	17.722	14.749	83,2%	15.601	88,0%	17.071	96,3%	14.802	83,5%
TOTAL	**403.543**	374.296	**92,8%**	381.058	**94,4%**	400.355	**99,2%**	345.027	**85,5%**

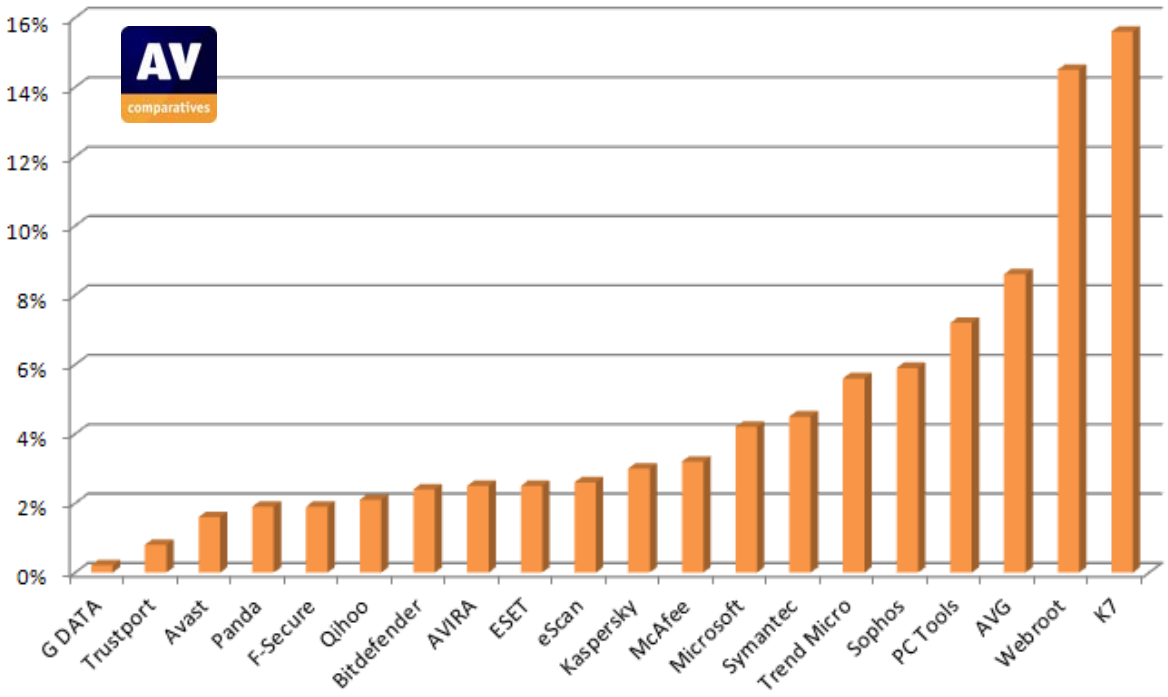
As announced in previous reports (and applied already in the Whole-Product Dynamic Test of 2010), this year the awards for this test are given as follow: The total detection rates (with two decimal places) are grouped by the testers after looking at the clusters build with the hierarchal clustering method. The false alarms are taken into account as usual (may be applied stricter in future for "very many" and "crazy many"), but we are evaluating to change the FP rating.

By using clusters, there are no longer fixed thresholds to reach, as the thresholds change based on the various results. The testers may group the clusters rationally and not rely solely on the clusters, to avoid that if e.g. all products would in future score badly, they do not get high rankings anyway.

Users which prefer the old award system, can apply themselves the rating system based on fixed percentages, but should keep in mind that the test-set is just a subset and not an absolute set, so fluctuations of single detection rates in different tests should not be overrated. Users can look at the numbers to compare the different detections rates of products within a specific test over a set of malware.

	Detection Rate Clusters/Groups (given by the testers after consulting statistical methods)			
	4	**3**	**2**	**1**
Few (0-15 FP's)	**TESTED**	**STANDARD**	**ADVANCED**	**ADVANCED+**
Many (16-100 FP's)	**TESTED**	**TESTED**	**STANDARD**	**ADVANCED**
Very many (101-500 FP's)	**TESTED**	**TESTED**	**STANDARD**	**STANDARD**
Crazy many (over 500 FP's)	**TESTED**	**TESTED**	**TESTED**	**TESTED**

Graph of missed samples (lower is better)



Percentages refer to the used test-set only. Even if it is just a subset of malware, it is important to look at the number of missed malware.

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, reputation-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.

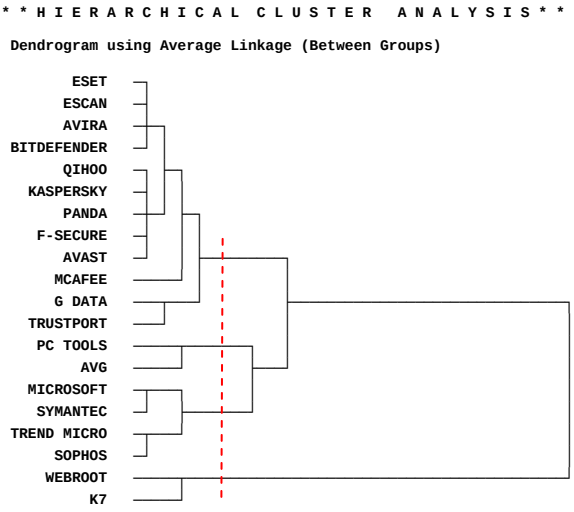
Even if we deliver various tests and show different aspects of Anti-Virus software, users are advised to evaluate the software by themselves and build their own opinion about them. Test data or reviews just provide guidance to some aspects that users cannot evaluate by themselves. We suggest and encourage 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

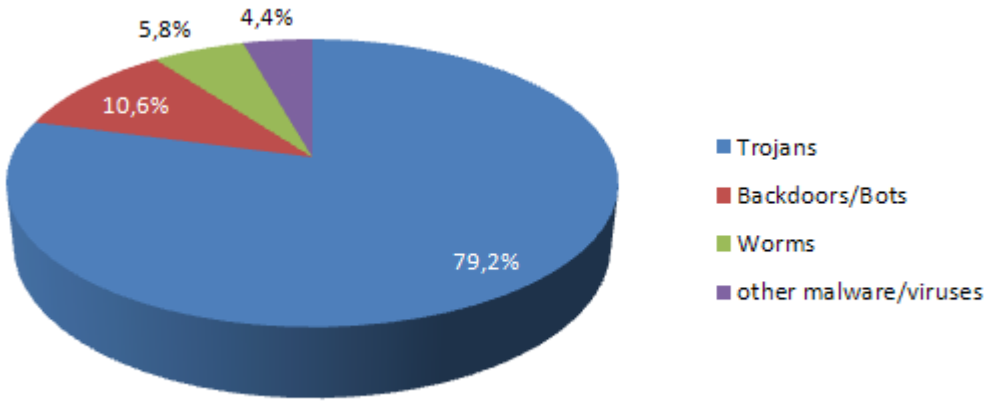
Please consider also the false alarm rates when looking at the below detection rates[4].

Total detection rates (clustered into four groups):

1.	G DATA	99.8%
2.	Trustport	99.2%
3.	Avast	98.4%
4.	Panda, F-Secure	98.1%
5.	Qihoo	97.9%
6.	Bitdefender	97.6%
7.	AVIRA, ESET	97.5%
8.	eScan	97.4%
9.	Kaspersky	97.0%
10.	McAfee	96.8%
11.	Microsoft	95.8%
12.	Symantec	95.5%
13.	Trend Micro	94.4%
14.	Sophos	94.1%
15.	PC Tools	92.8%
16.	AVG	91.4%
17.	Webroot	85.5%
18.	K7	84.4%



The used test-set contains about 400-thousands malware samples (not older than last 6 months) and consists of:



[4] We estimate the remaining error margin to be under 0.2%

False positive/alarm test

In order to better evaluate the quality of the detection capabilities (distinguish good files from malicious files) 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 should now have been already fixed.

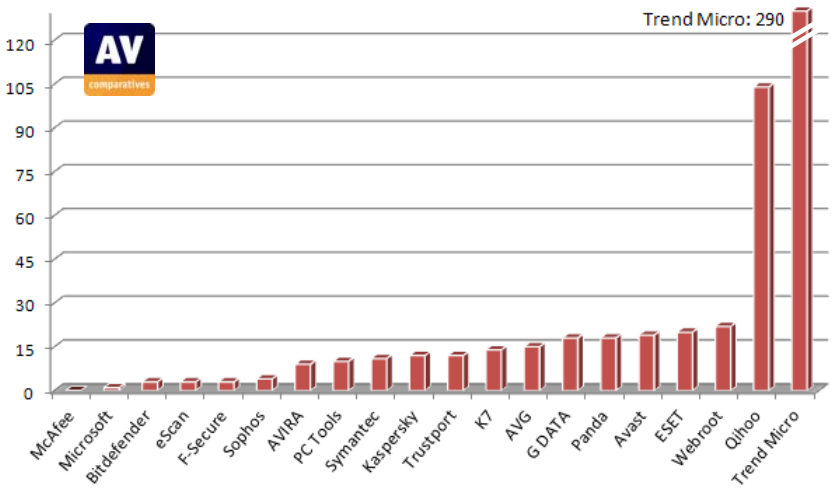
False Positive Results

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

1.	McAfee	0	
2.	Microsoft	1	very few FPs
3.	Bitdefender, eScan, F-Secure	3	
4.	Sophos	4	
5.	AVIRA	9	
6.	PC Tools	10	few FP's
7.	Symantec	11	
8.	Kaspersky, Trustport	12	
9.	K7	14	
10.	AVG	15	
11.	G DATA, Panda	18	
12.	Avast	19	many FP's
13.	ESET	20	
14.	Webroot	22	
15.	Qihoo	104	very many FP's
16.	Trend Micro	290	

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_fp_feb2011.pdf

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

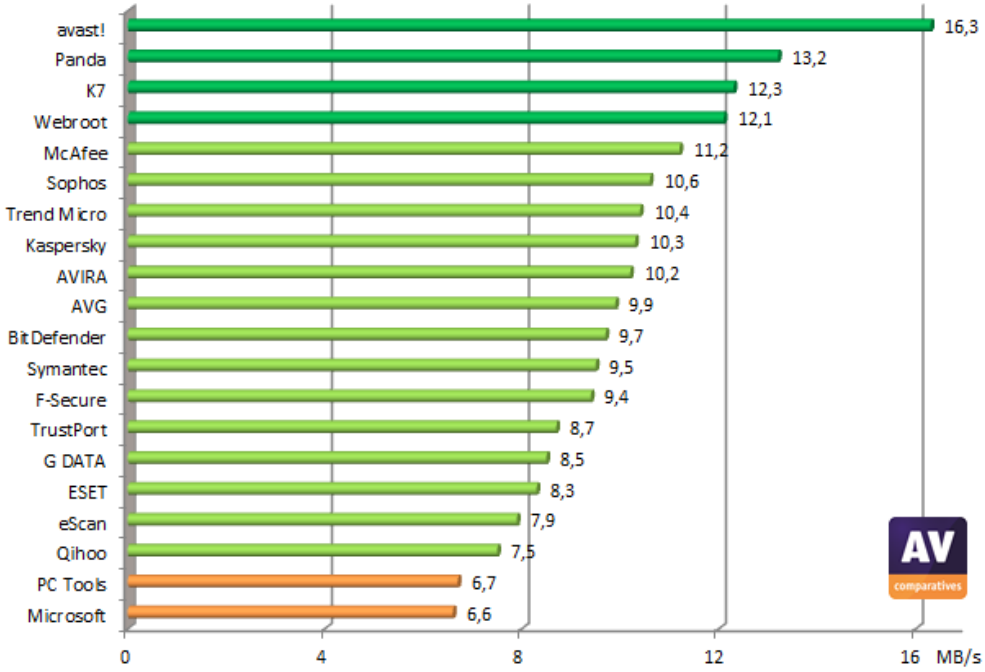


Scanning Speed Test

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 querying cloud data, 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 fingerprinting technologies are disabled and 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. In 2012 we will probably no longer provide the on-demand scanning speed test inside the on-demand detection report.

[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, expert 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
	✓ Trustport ✓ F-Secure ✓ Bitdefender ✓ AVIRA ✓ eScan ✓ Kaspersky ✓ McAfee
	✓ G DATA* ✓ Avast* ✓ Panda* ✓ ESET* ✓ Microsoft ✓ Symantec ✓ Sophos
	✓ Qihoo* ✓ Trend Micro* ✓ PC Tools ✓ AVG
	✓ Webroot* ✓ K7

*: 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. On page 7 of this report you can see how awards are being given.

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.

Copyright and Disclaimer

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

AV-Comparatives e.V. (April 2011)