Independent Tests of Anti-Virus Software

AV comparatives

Malware Protection Test
Consumer Products

File Detection Test with Execution including false alarm test

TEST PERIOD: MARCH 2023
LAST REVISION: 17TH APRIL 2023

WWW.AV-COMPARATIVES.ORG

Content

Introduction

In the Malware Protection Test, malicious files are executed on the system. While in the Real-World Protection Test the vector is the web, in the Malware Protection Test the vectors can be e.g. network drives, USB or cover scenarios where the malware is already on the disk.

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 are included in this test. However, some vendors asked us to include their (free) antivirus security product instead.

Tested products[1] (most current versions available at the time of testing):

- Avast Free Antivirus 23.1
- AVG AntiVirus Free 23.1
- Avira Prime 1.1
- Bitdefender Internet Security 26.0
- ESET Internet Security 16.0
- F-Secure Internet Security 19.0
- G Data Total Security 25.5
- K7 Total Security 17.0

- Kaspersky Standard 21.9
- McAfee Total Protection 26.5
- Microsoft Defender Antivirus 4.18
- Norton Antivirus Plus 22.23
- Panda Free Antivirus 22.0
- TotalAV Antivirus Pro 5.22
- Total Defense Essential Antivirus 14.0
- Trend Micro Internet Security 17.7

The test set used for this test consisted of 10,015 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 mid of February 2023. All products were installed on a fully up-to-date 64-Bit Microsoft Windows 10 system. Products were tested at the beginning of March with default settings and using their latest updates.

---

[1] Information about additional third-party engines/signatures used inside the products: **G Data** and **Total Defense** use the **Bitdefender** engine. **TotalAV** uses the **Avira** 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 any 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. 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
Avast, AVG	96.9%	99.5%	99.97%	2
Avira	97.0%	99.1%	99.96%	2
Bitdefender	98.1%		99.94%	6
ESET	97.4%		99.94%	0
F-Secure	96.9%	98.7%	99.96%	14
G Data	98.8%		99.95%	2
K7	96.6%		99.87%	67
Kaspersky	90.0%	97.9%	99.96%	2
McAfee	89.6%	99.7%	99.99%	9
Microsoft	83.1%	99.3%	99.98%	32
Norton	91.1%	99.7%	99.99%	3
Panda	72.2%	95.5%	99.97%	102
TotalAV	96.8%	98.8%	99.97%	0
Total Defense	98.1%		99.91%	6
Trend Micro	60.9%	91.8%	97.19%	10
average	*91.3%*	*98.1%*	*99.78%*	*16*
min	*60.9%*	*91.8%*	*97.19%*	*0*
max	*98.8%*	*99.7%*	*99.99%*	*102*

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 Blocked % + (User dependent % / 2)	Cluster
McAfee, Norton	10014	-	1	99.99%	1
Microsoft	10013	-	2	99.98%	1
Panda, TotalAV	10012	-	3	99.97%	1
Avast, AVG	10011	2	2	99.97%	1
Avira, F-Secure, Kaspersky	10011	-	4	99.96%	1
G Data	10010	-	5	99.95%	1
Bitdefender, ESET	10009	-	6	99.94%	1
Total Defense	10006	-	9	99.91%	2
K7	10002	-	13	99.87%	3
Trend Micro	9734	-	281	97.19%	4

The test-set used contained 10015 samples collected in the last few weeks.
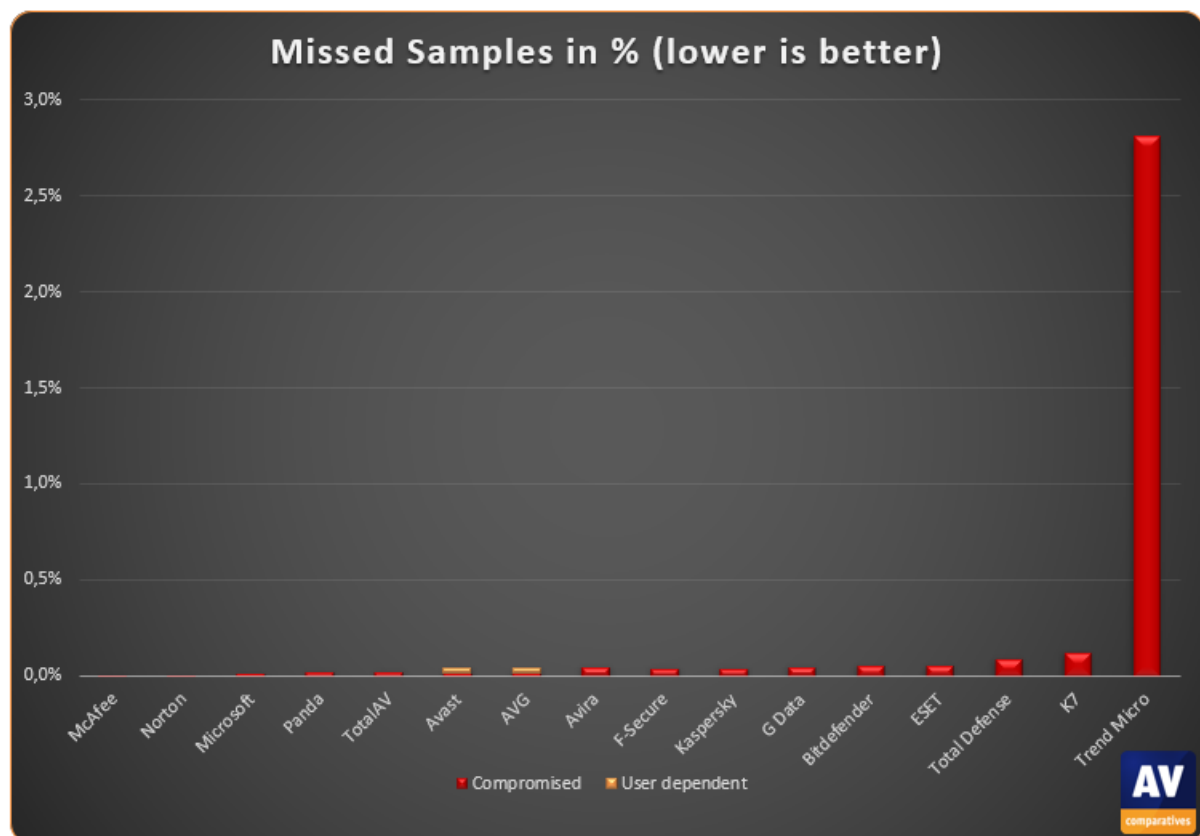
False positive (false alarm) test

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, a representative set of clean files was scanned and executed (as done with malware).

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

1.	ESET, TotalAV	0	very few FPs
2.	Avast, AVG, Avira, G Data, Kaspersky	2	
3.	Norton	3	few FPs
4.	Bitdefender, Total Defense	6	
5.	McAfee	9	
6.	Trend Micro	10	
7.	F-Secure	14	many FPs
8.	Microsoft	32	very many FPs
9.	K7	67	
10.	Panda	102	remarkably many FPs

Details about the discovered false alarms (including their assumed prevalence) can be seen in the separate report available at: https://www.av-comparatives.org/wp-content/uploads/2023/04/avc_fps_202303.pdf
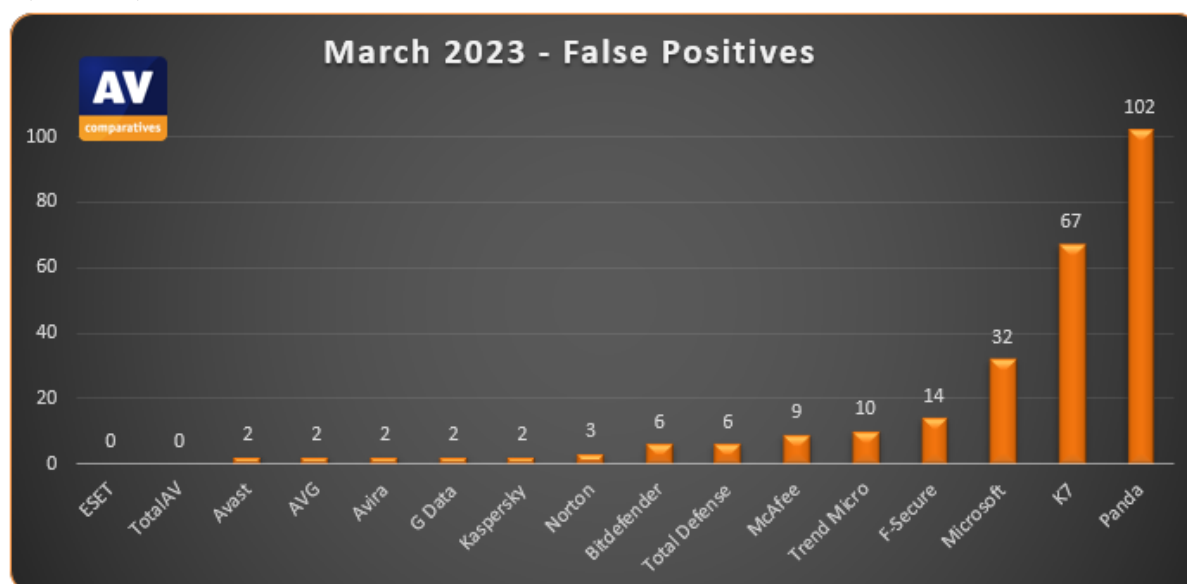
A product that is successful at detecting a high percentage of malicious files but suffers from false alarms may not be necessarily better than a product which detects fewer malicious files, but which generates fewer false alarms.

Ranking System

The malware protection rates are grouped by the testers after looking at the clusters built with the hierarchal clustering method (http://strata.uga.edu/software/pdf/clusterTutorial.pdf). 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.

The number of false positives can also affect a product's rating. Testers take statistical methods into account when defining false-positives ranges. The FP ranges for the various categories shown below might be adapted when appropriate (e.g. if we change the size of the set of clean files).

	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 (11-20 FP's)	TESTED	TESTED	STANDARD	ADVANCED
Very many (21-50 FP's)	TESTED	TESTED	TESTED	STANDARD
Remarkably many (over 50 FP's)	TESTED	TESTED	TESTED	TESTED

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 the previous page.

AWARDS (based on protection rates and false alarms)	PRODUCTS
ADVANCED+ ★★★ Malware Protection MAR 2023	✓ McAfee ✓ Norton ✓ TotalAV ✓ Avast ✓ AVG ✓ Avira ✓ Kaspersky ✓ G Data ✓ ESET ✓ Bitdefender
ADVANCED ★★ Malware Protection MAR 2023	✓ F-Secure* ✓ Total Defense
STANDARD ★ Malware Protection MAR 2023	✓ Microsoft*
TESTED Malware Protection MAR 2023	✓ K7* ✓ Panda* ✓ Trend Micro

*: these products got lower awards due to false alarms[2]

---

[2] Please see details in: https://www.av-comparatives.org/wp-content/uploads/2023/04/avc_fps_202303.pdf

Copyright and Disclaimer