Anti-Virus Comparative

Summary Report 2009

Awards, winners, comments

Language: English
December 2009
Last Revision: 24th December 2009

www.av-comparatives.org

Table of Contents

Introduction

At the end of every year, AV-Comparatives releases a summary report to comment on the various Anti-Virus products tested over the year, and to determine the winners in the various tests. Please bear in mind that this report includes **all** of the results achieved during the various comparative tests of 2009 (without corporate review), i.e. **not** only the latest ones. Comments and conclusions are based on the results contained in the various comparative test reports of AV-Comparatives (http://www.av-comparatives.org/comparativesreviews).

Overview of levels reached during 2009

Only high-quality Anti-Virus products with good detection rates can participate in the regular AV-Comparatives tests. It is important that readers understand that the STANDARD level/award is already a good score, since it requires the ability to detect a minimum percentage of malware. Many programs that are not listed on AV-Comparatives would not reach the minimum requirements to participate; therefore the ones that are included in our tests can be considered to be a selection of very good and high-quality Anti-Virus products.

Below is an overview of levels/awards reached by the various Anti-Virus products in the main tests[1] of AV-Comparatives during 2009.

	On-Demand Test February 2009	**Retrospective Test** February 2009	**On-Demand Test** August 2009	**Retrospective Test** August 2009	**RemovalTest** September 2009	**PUP-Test** November 2009	**Dynamic Test** December 2009	**Performance Test** December 2009
avast!	ADV	STD	ADV+	ADV+	ADV	ADV	ADV	ADV+
AVG	STD	STD	ADV	ADV	ADV	ADV	STD	ADV
AVIRA	ADV	ADV	ADV	ADV	ADV	ADV+	ADV	ADV+
BitDefender	ADV	ADV	ADV+	ADV+	ADV+	ADV+	ADV	ADV
eScan	ADV	ADV	ADV+	ADV+	ADV+	ADV+	STD	STD
ESET NOD32	ADV+	ADV+	ADV+	ADV+	ADV	ADV	ADV	ADV+
F-Secure	ADV	STD	ADV+	ADV+	ADV+	ADV+	ADV	ADV+
G DATA	ADV	ADV	ADV+	ADV+	STD	ADV+	ADV	ADV
Kaspersky	ADV+	ADV+	ADV	ADV+	ADV+	ADV	ADV+	ADV+
Kingsoft				STD		STD		ADV+
McAfee	ADV+	ADV	ADV	STD	ADV	ADV+	STD	ADV+
Microsoft	STD	ADV+	STD	ADV+	ADV+	ADV	ADV	ADV+
Norman				STD	STD	STD		ADV
Sophos	STD	ADV		STD	ADV	ADV	N/A	ADV+
Symantec	ADV+	ADV	ADV+	ADV	ADV+	ADV+	ADV+	ADV+
TrustPort	ADV	STD	ADV	STD	ADV	ADV+	STD	STD

[1] The various test report can be downloaded here:
http://www.av-comparatives.org/comparativesreviews/main-tests
http://www.av-comparatives.org/comparativesreviews/performance-tests
http://www.av-comparatives.org/comparativesreviews/dynamic-tests
http://www.av-comparatives.org/comparativesreviews/removal-tests
http://www.av-comparatives.org/comparativesreviews/pua-tests

Winners

If you plan to buy an Anti-Virus program, please visit the vendor's website and evaluate their software by downloading a trial version, as there are also many features and important considerations (e.g. compatibility, graphical user interface, ease of use, price, etc.) that you should evaluate for yourself. As explained above, the perfect Anti-Virus program or the best one for all needs and for every user does not exist. Our winners' category is based purely on the objective test data and does not evaluate or consider other factors that may be of importance for specific users' needs or preferences. Being recognized as "Best Product of 2009" does not mean that a product is the "best" in all cases and for everyone, it only means that it performed in general better than the other products in various tests performed during 2009.

a) Overall winners of 2009 (Best Products of the Year):

To be rated "Best Anti-Virus Product of 2009" by AV-Comparatives, an Anti-Virus product should preferably have very high detection rates (of malware and also potentially unwanted applications), high proactive on-demand detection (or provide proactive protection), very few false positives (FP), scan fast and reliably with a low system impact, provide good malware removal capabilities, protect the system against malware/websites with malicious software without relying too much on user decisions/interactions, cause no crashes or hangs, and have no annoying bugs.

Based on the awards given by AV-Comparatives during 2009, several products got many high awards and are very close, so that we decided to award not only the Best Product of 2009 but also the second and third places (Silver and Bronze). Looking into the detail of the raw results, we decided to give the following awards:

GOLD Symantec (Best Product of 2009)

SILVER Kaspersky

BRONZE ESET

Bitdefender and F-Secure came on a very close 4th place. Symantec and Kaspersky were very close to each other too, but Symantec had higher overall detection rates than Kaspersky, was often slightly better where they tied and can be recommended also for novice users. Anyway, all three products given awards above are excellent, as they showed generally very good results in the tests performed during 2009.

Previous Products of the Year:

2009: Symantec

2008: AVIRA

2007: ESET

2006: ESET

2005: Kaspersky

2004: Kaspersky

b) On-Demand Malware Detection winners:

A high detection rate of malware – without causing too many false alarms - is still one of the most important, deterministic and reliable features of an Anti-Virus product.

The following products received the ADVANCED+ award in both overall On-Demand Detection tests, in February and August 2009: Symantec (~98.6%, 20 FP) and ESET (~97.4%, 25 FP). The next product with good scores in the on-demand malware detection tests (but reaching only once ADVANCED+ due false alarms) was McAfee (~98.9%, 54 FP).

GOLD Symantec

SILVER ESET

BRONZE McAfee

Avast, AVIRA, Bitdefender, eScan, G DATA and Trustport had high on-demand malware detection rates, but at the cost of higher false alarm rates. Due to that, they could not be given awards.

c) Proactive On-Demand Detection winners:

The retrospective tests show how good the on-demand proactive detection of the various Anti-Virus products with highest settings is (how good they are at detecting on-demand new/unknown malware). A high (proactive) on-demand detection rate must be achieved with a low rate of false alarms. The on-demand proactive detection capability is especially important for the products that do not have (yet) other protection technologies like in-the-cloud, behavior-blockers, etc.

The following products received the ADVANCED+ award in both retrospective tests, in May and November 2009: ESET NOD32 (~58%, 25 FP), Kaspersky (~56%, 22FP) and Microsoft (~58%, 7 FP).

GOLD Microsoft

SILVER ESET

BRONZE Kaspersky

AVIRA and G DATA had high proactive on-demand detection rates, but at the cost of higher false alarm rates. Due that, they could not be given awards.

d) False Positives winners:

False positives can cause as much trouble as a real infection. Due to this, it is important that Anti-Virus products have stringent quality assurance testing before release to the public (in order to avoid false positives).

The products with the lowest rate of false positives during 2009 were Microsoft (7), F-Secure (11) and Symantec (20).

GOLD Microsoft

SILVER F-Secure

BRONZE Symantec

e) On-Demand Scanning Speed winners:

It is recommended that users regularly perform a full scan of their entire systems, in order to check that all the files on their machines are still clean.

The products with the highest on-demand throughput rate with best possible detection settings were Avast (~16.4 MB/sec), Kingsoft (~19.2 MB/sec) and Symantec (~17.1 MB/sec).

GOLD Kingsoft

SILVER Symantec

BRONZE Avast

f) Overall Performance (Low-System-Impact) winners:

Anti-Virus products must remain turned on under all circumstances, while users are performing their usual computing tasks. Some products may have a higher impact than others on system performance while performing some tasks.

The following products demonstrated a lower impact on system performance than others:

GOLD AVIRA

SILVER Kingsoft

BRONZE F-Secure

g) On-Demand PUA (potentially unwanted applications) Detection winners:

The amount of adware, spyware and other fraudulent software circulating on the Internet has increased a great deal over the past few years. Such applications are not typical malware and their classification is sometimes not an easy task; they are usually described using the term "potentially unwanted applications" (PUA).

Many products proved to have good coverage (over 98%) of potentially unwanted applications; therefore, it was not possible to limit the award to only three products.

GOLD Trustport, G DATA

SILVER McAfee, AVIRA

BRONZE Symantec, F-Secure, Bitdefender and eScan

h) Malware Removal winners:

Anti-Virus products should not only be able to detect malware, they should also be able to remove (preferably completely) the malware they detect on already infected/compromised systems.

The following products demonstrated very good malware removal capabilities in our tests:

GOLD eScan

SILVER Symantec

BRONZE Microsoft

i) Whole-Product Dynamic Protection winners:

Security products such as Internet security suites include various different features to protect systems against malware. Such protection features can be taken into account in whole-product-dynamic tests, which are tests under real-world conditions. Symantec and Kaspersky were both contenders in this dynamic test, but we decided that the first place should go to Symantec, as it showed fewer warnings than Kaspersky, and informed the user of one threat more than Kaspersky.

The following products were able to provide good protection against malware attacks:

GOLD Symantec

SILVER Kaspersky

BRONZE AVIRA

Summary of the Annual Awards

On-Demand Malware Detection

- GOLD: Symantec
- SILVER: ESET
- BRONZE: McAfee

On-Demand PUA Detection

- GOLD: Trustport, G DATA
- SILVER: McAfee, AVIRA
- BRONZE: Symantec, F-Secure, Bitdefender, eScan

Proactive On-Demand Malware Detection

- GOLD: Microsoft
- SILVER: ESET
- BRONZE: Kaspersky

Low False Positive Rate

- GOLD: Microsoft
- SILVER: F-Secure
- BRONZE: Symantec

Overall Performance - Low System Impact

- GOLD: AVIRA
- SILVER: Kingsoft
- BRONZE: F-Secure

On-Demand Scanning Speed

- GOLD: Kingsoft
- SILVER: Symantec
- BRONZE: Avast

Malware Removal

- GOLD: eScan
- SILVER: Symantec
- BRONZE: Microsoft

Whole Product Dynamic Protection

- GOLD: Symantec
- SILVER: Kaspersky
- BRONZE: AVIRA

Best Products of 2009:

GOLD: Symantec

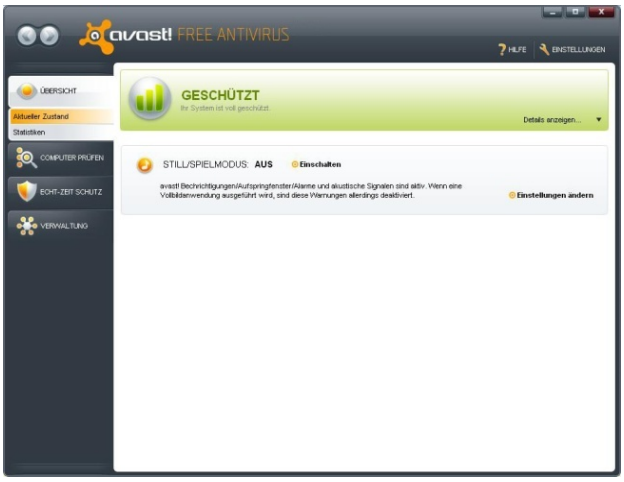
SILVER: Kaspersky

BRONZE: ESET

Comments

Below are some comments about the various products that were included in the test series of 2009.

Avast (www.avast.com): This year, avast! showed big improvements in its detection rates (esp. in the second half of 2009) and reduced its number of false alarms. Its on-demand scanning speed is one of the fastest. The recently released avast! v5 includes further enhancements (like a new graphical user interface) and new protection features. Avast also offers a free version of its product to home users.



+ high malware detection rates

+ fast on-demand scan speed

+ free version available

AVG (www.avg.com): AVG did not score as well as we expected this year, although it was still good. We hope to see it improving next year. All AVG products include AVG LinkScanner, which ensures that the user only surfs to safe websites. AVG also offers a free edition of AVG Antivirus for home users, providing basic security (i.e. without WebShield, advanced rootkit protection, etc.).

+ easy to use

+ free version available

+ LinkScanner

AVIRA (www.avira.com): AVIRA earned our Product of the Year award in 2008. It also showed very high detection rates and very high proactive detection rates this year, but at the price of a high false alarm rate. Due to the high detection rates of AVIRA and its WebShield, it also demonstrated good protection in our Whole-Product Dynamic test, even if AVIRA does not currently include some features such as a behaviour blocker. AVIRA has a low impact on system performance. A new version of AVIRA, including also a behaviour blocker, will be available in 2010.

+ very high detection rates

+ low system impact

+ free version available

BitDefender (www.bitdefender.com): BitDefender improved this year, and showed good detection rates and good heuristics, with fewer false alarms than in the past. BitDefender also demonstrated good malware removal capabilities.

+ high detection rates

+ good heuristics

+ good malware removal capabilities

eScan (www.mwti.com): eScan is a multi-engine product. eScan showed good detection rates and good heuristics, with fewer false alarms than in the past. eScan is very good at removing most malware completely, if it is able to detect it.

+ high detection rates

+ good heuristic

+ very good removal capabilities

A single product review of eScan Internet Security v10 can be found here:
http://www.av-comparatives.org/images/stories/test/single/escanreview09.pdf

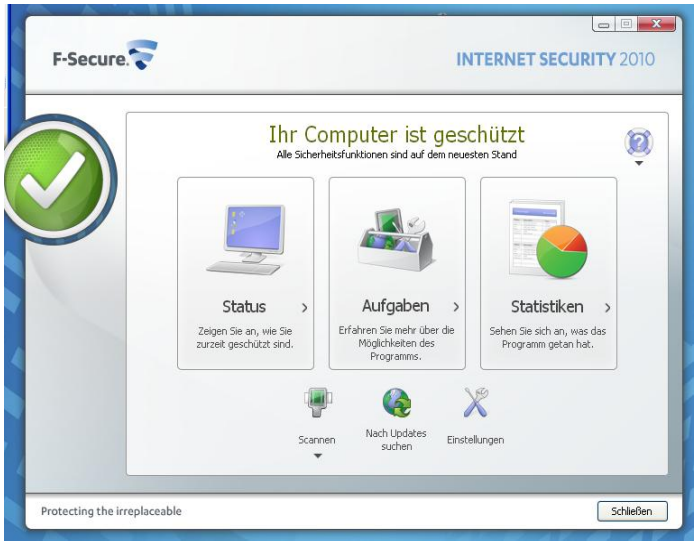
ESET (www.eset.com): Another year, another good showing by ESET. Its advanced heuristics led to high detection rates and relatively few false alarms and continuing to be quite light on system resources. Looking at the test results in general, ESET deserved a 3rd place as one of the best products of 2009.

+ high detection rates

+ very good heuristics

+ low system impact

F-Secure (www.f-secure.com): F-Secure uses a variety of engines in its product (including Bitdefender). F-Secure improved a lot with regard to its impact on system performance. Its malware removal capabilities are also quite good, as well as its low false alarm rate. The new 2010 version comes with a polished and easy-to-use graphical user interface.



+ high detection rates

+ good malware removal capabilities

+ easy-to-use program interface

GDATA (www.gdata.de): G DATA uses the Avast and BitDefender engines. Due to this combination, G DATA reaches very high detection rates, although this sometimes also means increased false alarms. In the August On-Demand Detection test this year, false positives were actually low. The impact on system performance improved a lot, due e.g. to the fingerprinting of already scanned files. The user interface is clearly structured.

+ very high detection rates

+ good engine combination

+ clear user interface

Kaspersky (www.kaspersky.com): Kaspersky shows very high proactive malware detection rates and good reactive malware detection rates (although it could be improved, as seen in the August on-demand detection test). Kaspersky also has good malware removal capabilities (also including Security+, which allows restoring settings modified by malware). The impact on system performance and resource usage is also low. Kaspersky includes many security features for advanced users, but also offers fully automatic protection mode for novice users. The user interface and logging feature could be improved further. Kaspersky was given a Silver award as being one of the best products of 2009.

+ very good heuristic

+ good detection rates

+ many protection features

Kingsoft (www.kingsoftresearch.com): Kingsoft was the first Chinese vendor to take the challenge of participating in an international Anti-Virus comparative, and has not used the poor excuse that Chinese antivirus programs mainly only detect Chinese malware. Kingsoft should be considered a reputable company just for this, as they know that there are no borders in the Internet, and Anti-Virus software should detect all malware, regardless of its origin. Kingsoft showed decent detection rates, but they were still too low and had too many false alarms to get a high award. Kingsoft is the fastest scanner according to our tests. The user interface is kept very simple and easy to use.

+ very fast scanner

+ low system impact

+ intuitive user interface

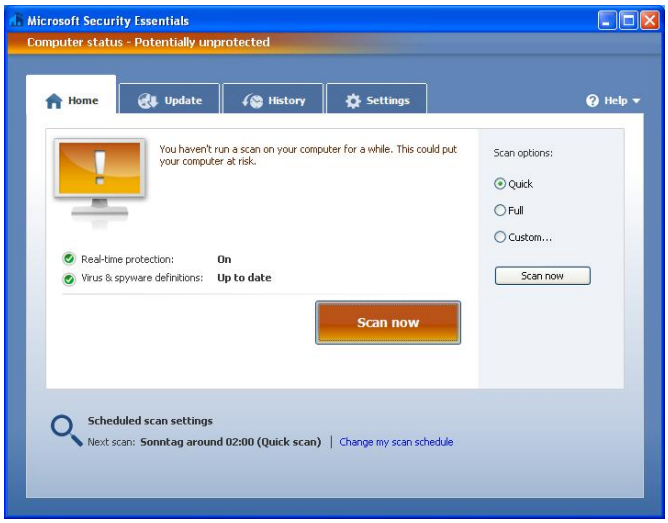
McAfee (www.mcafee.com): This year, McAfee had very high detection rates of malware and potentially unwanted applications, mainly due its powerful in-the-cloud technology. Unfortunately, it also generated many false alarms. In our opinion, McAfee needs some further important improvements, e.g. its graphical user interface, and heuristic detection while offline. We also noted the absence of a rescue disk, which for a worldwide brand like McAfee is in our opinion really a must-have feature. McAfee also includes SiteAdvisor, which warns about potentially dangerous websites.

+ very high malware detection rates

+ very high PUA detection rates

+ SiteAdvisor

Microsoft (www.microsoft.com/security_essentials): Microsoft proved to have very good proactive detection rates with a low false alarm rate, and very good malware removal capabilities. During 2009, Microsoft released Microsoft Security Essentials, which is a free Anti-Virus product with a very simple graphical user interface. Security Essentials is intended to be a simple Anti-Virus solution providing at least essential security for people who cannot afford, or do not want, to buy a full commercial security product.



+ very high proactive detection

+ low false alarm rate

+ very good removal capabilities

+ free

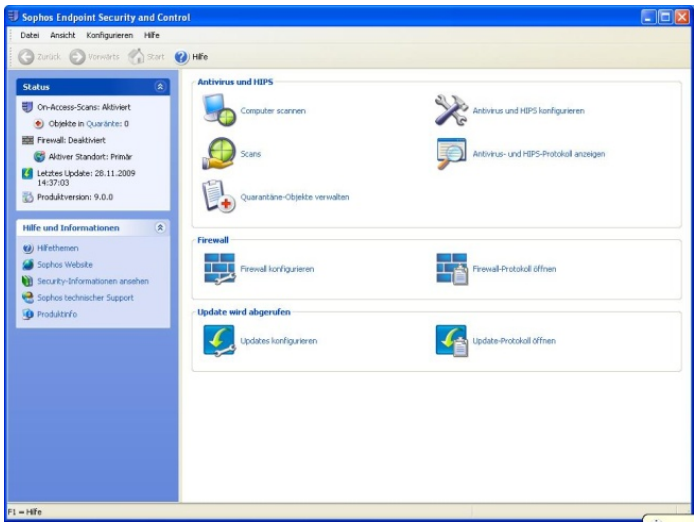
Norman (www.norman.com): This was not a good year for Norman according to our test results. Norman reached the STANDARD level in only four out of eight tests, while we were used to see Norman performing better in previous years. Anyway, Norman recently released a new version of its products, with a better graphical user interface and other enhancements. We expect to see Norman performing well again in future tests, as they now know where improvements are needed to stay competitive with other security products. Norman also supports older operating systems like Windows 95. Norman automatically performs a scan of the system while the user is away (when the screensaver is active).

+ clear user interface

+ supports older operating systems

+ screensaver mode scan

Sophos (www.sophos.com): Sophos is an enterprise-focused security company. In our tests, Sophos showed decent results and detection rates. Sophos also has a HIPS, which warns about potentially dangerous system modifications etc. – for administrators in an enterprise this can be useful. The graphical user interface is kept very simple and is very intuitive. Please read the results of Sophos in detail in the test reports; because our tests have strict rules geared towards home-user products, Sophos may sometimes score a bit lower in the awards, as we have to apply the same standards throughout, even if Sophos is an enterprise product.

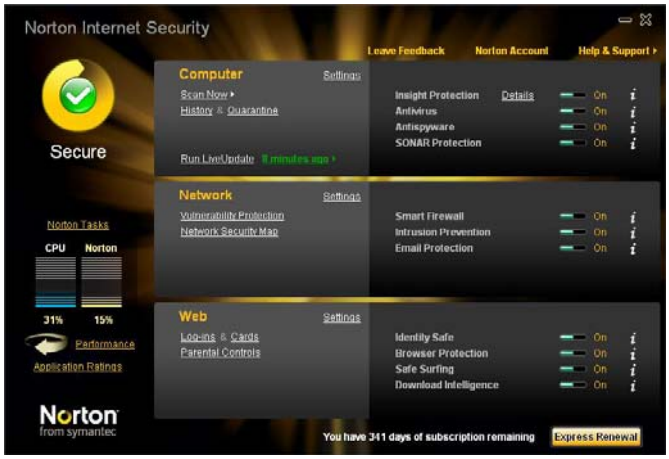


+ very easy to use user interface

+ for enterprises

+ HIPS

Symantec (www.symantec.com): Symantec (Norton) improved further with regard to its impact on system performance. While many years ago Norton was known to be a resource hog, it now has a very low system impact. The detection rates of malware and potentially unwanted applications are also very high, while still keeping a low false alarm rate. The graphical user interface is stylish and easy to use. The offline/local heuristics could be further improved. The product includes a behaviour analyzer and various other powerful protection features (e.g. in-the-cloud file reputation) which take the appropriate action without the need for user interaction, making it suitable for novice users too. Due the big improvements achieved by Symantec, and the various good scores it reached in most of our tests during 2009, Symantec was awarded Best Product of the Year 2009.



+ very high detection rates

+ low system impact

+ easy to use

TrustPort (www.trustport.com): TrustPort combines various Anti-Virus engines in its product, which can be selected by the user. By default, it now uses the AVG and Bitdefender engines. Thanks to the various engines it uses, TrustPort had very high on-demand detection rates and high results in the retrospective tests, but it still has a relatively slow on-demand scanning speed, and many false alarms compared to other products.

+ very high malware detection rates

+ very high detection of potentially unwanted applications

+ various engines can be chosen

Copyright and Disclaimer

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

AV-Comparatives e.V. (December 2009)