

Anti-Virus Comparative



Malware Protection Test

File Detection Test with Execution

including false alarm test

Language: English
September 2017

Last Revision: 12th October 2017

www.av-comparatives.org

Table of Contents



Tested Products	3
Introduction	4
Detection vs. Protection	5
Offline vs. Online Detection Rates	6
Results (Online Protection Rates)	7
False positive (false alarm) test	8
Ranking system	9
Award levels reached in this test	10
Copyright and Disclaimer	11

Tested Products

- Adaware Antivirus Pro 12.1
- Avast Free Antivirus 17.6
- AVG Free Antivirus 17.6
- AVIRA Antivirus Pro 15.0
- Bitdefender Internet Security 22.0
- BullGuard Internet Security 17.1
- CrowdStrike Falcon Prevent 3.4
- Emsisoft Anti-Malware 2017.7
- eScan Corporate 360 14.0
- ESET Internet Security 10.1
- F-Secure SAFE 17.192
- Fortinet FortiClient 5.6
- Kaspersky Internet Security 18.0
- McAfee Internet Security 20.2
- Microsoft Windows Defender 4.11
- Panda Free Antivirus 18.0
- Seqrite Endpoint Security 17.0
- Symantec Norton Security 22.10
- Tencent PC Manager 12.3
- Trend Micro Internet Security 11.1
- VIPRE Internet Security Pro 10.1

Introduction

The Malware Protection Test is an enhancement of the File Detection Test which was performed in previous years. Due to the increased scope of the test, readers are advised to read the methodology described below. Please note that we do not recommend purchasing a product purely on the basis of one individual test or even one type of test. Rather, we would suggest that readers consult also our other recent test reports, and consider factors such as price, ease of use, compatibility and support. Installing a free trial version allows a program to be tested in everyday use before purchase.

In principle, home-user Internet security suites were used for this test. However, some vendors asked to test their (free) antivirus, or business¹ security product.

Tested products (most current versions available at the time of testing)²:

- Adaware Antivirus Pro 12.1.856.11526
- Avast Free Antivirus 17.6.2310.0
- AVG Free Antivirus 17.6.2310.0
- AVIRA Antivirus Pro 15.0.29.32
- Bitdefender Internet Security 22.0.10.141
- BullGuard Internet Security 17.1.336.1
- CrowdStrike Falcon Prevent 3.4.5511.0
- Emsisoft Anti-Malware 2017.7.0.7838
- eScan Corporate 360 14.0.1400.1957
- ESET Internet Security 10.1.219.0
- F-Secure SAFE 14.192.128
- Fortinet FortiClient 5.6.0.1075
- Kaspersky Internet Security 18.0.0.405 (c)
- McAfee Internet Security 20.2.115
- Microsoft Windows Defender 4.11.15063.447
- Panda Free Antivirus 18.03.00
- Seqrite Endpoint Security 17.00.10.3.5.1
- Symantec Norton Security 22.10.1.10
- Tencent PC Manager 12.3.26477.901
- Trend Micro Internet Security 11.1.1045
- VIPRE Internet Security Pro 10.1.4.33

The test set used for this test consisted of 20,011 malware samples, assembled after consulting telemetry data with the aim of including recent, prevalent samples that are endangering users in the field. Malware variants were clustered, in order to build a more representative test-set (i.e. to avoid over-representation of the very same malware in the set). The sample collection process was stopped on the 24th August 2017.

All products were installed on a fully up-to-date 64-Bit Microsoft Windows 10 Professional RS2 system. Products were tested at the beginning of September with default settings and using their latest updates.

¹ The **CrowdStrike**, **eScan**, **Fortinet** and **Seqrite** programs tested here are business security products.

² Information about additional third-party engines/signatures used inside the products: **Adaware**, **BullGuard**, **Emsisoft**, **eScan**, **F-Secure**, **Seqrite**, **Tencent** (English version) and **VIPRE** use the **Bitdefender** engine. **AVG** is a rebranded version of **Avast**.

Methodology

The Malware Protection Test assesses a security program's ability to protect a system against infection by malicious files before, during or after execution. The methodology used for each product tested is as follows. Prior to execution, all the test samples are subjected to on-access and on-demand scans by the security program, with each of these being done both offline and online. Any samples that have not been detected by any of these scans are then executed on the test system, with Internet/cloud access available, to allow e.g. behavioural detection features to come into play. If a product does not prevent or reverse all the changes made by a particular malware sample within a given time period, that test case is considered to be a miss. If the user is asked to decide whether a malware sample should be allowed to run, and in the case of the worst user decision system changes are observed, the test case is rated as "user-dependent".

Detection vs. Protection

The File Detection Test we performed in previous years was a detection-only test. That is to say, it only tested the ability of security programs to detect a malicious program file before execution. This ability remains an important feature of an antivirus product, and is essential for anyone who e.g. wants to check that a file is harmless before forwarding it to friends, family or colleagues.

This Malware Protection Test checks not only the *detection* rates, but also the **protection** capabilities, i.e. the ability to prevent a malicious program from actually making changes to the system. In some cases, an antivirus program may not recognise a malware sample when it is inactive, but will recognise it when it is running. Additionally, a number of AV products use behavioural detection to look for, and block, attempts by a program to carry out system changes typical of malware. Our Malware Protection Test measures the overall ability of security products to protect the system against malicious programs, whether before, during or after execution. It complements our Real-World Protection Test, which sources its malware samples from live URLs, allowing features such as URL blockers to come into play. The Malware Protection Test effectively replicates a scenario in which malware is introduced to a system via local area network or removable media such as USB flash drives (as opposed to via the Internet). Both tests include execution of any malware not detected by other features, thus allowing "last line of defence" features to come into play.

One of the significances of cloud detection mechanisms is this: Malware authors are constantly searching for new methods to bypass detection and security mechanisms. Using cloud detection enables vendors to detect and classify suspicious files in real-time to protect the user against currently unknown malware. Keeping some parts of the protection technology in the cloud prevents malware authors from adapting quickly to new detection rules.

Offline vs. Online Detection Rates

Many of the products in the test make use of cloud technologies, such as reputation services or cloud-based signatures, which are only reachable if there is an active Internet connection. By performing on-demand and on-access scans both offline and online, the test gives an indication of how cloud-dependent each product is, and consequently how well it protects the system when an Internet connection is not available. We would suggest that vendors of highly cloud-dependent products should warn users appropriately in the event that the connectivity to the cloud is lost, as this may considerably affect the protection provided. While in our test we check whether the cloud services of the respective security vendors are reachable, users should be aware that merely being online does not necessarily mean that their product's cloud service is reachable/working properly.

For readers' information and due to frequent requests from magazines and analysts, we also indicate how many of the samples were detected by each security program in the offline and online detection scans.

	OFFLINE Detection Rate	ONLINE Detection Rate	ONLINE Protection Rate	False Alarms
Adaware	98.6%		99.85%	4
Avast	97.5%	99.3%	99.99%	9
AVG	97.5%	99.3%	99.99%	9
AVIRA	97.0%	99.4%	99.97%	12
Bitdefender	98.6%		99.95%	5
BullGuard	98.6%		99.98%	5
CrowdStrike	80.1%		99.46%	16
Emsisoft	98.6%		99.98%	6
eScan	98.6%		99.88%	3
ESET	97.2%		99.86%	0
Fortinet	98.6%		99.74%	26
F-Secure	98.6%	98.9%	99.93%	22
Kaspersky Lab	94.1%	97.8%	99.96%	10
McAfee	47.9%	97.7%	99.86%	2
Microsoft	84.9%	88.8%	98.84%	6
Panda	51.3%	79.7%	99.99%	42
Seqrite	98.6%		99.85%	8
Symantec	78.7%	99.9%	99.99%	274
Tencent	98.6%		99.98%	20
Trend Micro	49.8%	98.6%	100%	80
VIPRE	98.6%		99.90%	5
<i>average</i>	88.7%	96.5%	99.85%	27
<i>min</i>	47.9%	79.7%	98.83%	0
<i>max</i>	98.6%	99.9%	100%	274

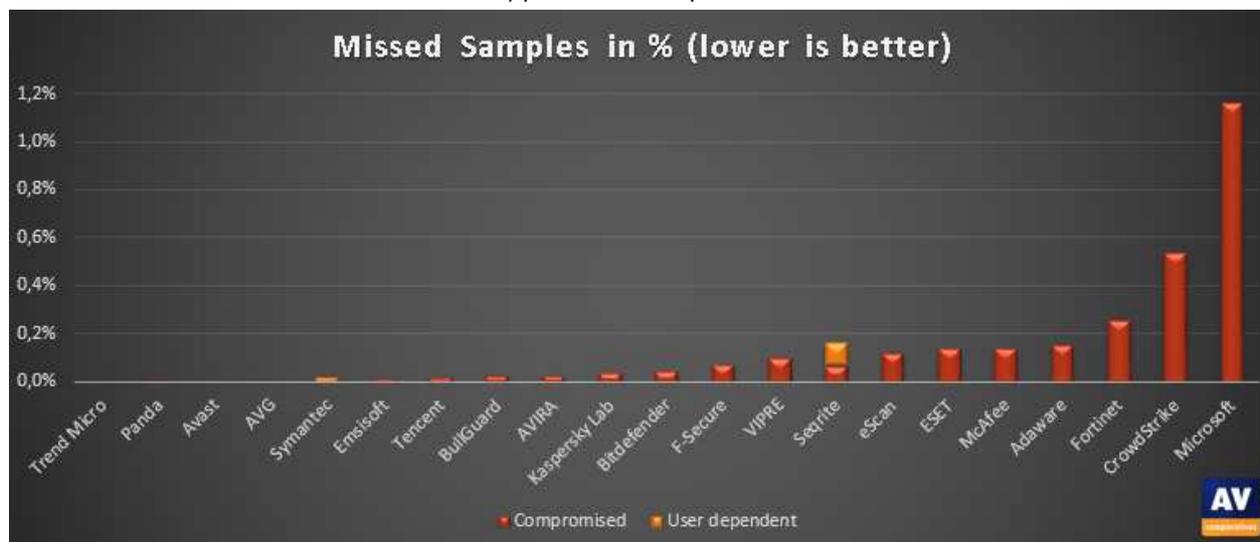
Results

Total Online Protection Rates (clustered in groups):

Please consider also the false alarm rates when looking at the protection rates below.

	Blocked	User dependent	Compromised	PROTECTION RATE ³ Blocked % + (User dependent % / 2)	Cluster ⁴
Trend Micro	20011	-	-	100%	1
Panda	20010	-	1	99.99%	1
Avast, AVG	20009	-	2	99.99%	1
Symantec	20007	4	-	99.99%	1
Emsisoft	20008	-	3	99.99%	1
Tencent	20007	-	4	99.98%	1
BullGuard	20006	-	5	99.98%	1
AVIRA	20005	-	6	99.97%	1
Kaspersky Lab	20003	-	8	99.96%	1
Bitdefender	20001	-	10	99.95%	1
F-Secure	19996	-	15	99.93%	1
VIPRE	19991	-	20	99.90%	1
Seqrite	19980	17	14	99.89%	1
eScan	19986	-	25	99.88%	1
ESET, McAfee	19983	-	28	99.86%	1
Adaware	19980	-	31	99.85%	1
Fortinet	19959	-	52	99.74%	2
CrowdStrike	19903	-	108	99.46%	3
Microsoft	19782	-	232	98.84%	4

The test-set used contained 20011 recent/prevalent samples from last few weeks.



³ User-dependent cases are given half credit. For example, if a program blocks 90% by itself, and another 10% of cases are user-dependent, we give half credit for the 10%, i.e. 5%, so it gets 95% altogether.

⁴ Hierarchical Clustering Method: defining clusters using average linkage between groups (Euclidian distance) based on the protection rate (see dendrogram on page 9).

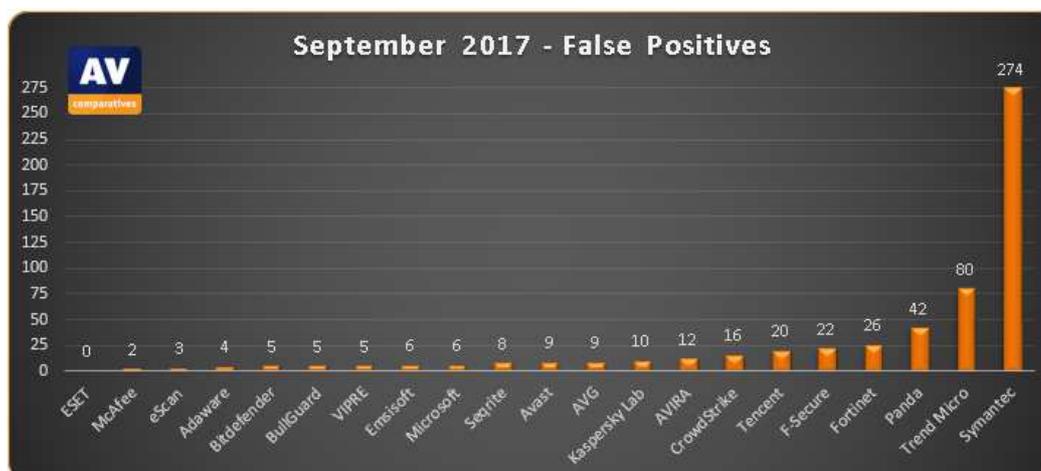
False positive (false alarm) test

In order to better evaluate the quality of the file detection capabilities (ability to distinguish good files from malicious files) of anti-virus products, we provide a false alarm test. False alarms can sometimes cause as much trouble as a real infection. Please consider the false alarm rate when looking at the detection rates, as a product which is prone to false alarms may achieve higher detection rates more easily. In this test, our whole clean-set is scanned and a representative subpart of the clean-set is executed.

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

1.	ESET	0	no/very few FPs
2.	McAfee	2	
3.	eScan	3	
4.	Adaware	4	
5.	Bitdefender, BullGuard, VIPRE	5	few FPs
6.	Emsisoft, Microsoft	6	
7.	Seqrite	8	
8.	Avast, AVG	9	
9.	Kaspersky Lab	10	
10.	AVIRA	12	
11.	CrowdStrike	16	
12.	Tencent	20	
13.	F-Secure	22	many FPs
14.	Fortinet	26	
15.	Panda	42	
16.	Trend Micro	80	very many FPs
17.	Symantec	274	remarkably many FPs

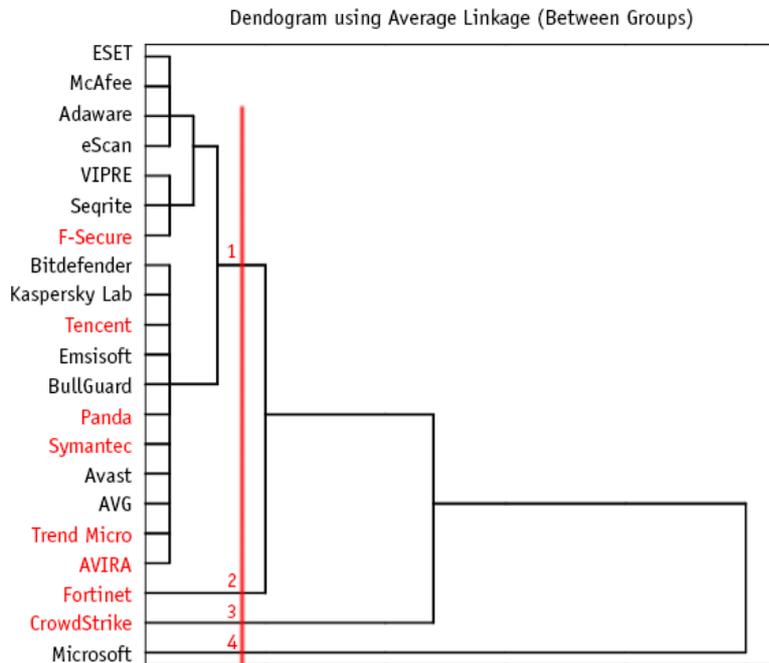
Details about the discovered false alarms (including their assumed prevalence) can be seen in the separate report available at: http://www.av-comparatives.org/wp-content/uploads/2017/10/avc_fps_201709_en.pdf



A product that is successful at detecting a high percentage of malicious files but suffers from false alarms may not be necessarily better than a product which detects fewer malicious files but which generates fewer false alarms.

Ranking system

Hierarchical Cluster Analysis



This dendrogram shows the results of the cluster analysis⁵ over the online protection rates. It indicates at what level of similarity the clusters are joined. The red drafted line defines the level of similarity. Each intersection indicates a group.

The malware protection rates are grouped by the testers after looking at the clusters built with the hierarchal clustering method. However, the testers do not stick rigidly to this in cases where it would not make sense. For example, in a scenario where all products achieve low protection rates, the highest-scoring ones will not necessarily receive the highest possible award.

	Protection Rate Clusters/Groups (given by the testers after consulting statistical methods)			
	4	3	2	1
Very few (0-1 FP's) Few (2-10 FP's)	TESTED	STANDARD	ADVANCED	ADVANCED+
Many (11-50 FP's)	TESTED	TESTED	STANDARD	ADVANCED
Very many (51-100 FP's)	TESTED	TESTED	TESTED	STANDARD
Remarkably many (over 100 FP's)	TESTED	TESTED	TESTED	TESTED

All the products included in this test achieved relatively high scores. There are two reasons for this. Firstly, a representative set of prevalent malware samples is used. Secondly, in addition to on-demand detection, the test includes on-access detection and on-execution protection with cloud connectivity. Due to the very high overall standard thus reached, the minimum scores needed for the different award levels is also very high compared to other tests.

⁵ For more information about cluster analysis, see this easy-to-understand tutorial: <http://strata.uga.edu/software/pdf/clusterTutorial.pdf>

Award levels reached in this test

AV-Comparatives provides ranking awards, which are based on levels of false positives as well as protection rates. As this report also contains the raw detection rates and not only the awards, expert users who may be less concerned about false alarms can of course rely on the protection rate alone. Details of how the awards are given can be found on page 9 of this report.

AWARDS (based on protection rates and false alarms)	PRODUCTS
	<ul style="list-style-type: none"> ✓ Avast ✓ AVG ✓ Emsisoft ✓ BullGuard ✓ Kaspersky Lab ✓ Bitdefender ✓ VIPRE ✓ Seqrite ✓ eScan ✓ ESET ✓ McAfee ✓ Adaware
	<ul style="list-style-type: none"> ✓ Panda* ✓ Tencent* ✓ AVIRA* ✓ F-Secure*
	<ul style="list-style-type: none"> ✓ Trend Micro* ✓ Fortinet*
	<ul style="list-style-type: none"> ✓ Symantec* ✓ CrowdStrike* ✓ Microsoft

*: these products got lower awards due to false alarms⁶

⁶ Please see details in: http://www.av-comparatives.org/wp-content/uploads/2017/10/avc_fps_201709_en.pdf

Copyright and Disclaimer

This publication is Copyright © 2017 by AV-Comparatives®. 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, 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.

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

AV-Comparatives (October 2017)