Results of the AV-TEST Private Windows Test

Acronis True Image 2021

(Date of Report: August 2020)

1. EXECUTIVE SUMMARY

Acronis commissioned AV-TEST to perform a private test of their True Image 2021 product against the test categories PROTECTION and USABILITY which are part of the AV-TEST certification tests.

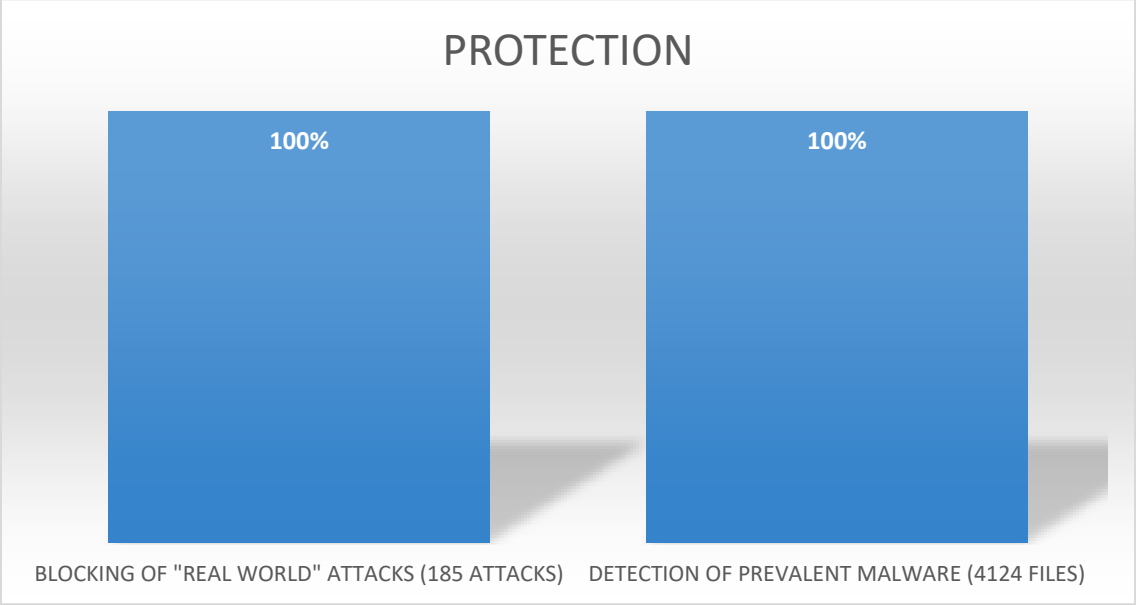
The version used in the test was the Cyber Protect product with the version number: 2021 Build 39350. The test was carried out on Windows 10 Professional (English), (64-Bit) in July and August 2020.

Acronis True Image detected and blocked every single attack in the PROTECTION test while only causing 1 false positive during the USABILITY test.

2. TEST RESULTS

2.1 PROTECTION

This category tests whether the product is able to defend a system against current and widespread attacks. The test is divided into the Real-World (malicious URLs and E-Mails) protection test and the detection of prevalent malware. All tests are carried out with an active internet connection and up-to-date products.



Real-World

In this test, the product has to defend the computer against malicious URLs that are visited with a browser or E-Mails with malicious attachments that are retrieved with a regular E-Mail client.

For this assessment 182 malicious URLs and 3 malicious E-Mails have been used.

During the test, both detection as well as protection are being rated. Acronis True Image detected 100% of the 185 malicious test cases.

Prevalent Malware Detection

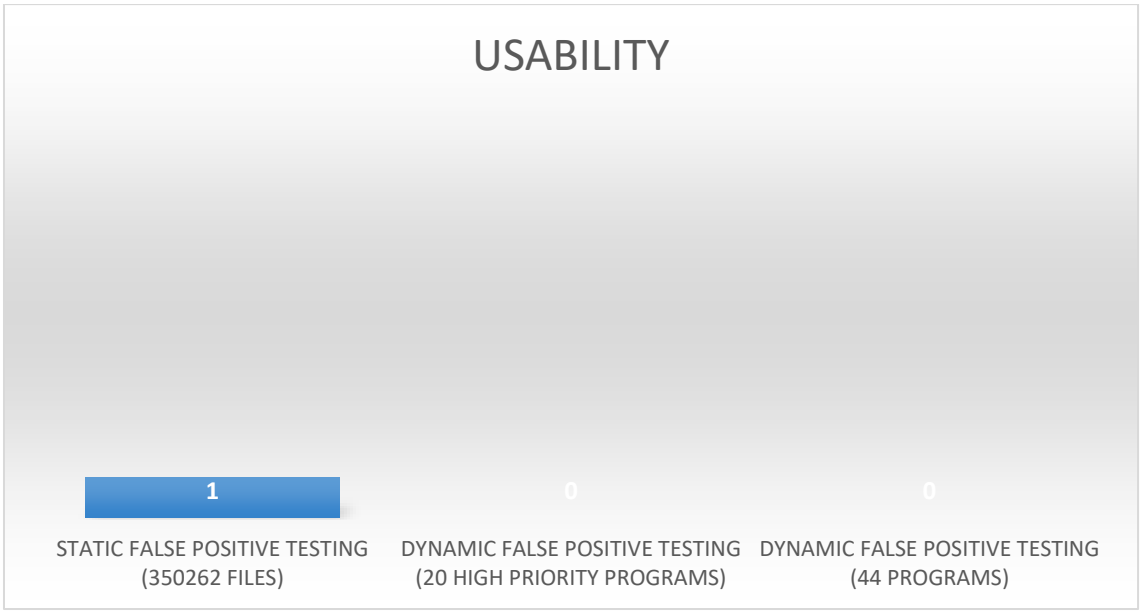
This test consists of malicious PE files that are not older than 2 weeks. Only files that have been reported as widespread and prevalent are included in this test. In total 4124 malicious files have been used in this assessment.

During the test, the files are scanned to determine the static detection rate. Afterwards we collect all not detected files and execute them file for file to test for dynamic detection. In the last step we repeat the scan to make sure no file was missed initially.

All 4124 files were being detected resulting in a detection rate of 100%.

2.2 USABILITY

The Usability category tests whether the product influences the usability of the system by causing false detection and false alarms. The test is divided into different parts: A static false positive test against different test sets and a dynamic false positive test.



Static False Positive Test

In this part, the product scans different sets of confirmed clean files to see if any false detections happen. There are three different file sets used:

1. Clean files from Windows and Office installations (172201 files)
2. Clean files from 3rd party software (158774 files)
3. Clean files from computer games obtained from different game download platforms (19287 files)

It is clear that absolutely no false positive should occur for the first set because this could harm the overall stability of the system. False positives in the other two sets can still be unpleasant, but are not a critical problem.

During the test, only one false positive in set 2 (Clean files from 3rd party software) was determined.

Dynamic False Positive Test

In this part normal user interaction is simulated by downloading clean software from the internet, installing and using it. During these actions the product is monitored to check whether it issues any false alarms or even blocks certain legitimate actions.

Two different test sets are used here:

1. “High Priority” set conaining widespread software such as Adobe Reader, Google Chrome or Java (20 different programs)
2. “Normal” set containing any other software (44 different programs)

There were absolutely no warnings or other problems during this test.

3. SUMMARY

Both the PROTECTION and USABILITY tests showed very good results. Protection was flawless and in case of Usability there was only one false positive detection which can be considered a minor issue. These results would definitely be enough to get certified and reach a high score in the official AV-TEST certification test.