Anti-Virus Comparative

Summary Report 2007

Results, winners, comments

Date: December 2007

Last revision: 18th December 2007

Author: Andreas Clementi

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

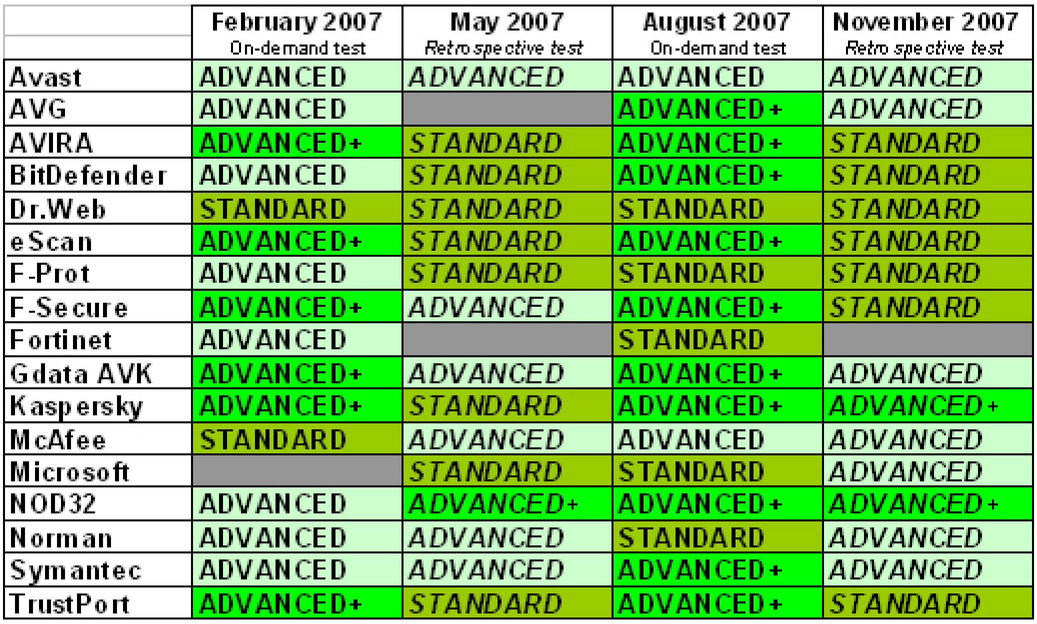
1. Introduction

At the end of every year, AV-Comparatives releases a summary report to comment on the various Antivirus products tested over the year, and to determine who are the „winners“ in the various tests. Please bear in mind that this report considers the results reached during all the various tests of 2007 and not only the latest ones. Comments and conclusions are based on the results contained in the various test reports of AV-Comparatives. You can find them on www.av-comparatives.org/seiten/comparatives.html.

2. Overview of levels reached during 2007

Only high-quality anti-virus products with good detection rates can participate in the regular main test-series of AV-Comparatives. It is important that readers understand that the STANDARD level/award is already a good score, as to achieve it requires the ability to detect a minimum percentage of malware. Many products that are not listed on AV-Comparatives would not reach the minimum requirements to participate[1]; therefore the ones that are included in the tests of AV-Comparatives can be considered to be a selection of very good and high-quality Antivirus products.

Below the overview of levels/awards reached by the various Antivirus products in the main tests of AV-Comparatives during 2007.



	February 2007 On-demand test	May 2007 *Retrospective test*	August 2007 On-demand test	November 2007 *Retrospective test*
Avast	ADVANCED	*ADVANCED*	ADVANCED	*ADVANCED*
AVG	ADVANCED	▨	ADVANCED+	*ADVANCED*
AVIRA	ADVANCED+	*STANDARD*	ADVANCED+	*STANDARD*
BitDefender	ADVANCED	*STANDARD*	ADVANCED+	*STANDARD*
Dr.Web	STANDARD	*STANDARD*	STANDARD	*STANDARD*
eScan	ADVANCED+	*STANDARD*	ADVANCED+	*STANDARD*
F-Prot	ADVANCED	*STANDARD*	STANDARD	*STANDARD*
F-Secure	ADVANCED+	*ADVANCED*	ADVANCED+	*STANDARD*
Fortinet	ADVANCED	▨	STANDARD	▨
Gdata AVK	ADVANCED+	*ADVANCED*	ADVANCED+	*ADVANCED*
Kaspersky	ADVANCED+	*STANDARD*	ADVANCED+	*ADVANCED+*
McAfee	STANDARD	*ADVANCED*	ADVANCED	*ADVANCED*
Microsoft	▨	*STANDARD*	STANDARD	*ADVANCED*
NOD32	ADVANCED	*ADVANCED+*	ADVANCED+	*ADVANCED+*
Norman	ADVANCED	*ADVANCED*	STANDARD	*ADVANCED*
Symantec	ADVANCED	*ADVANCED*	ADVANCED+	*ADVANCED*
TrustPort	ADVANCED+	*STANDARD*	ADVANCED+	*STANDARD*

Note: ‘grey’ means ‘certification level not reached’.

3. “Winners”

If you plan to buy an Anti-Virus, please visit the vendor's site and evaluate their software by downloading a trial version, as there are also many other additional features (e.g. firewall, behavior blocker, spamfilter, etc.) and important considerations (e.g. compatibility, graphical user interface, system impact, easy of use, price, etc.) for an Anti-Virus that you should evaluate by yourself. As explained above, a perfect Antivirus or the „best“ Antivirus for all needs and for every user does not exist. Our „winners“ label takes in to consideration only the objective test data and does not evaluate or consider other factors that may be of importance for specific users’ needs or preferences.

[1] http://www.av-comparatives.org/seiten/avlist.html

a) Overall winner(s) of 2007 based on the reached levels and subtest results:

To be rated „best Anti-Virus product of 2007“ by AV-Comparatives, an Anti-Virus product should have high detection rates; including detection of difficult polymorphic viruses; high proactive detection rates, very few false positives (zero is preferable), be fast with a low system impact, cause no crashes or hangs, and have no annoying bugs. The following products received at least 3 ADVANCED+ awards during 2007: Kaspersky and ESET NOD32. The following products reached high scores by counting the various award levels of 2007: ESET NOD32 (11), Kaspersky (10), GDATA AVK (10), Symantec (9), F-Secure (9). GDATA AVK and F-Secure are multi-engine products. The negative side of multi-engine products is their higher impact on the scanning speed and system performance, and the potential for multiplied false alarm occurence.

The overall Anti-Virus product winner of 2007 is again: **ESET NOD32**.

b) On-Demand detection winner(s):

The following products received the ADVANCED+ award in both overall on-demand detection tests of February and August 2007: AVIRA, eScan, F-Secure, GDATA AVK, Kaspersky and TrustPort. The following products achieved results of about 99% in both tests: AVIRA, GDATA AVK, TrustPort. Therefore, the On-Demand detection winners are:

Single-engine: **AVIRA**

Multi-engine: **GDATA AVK**, **TrustPort**

c) Proactive On-Demand detection winner(s):

The retrospective tests show how good the on-demand proactive detection of the various Antivirus products is (how good they are at detecting on-demand new/unknown malware). A high (proactive) on-demand detection rate must be archivied together with a low rate of false alarms. The following products received the ADVANCED+ award in both retrospective tests of May and November 2007: ESET NOD32.

Therefore, the Proactive On-Demand detection winner is: **ESET NOD32**.

d) False Positives winner(s):

False positives can cause as much troubles as a real infection. Due to this, it is important that Antivirus products have stringent Quality Assurance testing before release to public (in order to avoid false positives). The products with the lowest rate of false positives during 2007 were: Symantec (1), ESET NOD32 (2), eScan (2) and F-Secure (2). Therefore, the product with the lowest rate of false alarms is: **Symantec**.

e) On-Demand Scanning Speed test winner(s):

The products with the highest on-demand througput rate (green bars in both speed tests in May and November 2007)[2] with best possible detection settings were: AVIRA, ESET NOD32, Symantec and Fortinet. Therefore, the On-Demand Scanning Speed winners with best possible detection settings are: **Fortinet, Symantec, AVIRA, ESET NOD32**.

f) Polymorphic Virus detection test winner(s):

The following products were able to detect 100% of all polymorphic viruses included in the test-set in both tests: Symantec, ESET NOD32. The Kaspersky-based products (GDATA AVK, eScan, F-Secure, Kaspersky) were only able to detect all samples in the last polymorphic test. Therefore, the Polymorphic Virus detection winners are: **Symantec, ESET NOD32**.

[2] *See graphs in reports Nr. 14 and Nr. 16 listed on http://www.av-comparatives.org/seiten/comparatives.html*

Summary:

a) Overall / Best Antivirus of 2007: **ESET NOD32**
other candidates were: Kaspersky, Symantec, F-Secure, GDATA AVK

b) On-Demand detection (single engine): **AVIRA**
other candidates were: Kaspersky
On-Demand detection (multi engine): **GDATA AVK, TrustPort**
other candidates were: eScan, F-Secure

c) Proactive on-demand detection rate: **ESET NOD32**
other candidates were: Kaspersky

d) Lowest false positive rate: **Symantec**
other candidates were: ESET NOD32, eScan, F-Secure

e) On-demand scanning speed: **Fortinet, Symantec, AVIRA, ESET NOD32**
other candidates were: McAfee, F-Prot

f) Most reliable polymorphic virus detection: **Symantec, ESET NOD32**
other candidates were: Kaspersky, GDATA AVK, eScan, F-Secure

4. Comments

Below some comments about the various products included in the test-series of 2007, regarding their results, capabilities and future prospectives:

Avast (www.avast.com): During 2007 Avast earned four ADVANCED awards and continued to improve compared to previous tests. Avast is quite fast in adding malware they receive. The unpacking engine and generic detections of Avast are also improved. It can be expected that Avast will continue to improve their detection rates next year.

AVG (www.grisoft.com): In 2007 we tested AVG Anti-Malware, which includes the Ewido engine. As expected, AVG Anti-Malware scored higher than in previous tests, earning one ADVANCED+ award in August 2007. AVG is a resource-friendly and easy to use antivirus. The heuristics can probably be improved further.

AVIRA (www.avira.com): AVIRA has very high detection rates (the highest on-demand detection rate of any single-engine product), a high proactive detection rate and a fast on-demand scanning speed. The only big downside of AVIRA is still the relativly high amount of false alarms it produces (although this has improved a bit). If AVIRA is able to further drop down the false alarm rate (without decreasing the detection rates), it would probably be nominated Antivirus of the year. Because it is easier to get high scores with a more paranoid heuristic, it does not yet deserve this title.

BitDefender (www.bitdefender.com): BitDefender again showed that it has a decent heuristic and a good overall on-demand detection rate, but unfortunatly it causes some false alarms. BitDefender also includes a behavior based heuristic (B-Have) and identity protection feature, which may show its full potential only when the malware is already executed. Tests of similar proactive detection technologies showed that they usually offer very high protection.

Dr.Web (www.drweb.com): Dr.Web is a very resource-friendly and easy to use antivirus which also works on older operating systems. Dr.Web is known for its heuristics (which recently has been further improved by the introduction of the origin detections), but unfortunately, these still cause too many false alarms. The relativly slow scanning speed due to the deep file scan in relation to the detection rate it provides is also problematic. The product crashed during our testing, but this (as well as the false alarms) was quickly fixed after being reported. Compared to other vendors, Dr.Web seems to be quite slow in adding the malware they missed in previous tests. The lower detection rates may be balanced by a higher successful cleaning rate for some malware (according to other tests[3]). However, perhaps things will change when version 5 of Dr.Web is released.

eScan (www.mwti.com): eScan is a multi-engine product (using the KAV engine), but in our tests it achieved scores very similar to KAV v6 (not KAV v7, which uses new heuristics). eScan did not have very good results in the retrospective tests, but provides high detection rates in the normal on-demand tests with up-to-date signatures.

ESET NOD32 (www.eset.com): Due to its high proactive on-demand detection rate and very low false positives, ESET NOD32 Antivirus has always reached the highest awards (ADVANCED+) in retrospective testing. It also scored well also in the overall on-demand detection tests, but there is room for improvement - more missed malware should be added and faster.
It has fast scanning speed and low system impact. In summary, ESET NOD32 Antivirus earned the status of overall winner of our tests for 2007.

F-Prot (www.f-prot.com): In 2007 we tested the new version of F-Prot. F-Prot is a resource-friendly, fast and relatively cheap antivirus with good heuristics (but it also still causes too many false alarms). Recently F-Prot added another improved heuristic to its scanner (Eldorado), from which much higher detection rates can be expected in future tests.

F-Secure (www.f-secure.com): F-Secure uses a variety of engines in its product, one of them being the AVP engine (which uses the signatures of Kaspersky, but not its new heuristics). This gives F-Secure very high results in the overall on-demand detection tests. As with most multi-engine AV products, a side-effect can be observed in the lower on-demand scanning speed.
F-Secure 2007 did not achieve very good results in the retrospective tests, but F-Secure includes a proactive detection technology (DeepGuard) to protect against new/unknown malware (which works when the malware is already executed and not on-access/on-demand). Tests of similar proactive detection technologies showed that they usually offer very strong protection.

Fortinet (www.fortinet.com): Fortinet was tested for the first time in 2007. The scanner is very fast, but the detection rates were not very high. Fortinet is doing its best to improve their detection rates, quickly adding malware it missed. Fortinet also includes heuristics in its home user product, but due to the enormous amount

[3] *Links to other testers websites can be found at* http://www.av-comparatives.org/forum/index.php?page=Board&boardID=5

of false alarms this produces, users should not enable it. It would be preferable if Fortinet would remove that heuristic from the home user version (not from the mail server versions) and replace it with a better, more reliable heuristic which makes sense for home users. Without its heuristics, the proactive on-demand detection rates of Fortinet are very low. Fortinet will not be included in the tests of 2008.

GDATA (AVK) (www.gdata.de): AVK 2007 used two engines in its product: the Kaspersky (v6) engine and the Avast engine. Thanks to this DoubleScan technology AVK 2007 earned the ADVANCED+ award in the on-demand tests of February and August and the ADVANCED award in the retrospective tests. Due to the engine change from BitDefender to Avast the proactive on-demand detection rate dropped a bit, but with the Avast engine it is a little bit faster (although still slow overall) and does not consume as many resources as in the past.

Kaspersky (www.kaspersky.com): Kaspersky earned 3 ADVANCED+ awards and 1 STANDARD award in May 2007 (with version 6), showing to have very high on-demand detection rates and also very good heuristics (with a low false alarm rate) since the release of version 7. It is probable that Kaspersky will be a candidate for the nomination of best antivirus next year, if it continues to show high results with its new engine. Kaspersky also has a behaviour blocker in its products (PDM) which will protect against malware during its execution. Tests of this proactive detection technology showed that it offers a very high protection (and can undo system changes caused by the malware).

McAfee (www.mcafee.com): In 2007, McAfee reached the STANDARD/ADVANCED award in the on-demand tests (improved due to the new 5200 engine). The detection rates in the retrospective test also improved (ADVANCED) with the new engine, but the false alarm rate was higher than in previous tests. The price for the McAfee product (which includes an Anti-Spyware, a Firewall and some kind of HIPS) is very competitive.

Microsoft (onecare.live.com): Microsoft entered the AV Market in 2006, showing rather poor results in its first test in February 2007. But since then, it has continuosly improved (from no award to STANDARD award in the on-demand tests and from STANDARD award to ADVANCED award in the retrospective tests). OneCare is an easy to use suite for home users and has a low false alarm rate. Microsoft is currently fast improving its detection rates, quickly adding detection for the samples they missed. If Microsoft continues this way, it will be soon on par with the big players in the next higher award.

Norman (www.norman.com): Through 2007 Norman continued to improve by enhancing its sandbox technology and adding faster detection for the malware it misses. In the on-demand retrospective tests of AV-Comparatives Norman reached the ADVANCED awards. Norman has a sandbox technology which may show its full potential only while the malware is executed. Tests of similar proactive detection technologies showed that they usually offer high protection.

Symantec (www.symantec.com): Symantec (NAV) also continued to improve during 2007, showing high on-demand detection rates and producing only very few false alarms (which got fixed quickly). The latest product versions of Symantec are no longer as resource-hungry as they were in past (but may still noticeably slow down some sytems, depending on the system configuration). The scanning speed is fast and Symantec provides a reliable detection of polymorphic viruses. The proactive on-demand detection rate is OK, but it could be higher. Symantec also includes in its products some kind of behavior blocker (SONAR) and proactive protection systems, which will block malicious software during the execution of malware (or e.g. drive-by downloads). Tests of similar proactive detection technologies showed that they offer usually very high protection. According to other tests, Symantec malware removal rate is relativly good.

TrustPort (www.aec.cz): TrustPort combines four antivirus engines in its product: AVG, BitDefender, Ewido and Norman. Soon they will also include Dr.Web and VBA32. Thanks to all those engines, TrustPort had very high overall on-demand detection rates and high results in the retrospective tests, but side-effect of using all those engines to reach such high scores is the slow on-demand scanning speed, the high system resource impact and an increased false alarm rate. With TrustPort it is possible to choose which engines to use (for on-demand and/or on-access scans), so it is of interest to users that want to use more than one antivirus engine on their PC (or using e.g. the AVG engine on-access and the BitDefender engine on-demand, etc.).

5. Copyright and Disclaimer

This publication is Copyright (c) 2007 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of AV-Comparatitves, prior to any publication. AV-Comparatives 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. 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.

Andreas Clementi, AV-Comparatives (December 2007)