Anti-Virus Comparative

# On-demand Detection of Malicious Software

includes false alarm and on-demand scanning speed test

Language: English
August 2010
Last Revision: 5th October 2010

**www.av-comparatives.org**

# Table of Contents

Tested Products 3

Conditions for participation and test methodology 4

Tested product versions 4

Comments 5

Test results 6

Graph of missed samples 8

Summary results 9

False positive/alarm test 10

Scanning speed test 11

Award levels reached in this test 12

Copyright and Disclaimer 13

# Tested Products

- avast! Free Antivirus 5.0
- AVG Anti-Virus 9.0
- AVIRA AntiVir Premium 10.0
- BitDefender Antivirus Pro 2011
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 4.2
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2011
- K7 TotalSecurity 10.0
- Kaspersky Anti-Virus 2011
- Kingsoft AntiVirus 2010
- McAfee AntiVirus Plus 2010
- Microsoft Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 8.0
- Panda Antivirus Pro 2011
- PC Tools Spyware Doctor with AV 8.0
- Sophos Anti-Virus 9.5
- Symantec Norton Anti-Virus 2011
- 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 6th August 2010. The system sets and the products were updated and frozen on the 16th August 2010. The following 20 up-to-date products were included in this public test:

- avast! Free[1] Antivirus 5.0.594
- AVG Anti-Virus 9.0.851
- AVIRA AntiVir Premium 10.0.0.603
- BitDefender Anti-Virus Pro 14.0.23.312
- eScan Anti-Virus 10.0.1058.677
- ESET NOD32 Antivirus 4.2.58.3
- F-Secure Anti-Virus 10.50.197
- G DATA[2] AntiVirus 21.0.3.1
- K7 TotalSecurity 10.0.0040
- Kaspersky Anti-Virus 11.0.1.400 (a)
- Kingsoft AntiVirus Pro 2010.07.27.193
- McAfee AntiVirus Plus 14.5.113
- Microsoft Security Essentials 1.0.1963.0
- Norman Antivirus & Anti-Spyware 8.00
- Panda Antivirus Pro 10.00.00
- PC Tools Spyware Doctor with Antivirus 8.0.0.594
- Sophos Anti-Virus 9.5.1
- Symantec Norton Anti-Virus 18.1.0.30
- Trend Micro AntiVirus plus AntiSpyware 2010
- Trustport[3] Antivirus 5.0.0.4134

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] Avast wanted to participate in the tests with their free product version.
[2] G DATA uses two third-party engines.
[3] 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.

**F-Secure, Kaspersky, Kingsoft, McAfee, Panda, Sophos, Symantec** and **Trend Micro** make use of cloud technologies, which require an active internet connection. Due the increasing number of cloud-supported products, we do not longer test the baseline detection rates and show instead only the results with active cloud. Please note that detection rates may in some few cases be much lower if the scan is performed while offline, although most vendors see the need not to put everything in the cloud and correctly consider the cloud 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.

We used also for this test metadata/cloud/telemetry data collected and shared within the AV industry in order to include current (2010) and prevalent samples in the test-set. This is why the size of the test-set is getting smaller and the products are reaching more easily higher detection rates. Due that, as announced already in the previous reports, we increased the thresholds for the awards to reflect this change. Currently we are also thinking to use in future clustered groups instead of fixed percentages for the awards.

The number of sources for the prevalence data increased among the industry, but we observed that the quality of some cloud/metadata is not very reliable, as some clouds seem to be poisoned with lot of clean files (and reported as prevalent malware) which have been removed afterwards from the sets. We will investigate those cases and provide feedback to the sources of this "poisoned" cloud data.

# Test Results

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

| *Company*<br>*Product*<br>*Program version* | | AVIRA<br>**AntiVir Premium**<br>10.0.0.603 | | Avast Software<br>**avast! Free Antivirus**<br>5.0.594 | | AVG Technologies<br>**AVG Anti-Virus**<br>9.0.851 | | BitDefender<br>**BitDefender AV Pro**<br>14.0.23.312 | |
|---|---|---|---|---|---|---|---|---|---|
| **Award reached in this test** | | ADVANCED+ | | ADVANCED+ | | ADVANCED | | ADVANCED+ | |
| **Number of false positives**<br>On-demand scanning speed | | **few**<br>fast | | **few**<br>fast | | **many**<br>average | | **few**<br>average | |
| Windows viruses | 21.368 | 21.247 | 99,4% | 21.348 | 99,9% | 20.954 | 98,1% | 21.336 | 99,9% |
| Macro viruses | 2.714 | 2.714 | 100,0% | 2.706 | 99,7% | 2.682 | 98,8% | 2.649 | 97,6% |
| Scripts | 3.566 | 3.511 | 98,5% | 3.547 | 99,5% | 2.606 | 73,1% | 3.335 | 93,5% |
| Worms | 123.240 | 123.169 | 99,9% | 123.129 | 99,9% | 122.352 | 99,3% | 122.989 | 99,8% |
| Backdoors/Bots | 124.246 | 124.084 | 99,9% | 123.298 | 99,2% | 122.557 | 98,6% | 123.564 | 99,5% |
| Trojans | 626.105 | 624.946 | 99,8% | 621.141 | 99,2% | 616.008 | 98,4% | 621.235 | 99,2% |
| other malware | 16.053 | 15.412 | 96,0% | 15.734 | 98,0% | 14.444 | 90,0% | 15.768 | 98,2% |
| **TOTAL** | **917.292** | 915.083 | **99,8%** | 910.903 | **99,3%** | 901.603 | **98,3%** | 910.876 | **99,3%** |

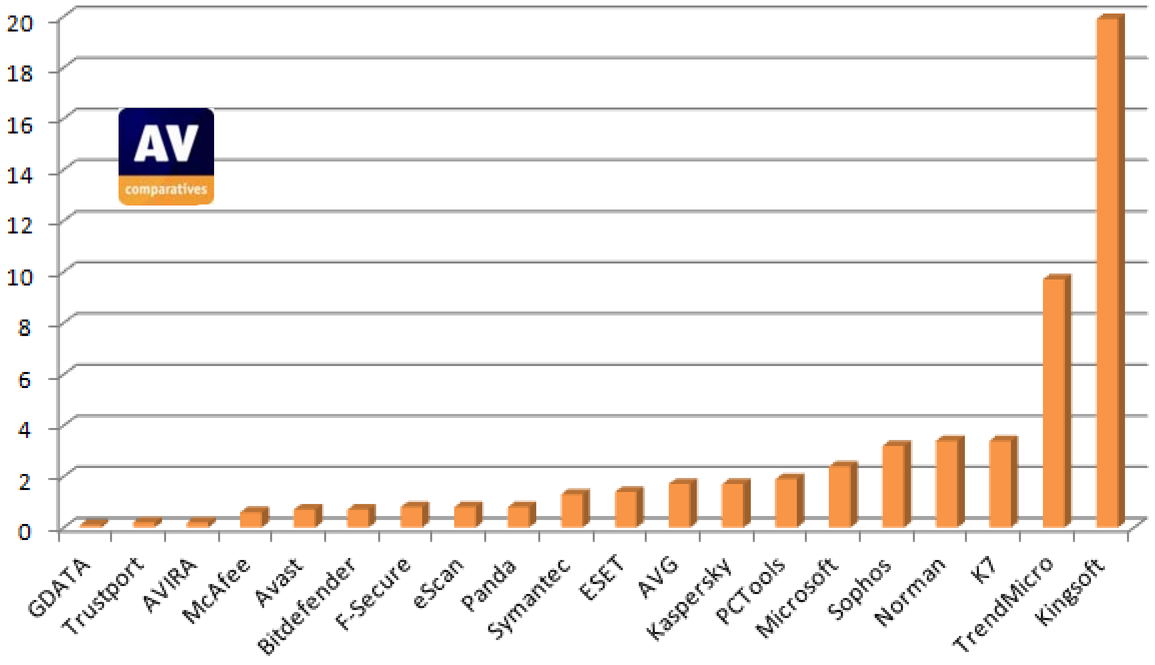
| *Company*<br>*Product*<br>*Program version* | | MicroWorld<br>**eScan Anti-Virus**<br>10.0.1058.677 | | F-Secure<br>**F-Secure Anti-Virus**<br>10.50.197 | | G DATA Security<br>**G DATA AntiVirus**<br>21.0.3.1 | | K7 Computing<br>**K7 TotalSecurity**<br>10.0.0040 | |
|---|---|---|---|---|---|---|---|---|---|
| **Award reached in this test** | | ADVANCED+ | | ADVANCED+ | | ADVANCED+ | | STANDARD | |
| **Number of false positives**<br>On-demand scanning speed | | **few**<br>average | | **very few**<br>average | | **few**<br>average | | **many**<br>average | |
| Windows viruses | 21.368 | 21.335 | 99,8% | 21.335 | 99,8% | 21.367 | 100,0% | 20.515 | 96,0% |
| Macro viruses | 2.714 | 2.649 | 97,6% | 2.649 | 97,6% | 2.714 | 100,0% | 2.699 | 99,4% |
| Scripts | 3.566 | 3.335 | 93,5% | 3.341 | 93,7% | 3.562 | 99,9% | 1.485 | 41,6% |
| Worms | 123.240 | 122.959 | 99,8% | 122.965 | 99,8% | 123.215 | 100,0% | 121.784 | 98,8% |
| Backdoors/Bots | 124.246 | 123.467 | 99,4% | 123.482 | 99,4% | 124.097 | 99,9% | 121.564 | 97,8% |
| Trojans | 626.105 | 620.717 | 99,1% | 620.812 | 99,2% | 625.444 | 99,9% | 606.588 | 96,9% |
| other malware | 16.053 | 15.746 | 98,1% | 15.780 | 98,3% | 16.000 | 99,7% | 11.039 | 68,8% |
| **TOTAL** | **917.292** | 910.208 | **99,2%** | 910.364 | **99,2%** | 916.399 | **99,9%** | 885.674 | **96,6%** |

| *Company*<br>*Product*<br>*Program version* | | Kaspersky Labs<br>**Kaspersky AV**<br>11.0.1.400 (a) | | Kingsoft<br>**Kingsoft AV Pro**<br>2010.07.27.193 | | McAfee<br>**McAfee AntiVirus +**<br>14.5.113 | | ESET<br>**NOD32 Antivirus**<br>4.2.58.3 | |
|---|---|---|---|---|---|---|---|---|---|
| **Award reached in this test** | | ADVANCED | | TESTED | | ADVANCED | | ADVANCED+ | |
| **Number of false positives**<br>On-demand scanning speed | | **many**<br>average | | **many**<br>average | | **many**<br>average | | **few**<br>average | |
| Windows viruses | 21.368 | 21.106 | 98,8% | 17.138 | 80,2% | 21.341 | 99,9% | 21.243 | 99,4% |
| Macro viruses | 2.714 | 2.714 | 100,0% | 2.346 | 86,4% | 2.714 | 100,0% | 2.701 | 99,5% |
| Scripts | 3.566 | 3.334 | 93,5% | 1.258 | 35,3% | 2.686 | 75,3% | 3.266 | 91,6% |
| Worms | 123.240 | 122.667 | 99,5% | 88.342 | 71,7% | 122.975 | 99,8% | 122.879 | 99,7% |
| Backdoors/Bots | 124.246 | 122.529 | 98,6% | 89.231 | 71,8% | 123.984 | 99,8% | 122.700 | 98,8% |
| Trojans | 626.105 | 613.398 | 98,0% | 529.551 | 84,6% | 624.268 | 99,7% | 616.397 | 98,4% |
| other malware | 16.053 | 15.838 | 98,7% | 7.117 | 44,3% | 14.179 | 88,3% | 15.050 | 93,8% |
| **TOTAL** | **917.292** | 901.586 | **98,3%** | 734.983 | **80,1%** | 912.147 | **99,4%** | 904.236 | **98,6%** |

| *Company*<br>*Product*<br>*Program version* | | Norman ASA<br>**Norman AV+AS**<br>8.00 | | Symantec<br>**Norton Anti-Virus**<br>18.1.0.30 | | Panda Security<br>**Panda Antivirus Pro**<br>10.00.00 | | Microsoft<br>**Security Essentials**<br>1.0.1963.0 | |
|---|---|---|---|---|---|---|---|---|---|
| **Award reached in this test** | | STANDARD | | ADVANCED+ | | ADVANCED | | ADVANCED | |
| **Number of false positives**<br>On-demand scanning speed | | **many**<br>slow | | **few**<br>average | | **many**<br>fast | | **very few**<br>slow | |
| Windows viruses | 21.368 | 21.003 | 98,3% | 20.978 | 98,2% | 21.331 | 99,8% | 20.990 | 98,2% |
| Macro viruses | 2.714 | 2.696 | 99,3% | 2.709 | 99,8% | 2.428 | 89,5% | 2.707 | 99,7% |
| Scripts | 3.566 | 2.715 | 76,1% | 3.438 | 96,4% | 1.966 | 55,1% | 3.142 | 88,1% |
| Worms | 123.240 | 120.965 | 98,2% | 122.420 | 99,3% | 122.964 | 99,8% | 122.567 | 99,5% |
| Backdoors/Bots | 124.246 | 120.238 | 96,8% | 121.905 | 98,1% | 124.180 | 99,9% | 121.740 | 98,0% |
| Trojans | 626.105 | 605.309 | 96,7% | 618.413 | 98,8% | 625.487 | 99,9% | 609.359 | 97,3% |
| other malware | 16.053 | 13.609 | 84,8% | 15.687 | 97,7% | 11.442 | 71,3% | 14.698 | 91,6% |
| **TOTAL** | **917.292** | 886.535 | **96,6%** | 905.550 | **98,7%** | 909.798 | **99,2%** | 895.203 | **97,6%** |

| *Company*<br>*Product*<br>*Program version* | | Sophos<br>**Sophos Anti-Virus**<br>9.5.1 | | PC Tools<br>**SpywareDoctor+AV**<br>8.0.0.594 | | Trend Micro<br>**Trend Micro AV+AS**<br>2010 | | Trustport<br>**TrustPort AV**<br>5.0.0.4134 | |
|---|---|---|---|---|---|---|---|---|---|
| **Award reached in this test** | | ADVANCED | | ADVANCED+ | | TESTED | | ADVANCED | |
| **Number of false positives**<br>On-demand scanning speed | | **few**<br>average | | **few**<br>average | | **many**<br>average | | **many**<br>average | |
| Windows viruses | 21.368 | 21.161 | 99,0% | 20.966 | 98,1% | 20.182 | 94,4% | 21.352 | 99,9% |
| Macro viruses | 2.714 | 2.700 | 99,5% | 2.709 | 99,8% | 2.701 | 99,5% | 2.713 | 100,0% |
| Scripts | 3.566 | 2.609 | 73,2% | 3.437 | 96,4% | 3.032 | 85,0% | 3.376 | 94,7% |
| Worms | 123.240 | 119.610 | 97,1% | 122.012 | 99,0% | 121.712 | 98,8% | 123.158 | 99,9% |
| Backdoors/Bots | 124.246 | 119.610 | 96,3% | 121.745 | 98,0% | 120.282 | 96,8% | 124.086 | 99,9% |
| Trojans | 626.105 | 607.038 | 97,0% | 613.616 | 98,0% | 546.475 | 87,3% | 624.882 | 99,8% |
| other malware | 16.053 | 14.788 | 92,1% | 15.665 | 97,6% | 13.937 | 86,8% | 15.958 | 99,4% |
| **TOTAL** | **917.292** | 887.516 | **96,8%** | 900.150 | **98,1%** | 828.321 | **90,3%** | 915.525 | **99,8%** |

## 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. For example missing 0.1% means missing almost one thousand malicious files.

*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

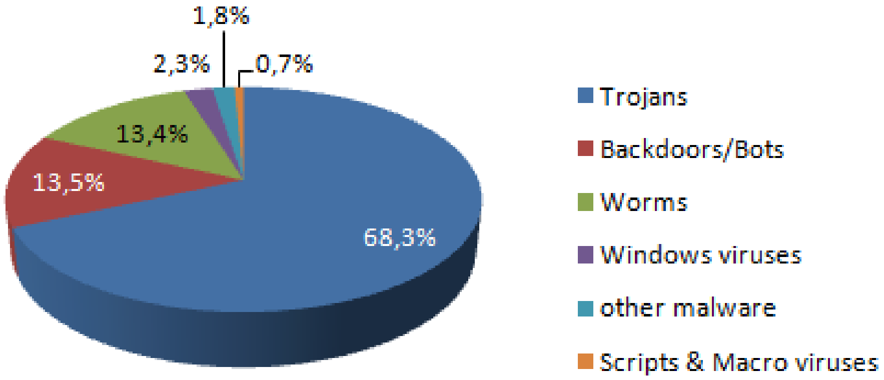
Please consider also the false alarm rates when looking at the below detection rates[4]!

Results may look higher in this test than in previous tests due the use of more prevalent malware. This is why also the test-set size decreased and the products are reaching more easily higher detection rates. We increased the thresholds for the awards to reflect this change.

**Total detection rates:**

| | | |
|---|---|---|
| 1. | G DATA | 99.9% |
| 2. | Trustport, AVIRA | 99.8% |
| 3. | McAfee | 99.4% |
| 4. | Avast, Bitdefender | 99.3% |
| 5. | F-Secure, eScan, Panda | 99.2% |
| 6. | Symantec | 98.7% |
| 7. | ESET | 98.6% |
| 8. | AVG, Kaspersky | 98.3% |
| 9. | PC Tools | 98.1% |
| 10. | Microsoft | 97.6% |
| 11. | Sophos | 96.8% |
| 12. | Norman, K7 | 96.6% |
| 13. | Trend Micro | 90.3% |
| 14. | Kingsoft | 80.1% |

The used test-set contains about 0.9 million malware samples and consists of:



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

# 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.

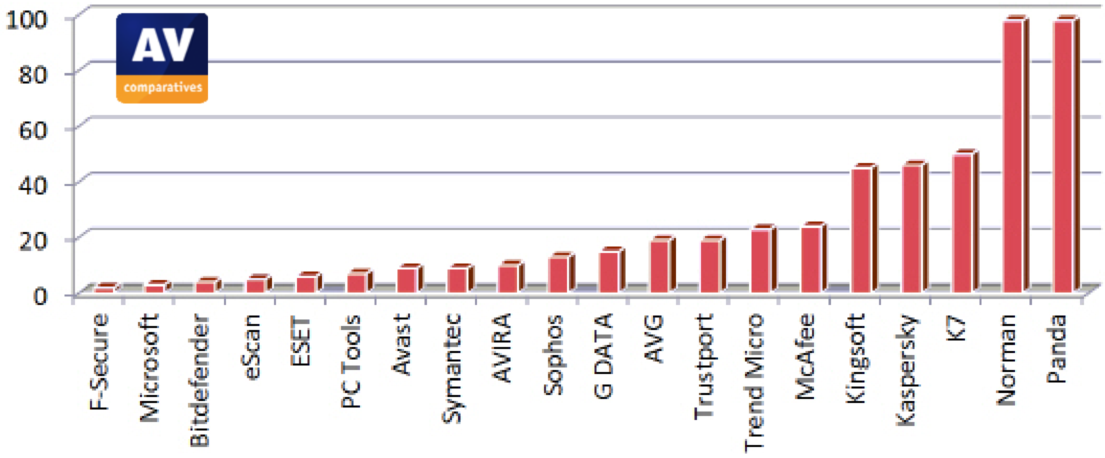
## False Positive Results

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

| | | | |
|---|---|---|---|
| 1. | F-Secure | 2 | very few FPs |
| 2. | Microsoft | 3 | |
| 3. | Bitdefender | 4 | |
| 4. | eScan | 5 | |
| 5. | ESET | 6 | |
| 6. | PC Tools | 7 | few FP's |
| 7. | Avast, Symantec | 9 | |
| 8. | AVIRA | 10 | |
| 9. | Sophos | 13 | |
| 10. | G DATA | 15 | |
| 11. | AVG, Trustport | 19 | |
| 12. | Trend Micro | 23 | |
| 13. | McAfee | 24 | |
| 14. | Kingsoft | 45 | many FP's |
| 15. | Kaspersky | 46 | |
| 16. | K7 | 50 | |
| 17. | Norman, Panda | 98 | |

**The details about the discovered false alarms (incl. prevalence) can be seen in a separate report available at: http://www.av-comparatives.org/comparativesreviews/false-alarm-tests**

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

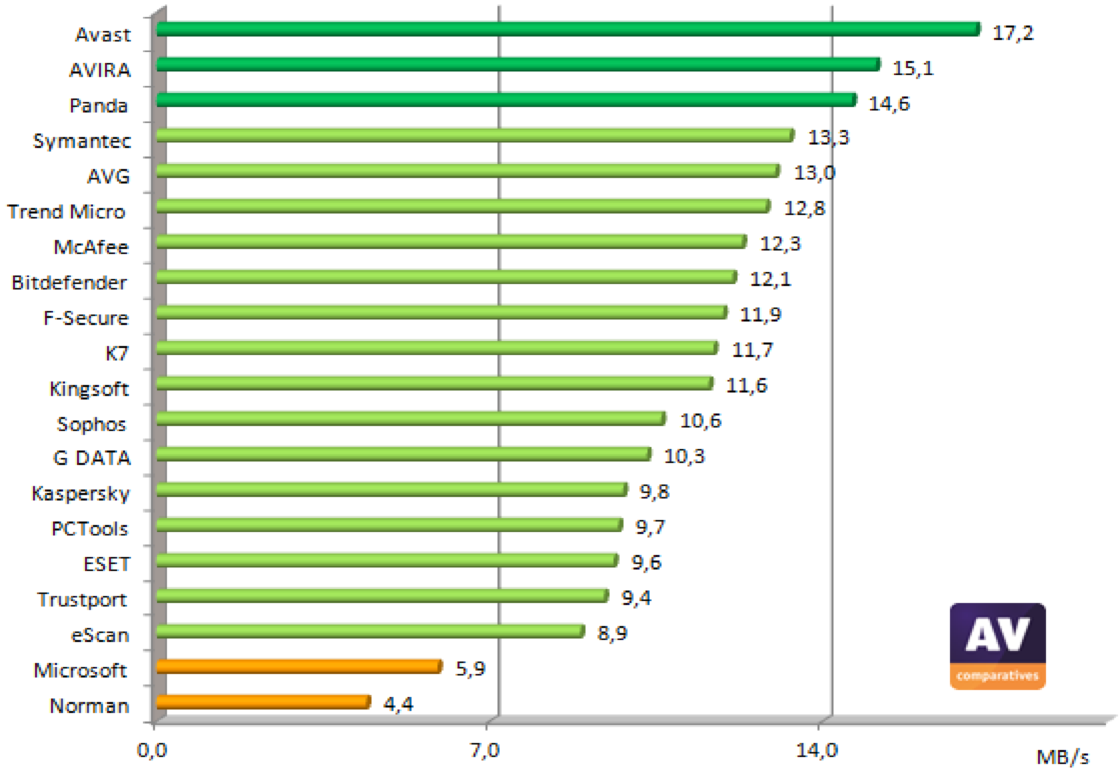


## Scanning Speed Test

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**<br>(based on detection rates and false alarms) | **PRODUCTS**<br>(in no special order) |
|---|---|
| AV comparatives ADVANCED+ ★★★ ON DEMAND DETECTION TEST AUG 2010 | ✓ G DATA<br>✓ AVIRA<br>✓ Avast<br>✓ BitDefender<br>✓ F-Secure<br>✓ eScan<br>✓ Symantec<br>✓ ESET<br>✓ PC Tools |
| AV comparatives ADVANCED ★★ ON DEMAND DETECTION TEST AUG 2010 | ✓ TrustPort*<br>✓ McAfee*<br>✓ Panda*<br>✓ AVG*<br>✓ Kaspersky*<br>✓ Microsoft<br>✓ Sophos |
| AV comparatives STANDARD ★ ON DEMAND DETECTION TEST AUG 2010 | ✓ Norman*<br>✓ K7* |
| AV comparatives TESTED ON DEMAND DETECTION TEST AUG 2010 | ✓ Trend Micro<br>✓ 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:**

| | Detection Rate | | | |
|---|---|---|---|---|
| | < 90% | 90 - 95% | 95 - 98% | 98 - 100% |
| **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 |

## Copyright and Disclaimer

This publication is Copyright © 2010 by AV-Comparatives® e.V. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. 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 2010)