ENDPOINT PROTECTION SOLUTIONS REPORT 03/18

Endpoint protection solutions must constantly adapt to new threats to protect users, endpoints and ultimately businesses. The endpoint is usually the last line of defense. This report compares the manufacturers of current and long-established antivirus solutions with next-generation solutions. This raises the question: is the detection rate of traditional AV products still sufficient or do new approaches and technologies offer a significant advantage in terms of protection against known, unknown and new malware?

EPSR, March 2018

This report is the fourth edition. In order to ensure comparability with previous reports, tests were conducted in a similar scenario as before. Only the tested AV products have been updated to the latest available version.

The result of the investigation is clear: next-Gen solutions offer a significantly higher detection rate compared to classical AV solutions while using significantly less system resources.

Next-Gen solutions are usually new products developed from scratch that ensure protection by using artificial intelligence (AI), behavioural analysis and intelligent process monitoring. It is irrelevant for these products whether it is known or unknown malware they are dealing with. These products work without signatures and offer support for the most common operating systems and platforms (Windows, Linux, Mac).

All products are registered as an AV manufacturer at Microsoft. The test scenarios are based solely on the protection against malware. The samples are already on the test systems at the beginning of the test. Other relevant protection components for protection against cyber-attacks such as, among other things, browser security, protection against malicious E-Mails and perimeter protection are not part of this test. Furthermore, the test for protection against exploits is also excluded from this report.

INVESTIGATED SOLUTIONS

Next-Generation-Solutions

CylancePROTECT Version 1470 (2.0.1470.17)
Cylance primarily uses AI with machine learning techniques for detecting malware and exploits. The AI recognizes whether a file is benign or malicious by using static analysis of executables and DLLs without having to execute it (pre-execution and predictive).

In addition to the AI, Cylance also uses other protection modules and functions to protect the endpoint, such as Script Control against scripts or macros, which are often used in Ransomware attacks, or Memory Protection to protect against exploits in software.

Palo Alto Networks Traps 4.1.3 (v4.1.3-33176, 35-2390)
Traps is part of the Palo Alto Networks security platform and protects against known and unknown malicious executables, DLLs and office files using a unique multi-method prevention approach. This approach maximizes protection against unknown malware and exploits while simultaneously reducing the area of attack.

By combining a wide range of prevention methods, malware is stopped from compromising a system. Script based attacks are prevented out-of-the-box.

Ransomware is immediately stopped by Traps in case of an attack and the encryption of data is prevented. The multi-method exploit prevention is designed to prevent exploits by using modules such as Pre-Exploit-Protection, Technique-Based-Exploit-Prevention and Kernel-Exploit-Prevention.

**Sophos Endpoint Protection 2017 (11.5.11)
with Intercept X 2.0 (Beta-Features enabled)**
Intercept X extends Sophos Anti-Virus protection to include threat and exploit detection, as well as –new- by a Machine Learning Model. Unauthorized encryption (such as Ransomware) is prevented by a module called CryptoGuard. These technologies should enable Intercept X to detect and prevent Zero-Day malware in advance therefore complementing the signature based AV protection.

Established Solutions

Kaspersky Endpoint Security 10 (10.3.0.6409)
Kaspersky Endpoint Security offers protection for PC, Mac und mobile devices. The protection modules are similar to the modules used by Symantec Endpoint. It has an integrated AV scanner with a signature database and also has the ability for heuristic analysis of files. Kaspersky also offers additional modules like a password manager, mobile device security, firewall functionality and program control.

McAfee Endpoint Security 10.5 (10.5.3)
McAfee offers machine-learning techniques in addition to its AV scanner. They are divided into static and behavioural analyses. To supplement its protection firewall modules and web control are also included. The threat prevention module should also provide protection against exploits.

Symantec Endpoint Protection Cloud 22 (22.11.2.7)
Symantec offers many new and improved recognition features in addition to the conventional signature database. Modules such as behavioural analysis, machine-learning and static analysis are used to detect malware.

SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00
www.securelink.de

Trend Micro Office Scan 12 (12.0.4430 SP1)
Office Scan uses a signature based AV scanner like all conventional solutions. Since the latest version, additional machine learning techniques have been used to analyse files before execution. Likewise, behavioural analyses of scripts and browser attacks are carried out.

Windows Defender by Microsoft (4.12.17007)
Windows Defender provides a conventional AV scanner with additional features such as an integrated firewall. This program is a lean and above all integrated and cost-free alternative.

All tested solutions offer a central management console (in the cloud and / or on premise). An exception is Windows Defender which does not provide a central management console as it is an integrated product of Microsoft Windows.

TEST CRITERIA AND METHODOLOGY

Test setup

A total of 1,708 malware samples were used in the first and second test phase hereinafter referred to as Basic Test and Holiday Test. In the Basic Test the 1,708 samples were first tested offline then online. The machines were reset between the tests.

A quarter of the samples were downloaded from the sources below without being altered. These samples were subsequently modified (obfuscation) several times after an initial analysis and thus mutated in three different ways in order to simulate unknown and Zero-Day malware respectively.

These files are usually no longer recognized by signature based methods. For a basic mutation the hash value of the files has been altered. For the two advanced mutations packing techniques for executable files, using software packers such as UPX and mPress, were used.

Testing methodology

Basic Test
The key criterion for testing the endpoint security solutions was the recognition rate (efficacy).
All endpoint security solutions were tested under the same conditions in the SecureLink test lab over a 14-day period as follows:

- The signature databases and all other modules have been updated to the latest available version.
- In order to enable the AV solutions to access reputation databases, intelligence in the cloud and sandboxes, an internet connection was provided.
- Using a scanning function, the malware samples were scanned before execution and the detection rate was determined.
- The remaining samples were then executed (execution test).
- In order for the executed malware to perform, for example, C2 communication and to load additional malicious code, Internet Access was enabled (detection rate online).
- In addition, a test was performed with all samples with- out internet access (recognition rate offline).
- The tested malware samples consisted of a mix of about 50% ransomware, 20% Trojans, 10% Zero Day and 20% other malware. The samples were collected over a period of 14 days.
- The samples were taken from various public sources: *http:// malwr.com, http://dasmalwerk.com, http://malc0de.com/ database, http://testmyav.com, http://virustotal.com, https://malpedia.caad.fkie.fraunhofer.de*

Holiday Test
The second test scenario is the Holiday Test. The test devices were disconnected from the internet 14 days prior to the test and were no longer updated. Afterwards the 1,708 malware samples were copied to the systems and scanned. This test represents a realistic scenario in which an employee returns from vacation and is infected with malware before the signature databases can be updated. The test should show the recognition rates dependency in relation to signature databases. Internet access was not set up on principle.

RESULTS AND INTERPRETATION

Next Generation Solutions

Solution B and A consistently achieved very high detection rates (B 94.3% and A 99.8%). Solution C reached 91.8%.

The Holiday Test confirms the effectiveness of the signatureless approaches of Solution A and B. Other solutions offer only limited protection, which has to be paid for with a lot of computing power.

The maturity of Solution A's AI model once again demonstrates high reliability and consistently very good detection rates, without the need to execute a file.

The multi-method preventive approach Solution B also delivers very good results without burdening the endpoint.

Conventional AV Solutions

With conventional AV solutions, the sole use of the signature database would not have been sufficient and would have resulted in a recognition rate of only 62.2 % with solution H, for example. Due to the additional modules and technologies such as static analysis, behavioural analysis and confidentiality checks, significantly higher rates of up to 95.7 % (solution D) are achieved in some cases. However, these are still behind the endpoint solutions of solution A, B and C. The test candidates Solution H and F were disappointing. Despite innovative technologies and modules, both were unable to achieve satisfactory detection rates. The products were therefore not convincing. Solution G, as free protection, was included as a reference in the test. Surprisingly, the solution was able to outbid other manufacturers in some cases.

SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00

Unfortunately, we can only make the data available to you anonymously at this point, and we will be happy to answer any questions personally.

SOLUTIONS IN COMPARISON – BASIC TEST

Solution	Scenario			
	Detectionrate before execution offline	Detectionrate before execution online	Detectionrate at execution offline	Detectionrate at execution online
Solution A	**97,89 %**	**99,88 %**	**97,89 %**	**99,88 %**
Solution B	-	-	**91,69 %**	**94,25 %**
Solution C	**83,08 %**	**85,83 %**	**91,86 %**	**91,80 %**
Solution D	**61,65 %**	**63,11 %**	**93,97 %**	**95,73 %**
Solution E	**70,43 %**	**80,33 %**	**93,15 %**	**95,32 %**
Solution F	**35,83 %**	**36,53 %**	**83,20 %**	**86,65 %**
Solution G	**57,79 %**	**62,00 %**	**63,23 %**	**66,92 %**
Solution H	**52,75 %**	**61,18 %**	**62,12 %**	**62,94 %**

SOLUTIONS IN COMPARISON – HOLIDAY TEST

Solution	Scenario
	Detectionrate Offline for Holiday Test-Szenario
Solution A	**97,89 %**
Solution B	**91,69 %**
Solution C	**84,07 %**
Solution D	**69,03 %**
Solution E	**59,66 %**
Solution G	**57,26 %**
Solution H	**51,46 %**
Solution F	**39,99 %**

All values were collected under the above stated test conditions. Deviations of 1% cannot be excluded.

SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00

SYSTEM RESOURCE CONSUMPTION

In order to evaluate the system resource consumption CPU and memory utilization of the processes belonging to the respective solution were monitored and measured. The system utilization is of course higher during an ongoing attack. However, there were significant differences in how much the load increases for different solutions. Some products had more than 20 active processes to operate the endpoint solution resulting in a negative impact on the total workload of the systems used.

Solution A and Solution B use very few system resources, in normal operation about 1% CPU load and during an ongoing attack up to a maximum of 10% CPU load. The same applies to the memory usage, which is in the range of 20-50 MB maximum.

All other solutions tested consume far more system resources.

The solutions are still quite modest during normal operation with a CPU load of about 2-4%, but during an attack attempt this increases to up to 100% CPU load.

The memory usage rises to several hundred megabytes, in some cases even up to several gigabytes. This renders the computer practically useless at least during the time of the attack.

SUMMARY

The results of the test show a partly significant increase in detection rates, especially with the new versions.

The next-generation solutions were able to approach the one hundred percent mark even further than in previous tests. However, progress was also made in the rest of the test field. The new solutions are still unrivalled in terms of resource consumption. Here, the new generation performs considerably better than any established solution in the test field.

The following diagram shows the results in relation to overall performance.