Advanced Threat Prevention Test

Date of the Report: February 2nd 2017

Executive Summary

Cylance commissioned AV-TEST to perform an advanced threat prevention test of enterprise endpoint protection software. The testing methodology was developed jointly to provide additive testing to the commodity Anti-Virus protection tests currently produced by AV-TEST.

CylancePROTECT® was tested against 5 competitor endpoint products from Kaspersky, McAfee, Sophos, Symantec and Trend Micro. The test was performed in December 2016 and January 2017. This report contains the results of four test cases. The primary goal was to show the detection and prevention capabilities of new and unknown malicious executables.

Test Case 1 - The Holiday Test: The purpose of this test is to reproduce a real world scenario whereby an end user goes on holiday for a given period. Upon returning from the holiday the end user returns to their endpoint and gets infected prior to the endpoint being able to update their protection measures. This is also a scenario encountered by organizations who may ultimately be forced to go to extreme measures such as delaying signature updates by a quarter due to performance impact to the user. This scenario is also a fairly easy way to test for “zero-day” detection and prevention capabilities. The test itself freezes the product at Day 0 and then removes it from being online. We then wait 7 days and collect new malware (executables) that are considered newly discovered on day 7 and start testing. We bring up the frozen product without connectivity to the internet so that the protection measures are essentially 7 days old. Testing is performed completely offline with the outdated protection measures. Products were unable to update themselves or query the cloud. We then ran the newly discovered malware against the products for detection and prevention efficacy against what essentially would be unknowns to the security solution being tested.

Test Case 2 - Simulated Attacks: The second test simulated a targeted attack where an attacker was able to introduce an executable file on the system. These executables were created by AV-TEST to simulate certain types of attacks that had to be detected and blocked by the products. These executables are based upon common advanced attacks seen today. The new zero-days are executed on systems first in offline mode to validate endpoint security solutions ability to detect true unknown attacks without connectivity to the cloud. And then online to show the impact of cloud queries.

Test Case 3 - Malware distributed by Websites: This test looked at malware executables delivered via websites. The URL itself is not malicious, it’s the content of the website that is malicious. This test turns off URL Filtering of all products under test to determine if they can truly detect malicious nature of visited website.

Test Case 4: False Positives – Every protection test should be verified by a false positive test to make sure, good detection rates are not sacrificed for usability and false positives. In order to test this we downloaded, installed and actually used 38 different, common applications including Adobe reader, Google Chrome, Java JDK or Skype. Any warning messages or blockings of the tested protection product was noted.

In all test cases CylancePROTECT® showed extremely high efficacy prevention rates. They have a very reliable approach that works offline, without the need for regular updates even before execution of the malware. It also shows the dependency for the other products on regular updates, cloud queries or dynamic analysis. The tests have shown that CylancePROTECT® is able to detect unknown attacks, while most of the other tested vendors could not demonstrate this ability.

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Testing Methodology

Hardware Platform and Operating System

All tests were performed on identical hardware platforms with the following specifications.

Operating system	Windows 10 Professional with all patches available on December 1st 2016.
Hardware	• Intel Xeon Quad-Core X3360 CPU • 4 GB RAM • 500 GB HDD (Western Digital) • Intel Pro/1000PL (Gigabit Ethernet) NIC

Tested Products

The products tested and their versions are listed in the following table.

Product Name	Version
CylancePROTECT®	1.2.1410.60
Kaspersky Endpoint Security	10.2.5.3201 (mr3)
McAfee Endpoint Security	10.2.0.620
Sophos Endpoint Security and Control	10.6.4.1150
Symantec Endpoint Protection	14.0.1886.0000
Trend Micro OfficeScan	12.0.1901

Test Case 1: Holiday Test

The purpose of this test is to show the detection capabilities of a product against new malware (PE files), with week old security measures, signatures, machine learning models or ability to query the cloud:

1. Installation: The product is installed and updated to the latest program version and signatures
2. Freeze the product: A disk image is created at day 0 and removed from being online
3. Wait 7 days, then collect new malware (PE's) that are considered newly discovered on day 7.
4. Bring up the frozen product without connectivity to any form of the internet so that the signature update file is essentially 7 days old.
5. Run the newly discovered malware (PE's) against the VUT
    a. Static Detection: First perform an on-access test by copying the files on the hard disk and then perform an on-demand scan of the remaining files
    b. Dynamic Detection: Then execute all remaining samples
6. Record efficacy results.

Sample Selection

For this test, 98 samples have been randomly selected that were first seen by AV-TEST on January 19th and 20th. They were all PE files and contained Backdoors, Downloaders, Droppers, Generic Trojans and Viruses.

Test Case 2: Simulated Attacks

When attackers perform targeted attacks they will either modify existing malware/tools or write new tools to make sure there are no signatures for them. In order to simulate such a targeted attack AV-

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

TEST created binaries for five possible attack scenarios. These were then modified in two different ways creating 15 test cases.

1. Installation: The product is installed and updated to the latest program version and signatures
2. The test was performed in three steps. The first two without internet access, the final one with internet access:
    a. Static Detection (Offline): First perform an on-access test by copying the files on the hard disk and then perform an on-demand scan of the remaining files
    b. Dynamic Detection (Offline): Then execute all remaining samples
    c. Dynamic Detection (Online): The connect the system to the internet and execute all remaining samples
3. Record efficacy results.

Sample Selection

There were five different tools created with the behaviors listed below. All of the tools have been written in C/C++ and compiled with Microsoft Visual C++

	Persistence	Payload
Attack 1	Registry: HKCU	Credential harvesting and upload to external server
Attack 2	Startup Folder	Credential harvesting and upload to external server
Attack 3	-	Download and execute further executable
Attack 4	-	Modify HDD sectors
Attack 5	-	Encrypt files

Table 1: Simulated attacks

The five resulting test cases were then modified with two different approaches. The first approach was to add a section to the PE file. The second approach was to append data to the end of the PE file.

This resulted in 15 different files with different hashes.

Test Case 3: Malware distributed by Websites

Many infections these days are spread via websites. Most protection products use a layered approach to block these. They try to cover the URL and the malicious content. Different products have different priorities here and some may focus more on URL blocking than others. However it is rather easy for attackers to change the URL to defeat this kind of detection. Therefore this test is designed to determine the detection rate of the malicious PE file delivered by the website, when no URL is available.

1. Installation: The product is installed and updated to the latest program version and signatures
2. Turn off URL filtering of the product if applicable.
3. From victim connect to the website, download and execute the file
4. Record efficacy results.

Sample Selection

For this test, 69 websites have been randomly selected that are spreading malware.

Test Case 4: False Positives

It would be easy to create a protection product that scores 100% in all protection tests but at the same time creates false positives on all benign files. Therefore we tested how the products do react to common and less common software when downloading them from their original source, installing

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

and using them on the computer. Whenever the security product detected something and warned or blocked an action this was noted for the result.

Sample Selection

In total 38 different common and less common applications have been used for the testing. The full list is given in the appendix at the end of this document.

General notes regarding the testing methodology:

There is one issue we would like to briefly discuss about writing attack simulation tools.

When testing protection against new or targeted attacks it is always necessary to create own test cases. This can happen by modifying existing malware or by creating own attack simulation tools. Both is controversially discussed not only in the anti-malware industry. We opted to create our own attack simulation tools in order to have full control over the tools and to be able to make sure that no harm could be done by them.

The Anti-Malware Testing Standards Organization (AMTSO) created several documents for best practices of anti-malware testing. One of those documents is named “Issues Involved in the ‘Creation’ of Samples for Testing”[1]. This document discusses the arguments in favor and in opposition to modifying malware or creating files like the attack simulators that we did. The document neither forbids nor explicitly endorses the creation of new samples for testing. It depends on what exactly shall be achieved with the test. After carefully consulting the document we are convinced that our approach is in line with the presented arguments.

[1] http://www.amtso.org/download/amtso-issues-involved-in-the-creation-of-samples-for-testing/

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Test Results

The test results for all other vendors but CylancePROTECT® are presented in an anonymized form. Instead of giving exact product names, the products are called Vendor 1 to 5. They are sorted by the result in Test Case 1 and the same vendor is always given the same number throughout all three test cases.

The first test case covered 100 new samples that had to be detected offline and with 7 day old signature databases. The results displayed in figure 1 show that Cylance achieved by far the best result in this test.

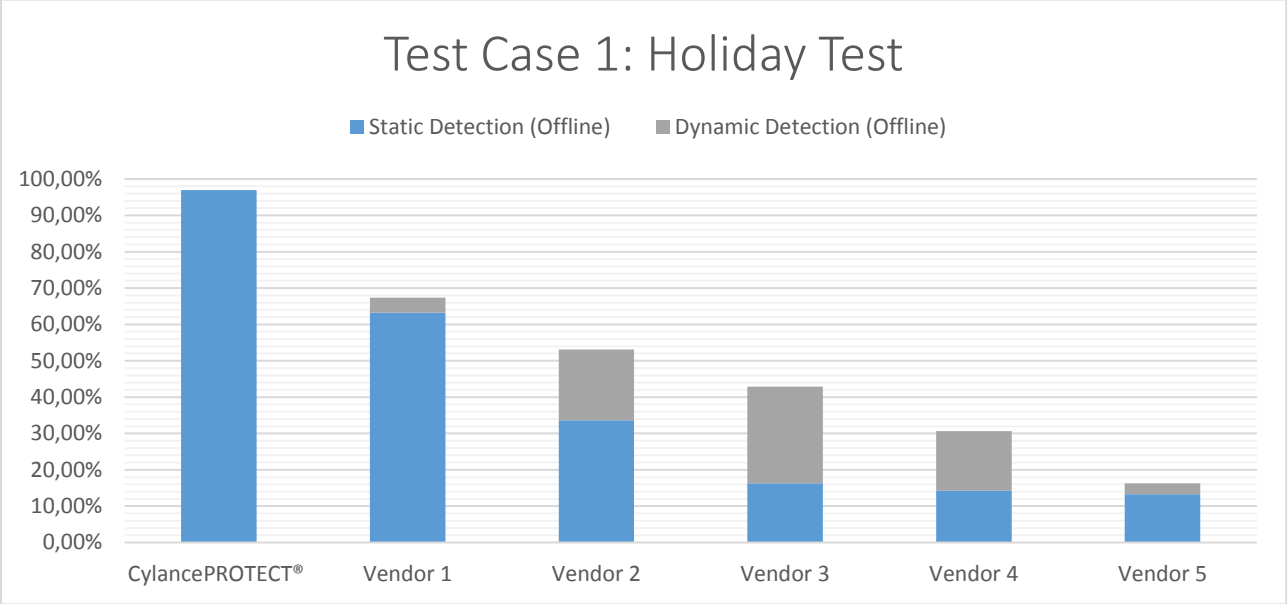

Figure 1: Static and Dynamic detection results of new malware

CylancePROTECT® detected over 97% of the samples before execution. The best other product detected 67% and the average of Vendor 1 to Vendor 5 was only 42% detection rate. However only when combining static and dynamic detection. The static detection alone was even lower at 28% for the average of Vendor 1 to 5. The best product scored 63% compared to 97% of Cylance.

While this may not be a typical use case, it can still happen. Some companies may not deploy updates regularly or people come back from holidays to a not updated machine with outdated signature databases. Cloud queries can also go wrong. We have seen outages at vendors as well as high sensitivity to network issues for some products. Even if the internet connection is still working, cloud queries could go wrong if there is for example packet loss. This can happen in public Wifis like Starbucks or at airports. There are more cases where offline testing could be relevant and we suggest to at least discuss these options if applicable for the evaluated security product:

- Retail POS/ATM – In some deployment cases all network communication is constrained or reduced to a single application within the POS/ATM or constricted by the firewall.
- Diversionary Tactic – Take out a network segment, have SecOps focus on it, then go do damage/exfiltration elsewhere
- Bottom-up DDoS – Could be paired with above– take out network segment and cause damage (also would be a case in universities, government, healthcare, etc.)
- Malware that attacks the connection

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

More important are the technical implications from this test: CylancePROTECT® doesn't need regular signature updates nor does it require cloud queries to detect new files, even before execution. On the other hand, the other tested products depend on updated signature databases and cloud queries to provide additional level of detection.

The results in figure 2 show the success in detecting new binaries that simulate attacks on an endpoint. The figure displays the offline detection. Again CylancePROTECT® detected all threats even before execution and even without internet connectivity.

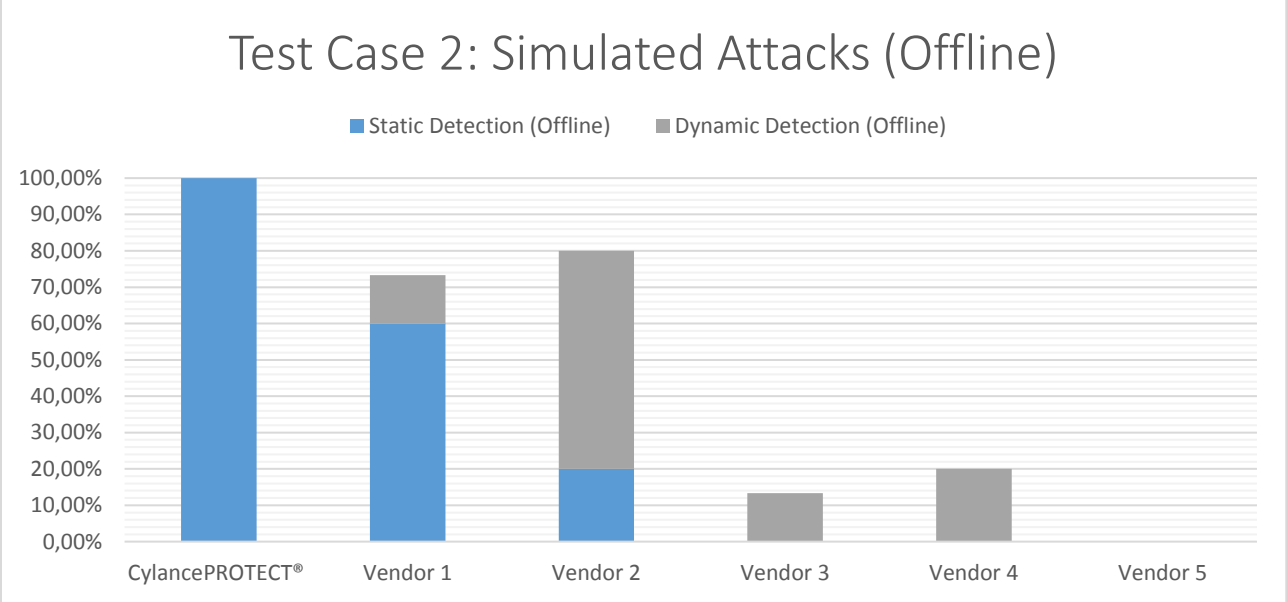

Figure 2: Detection of new binaries simulating attacks

Only two other vendors besides CylancePROTECT® were able to detect some files offline before execution. Most of the other detections came from behavioral analysis during execution of the tools. Two vendors did provide additional detection when the test was carried out with online detection. These results are shown in figure 3.

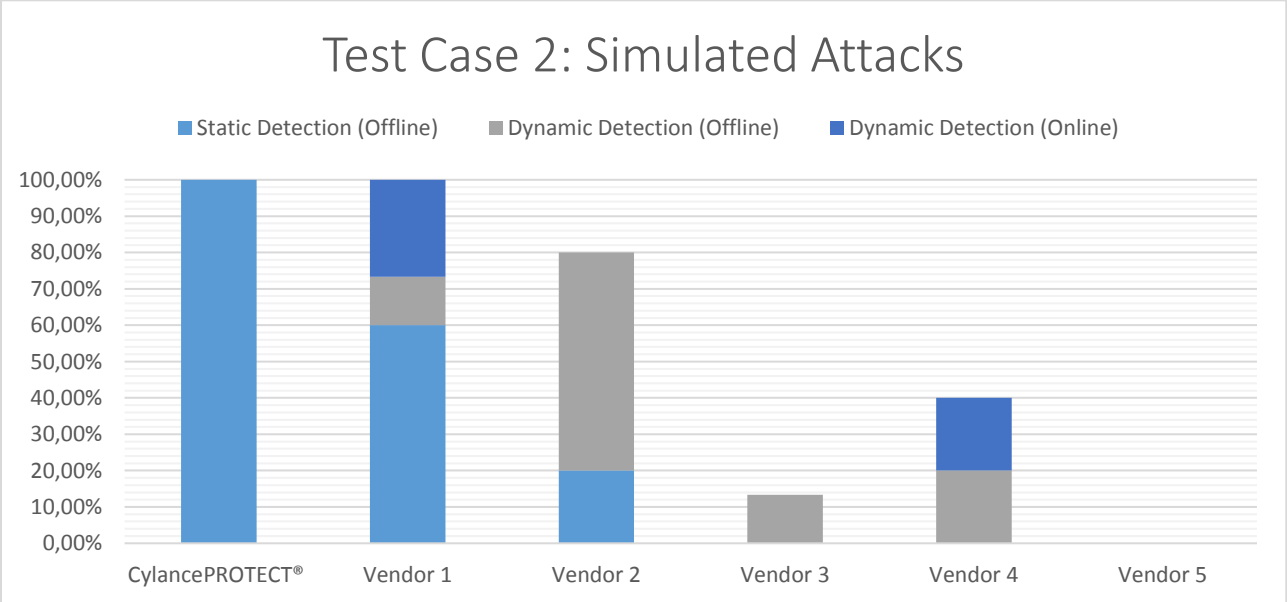

Figure 3: Detection of new binaries simulating attacks (with online detection)

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

These additional online detections were primarily reputation based decisions for one of the products. This product did report that the files are new and have never been seen before. However, it did not find anything suspicious in them. The following table shows the detection per product.[2]

Test Case:	1	2	3	4	5	1S	2S	3S	4S	5S	1A	2A	3A	4A	5A
CylancePROTECT®	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Vendor 1	D	D	R	R	R	S	S	S	S	S	S	S	S	R	S
Vendor 2	D	D	S	-	D	D	D	S	-	D	D	D	S	-	D
Vendor 3	-	D	-	-	-	-	D	-	-	-	-	-	-	-	-
Vendor 4	D	-	-	DO	-	D	-	-	DO	-	D	-	-	DO	-
Vendor 5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 2: Detection per sample

In the final test case the products had to detect malware distributed by websites, without using their URL filtering component. Not surprisingly we are seeing a similar picture as in the previous tests. CylancePROTECT® again detected nearly all test cases with static detection and the one remaining case was detected during execution of the downloaded binary.

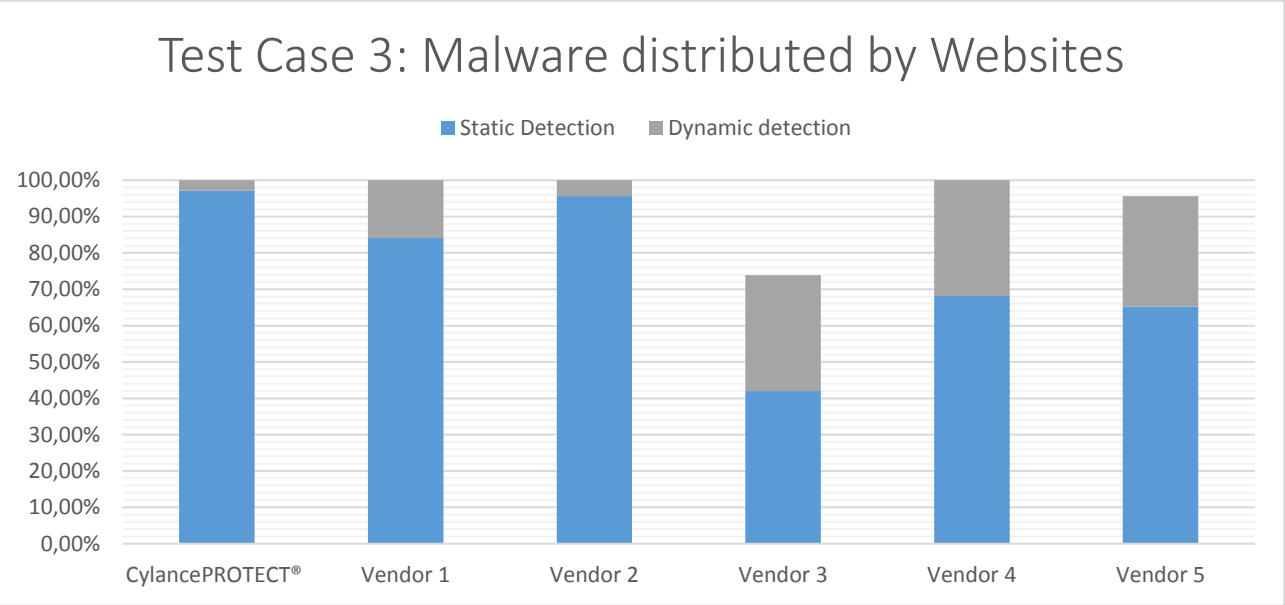

Figure 4: Detection of executables spread by websites

The other products detected 71% of the samples by static detection and 22% more by dynamic detection after execution. Vendor 3 had serious problems with detection, when taking away the URL filtering component dropping to 73%.

When it comes to false positives, there were no serious problems with any of the tested products. We did see two detections of installed files by CylancePROTECT® for Android Studio as well as for Samsung SideSync. The other products didn't generate a false positive.

All three protection test cases show that CylancePROTECT® has a very reliable approach that works offline, without the need for regular updates even before execution of the malware. It also shows the dependency of the other products on regular updates, cloud queries or dynamic analysis/behavioral

[2] Explanation for Table 1:
Test Case 1S = Sample 1 with added section
Test Case 1A = Sample 1 with appended data to the end of the file
Detection Type: S = Static Offline, D = Dynamic Offline, DO = Dynamic Online, R = Reputation

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

detection. The tests have shown that CylancePROTECT® is able to detect and prevent unknown attacks, while the other vendors have more problems with new attacks.

The regular tests performed by AV-TEST show that the products do provide reliable protection from commodity malware if the products have access to the cloud, can use all protection layers and have updated signature databases. But as shown above, this is no longer enough to be able to protect from new and unknown threats.

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Appendix

List of products used for the false positive test

7-zip 16.04	HD Clone 6.0.7	Samsung Sidesync 4.5.0.86
Adobe Reader DC 2015.020.20039	iTunes 12.5.3	Skype 7.30.0.105
Argusmonitor 3.3.7	Java JDK 8u112	Snappy Driver R513
Android Studio 2.2	Kindle for PC 1.17.44183	Steam 3.61.93.65
Classic Ftp 2.38	Libre Office 5.2.3	Teamviewer v12.0.71503.0
Clone BD 1.0.8.8	Linux Multi Media Studio 1.1.3	Thunderbird 45.5.1
doPDF 8.8	Mycommander 3.3	Tomahawk 0.8.4
DVR Studio HD 4.11	MyPhoneexplorer 1.8.7	Tor Browser 6.0.7
Firefox 50.02	Nettalk 6.7.16 2.12.1	Ultravnc 1.2.12
Freecad 0.16	Notepad++ 7	VLC Media Player 2.2.4
Gimp 2.8.18	Opera 41.0.2353.69	Vmware Player 12.5.1-4542065
Google Chrome 55.0.2883.75 m	Picard 1.3.2	Winrar 5.40
Google Earth 7.1.7.2606	Residualvm 0.2.1	

Copyright © 2017 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org