Results of the Windows 10 Test of “Sangfor Endpoint Security Protect”, performed by AV-TEST GmbH.

(Date of Report: 30th September 2020)

1. EXECUTIVE SUMMARY

Sangfor commissioned AV-TEST to perform a review of their Endpoint Security Protect product against the test categories PROTECTION, PERFORMANCE and USABILITY which are part of the AV-TEST certification tests.

We used the Sangfor Endpoint Security Protect product with the version number 3.2.18EN. The test was carried out on Windows 10 Professional (English, 64-Bit) in July and August 2020.

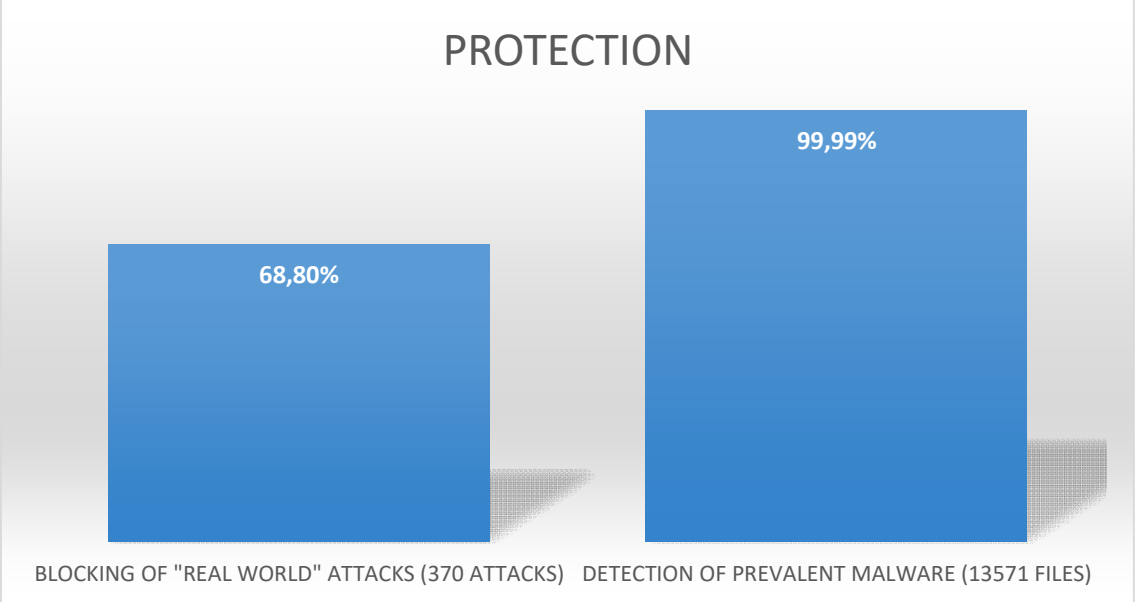
Sangfor showed a minimal system impact in the PERFORMANCE test and 13 non-critical false positives in the USABILITY part. PROTECTION of the prevalent malware is at a very high level, while the detection rate of the more "critical" real-world test cases is well below the industry average.

In summary, the criteria of the standard AV-TEST certification were met.

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 264 malicious URLs and 106 malicious e-mails have been used.

During the test, both detection as well as protection are being rated. Sangfor Endpoint Security Protect detected only 68% of the 370 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 13,571 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.

In total 13,562 files were being detected resulting in a detection rate of 99.99%.

2.2 Performance

In order to investigate the influence of security solutions on speed, typical operations for daily computer work are performed, measured and analyzed.

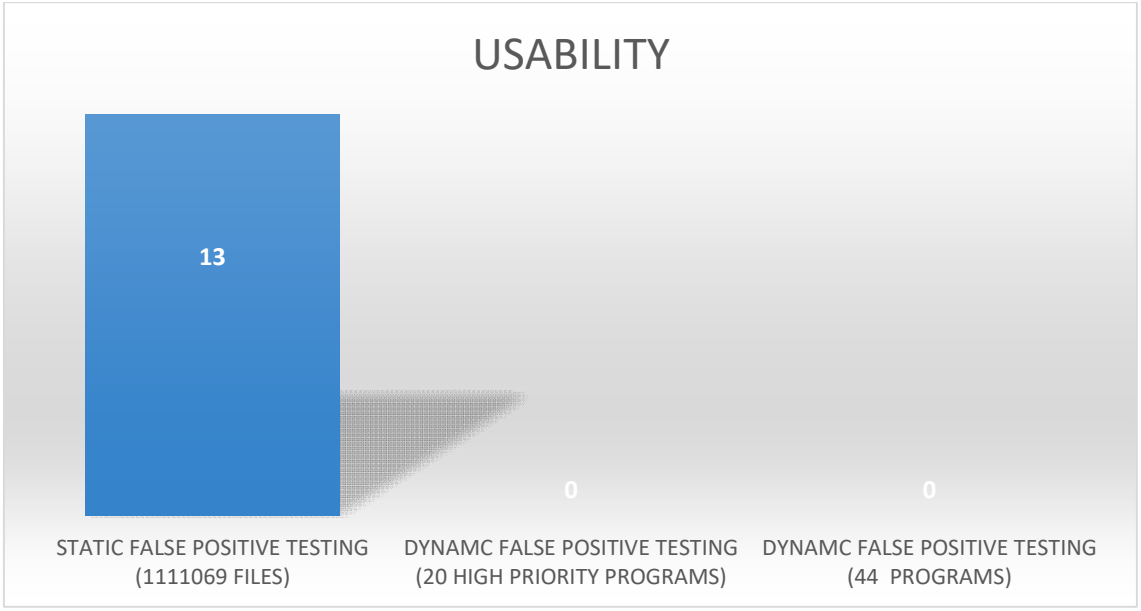
The following are carried out in the test:

- Slowdown at the start of popular websites
- Slower downloading of frequently used programs
- Slower introduction of standard software programs
- Slower installation of frequently used programs
- Slower copying of files (locally and in a network)

Sangfor slows down the system only minimally with an impact of 8%, thus achieving a very good result.

2.3 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 (527,196 files)
2. Clean files from 3rd party software (531,409 files)
3. Clean files from typical Business software installations (52,464 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, 13 false positives in set 2 (clean files from 3rd party software) ware determined. These are not rated critical, but they lower the score in the Usability part.

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 containing 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 no warnings or other problems during this test.

3. SUMMARY

The PERFORMANCE test showed a very good result and the USABILITY results are also well despite the 13 false positive detections for third party software. On the PROTECTION side Sangfor scored perfectly in the prevalent malware detection test. But the Real-World results are far below the industry average.

In summary, the criteria of the standard AV-TEST certification were met.

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org