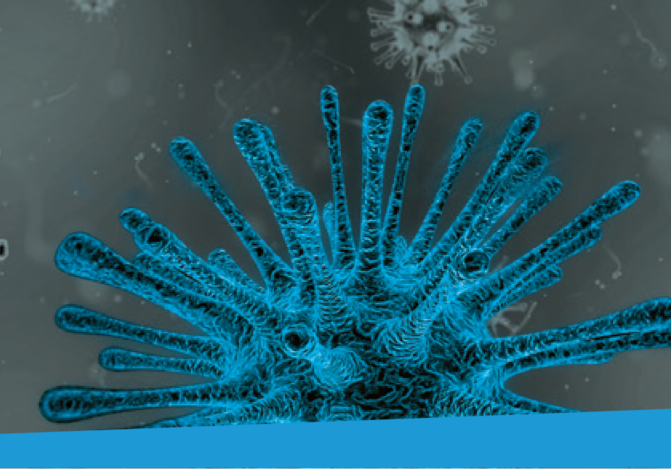
SecureLink



ENDPOINT PROTECTION SOLUTIONS REPORT 10/17

Authors: Kevin Börner, Markus Reiniger, Daniel Vollmer

Endpoint protection solutions must constantly adapt to new threats. Without adaptation, we cannot protect users, endpoints or, ultimately, businesses. The endpoint is usually the last line of defense. This report compares large vendors of recent and existing antivirus solutions with so-called Next-Generation solutions. Is the detection rate of traditional AV products still sufficient, will new approaches and technologies offer a significant advantage against known, unknown and new malware?

EPSR, October 2017

This report is the third edition, collecting even more malware samples compared to previous reports to emphasis the results' significance. The tested AV products were updated to their latest available versions.

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

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

All products are registered as AV manufacturers at Microsoft. The test scenarios were based solely on protection against malware. The samples were installed on systems before beginning the test. Other relevant protection components for protection against cyber attacks – including browser security, protection against malicious e-mails and perimeter protection – were not part of this test.

TESTED SOLUTIONS

Next-Generation Solutions

CylancePROTECT Version 1450 (2.0.1450.8)
Cylance primarily uses AI with machine learning techniques to detect malware and exploits. AI recognises whether a file is benign or malicious by using static analysis of executables and DLLs without having to execute the malware itself (pre-execution and predictive). In addition to the AI, Cylance employs other protection modules and functions to protect the endpoint; these include Script Control against scripts or macros (often used in ransomware attacks) and Memory Protection to protect against exploits in software.

Palo Alto Networks Traps Advanced Endpoint Protection 4.1 (v4.1.0.28239, 21-1729)
Traps, part of the Palo Alto Networks security platform, uses a unique multi-method prevention approach that protects against both known and unknown malicious executables, DLLs and files. This approach maximise protection against unknown malware and exploits while simultaneously reducing the area of attack.

By combining a wide range of deterrence methods, Traps stops malware from compromising a system. Script-based attacks are prevented out-of-the-box.

The centerpiece of the client's malware prevention is local analysis, which protects the system without conventional signatures, scan functions or behavioural analyses. Traps scans hundreds of file properties in real-time. On the basis of these properties, machine learning is used to determine whether a file is benign or malicious. Traps immediately stops ransomware in case of an attack, thereby preventing data encryption. The multi-method exploit prevention is designed to prevent exploits through modules such as Pre-Exploit Protection, Technique-Based Exploit Prevention and Kernel Privilege Escalation Protection.

Sophos Endpoint Protection 2017 (11.5.6) with Intercept X (3.7.0)
Intercept X extends Sophos' anti-virus protection to include threat and exploit detection. Unauthorised encryption (such as ransomware) is prevented by the CryptoGuard module. These technologies enable Intercept X to detect and prevent zero-day malware in advance, complementing the signature-based AV protection.

Conventional Solutions

Kaspersky Endpoint Security 10 (10.3.0.6294)
Kaspersky Endpoint Security offers protection for PC, Mac and mobile devices. The protection modules are similar to modules used by Symantec EP 14. Endpoint has an integrated AV scanner with a signature database with the ability for heuristic analysis of files. Kaspersky also offers additional modules, such as a password manager, mobile device security, firewall functionality and program control.

McAfee Endpoint Security 10.5 (10.5.2.2041)
McAfee offers machine-learning techniques in addition to its AV scanner. The searches are divided into static and behavioral analyses. To supplement its protection, firewall modules and web control are also included. Threat prevention modules also provide protection against exploits.

Symantec Endpoint Protection Cloud 22 (22.10.1.10)
Symantec provides new and improved recognition features in addition to the conventional signature database. Modules such as behavioral analysis, machine-learning and static analysis are used to detect malware.

Trend Micro Office Scan 12 (12.0.1556)
OfficeScan uses a signature-based AV scanner, similar to other conventional solutions. With this latest version, additional machine learning techniques have been used to analyse files before execution. Behavioral analyses of scripts and browser attacks are also carried out.

Windows Defender from Microsoft (1.251.959.0)
Windows Defender delivers 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 of the above-tested software offer a central management console (in the cloud and 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

The number of malware samples tested was greatly increased compared to the previous reports. A total of 8,000 malware samples were used in the first and second test phases, hereinafter referred to as Basic Test and Holiday Test. In the Basic Test, the 8,000 samples were first tested offline then online. The machines were reset between the tests.

A quarter of the samples were downloaded from sources without being altered. These samples were subsequently modified (obfuscated) several times after an initial analysis and mutated in three ways to simulate unknown and zero-day malware.

Usually, these altered files were no longer recognised by signature-based methods. For a basic mutation, the hash value of the files had been changed. Two advanced mutations-packing techniques for executable files used software packers such as UPX and mPress. The Basic Test used 2,000 original files, 2,000 hash-changed files, 2,000 UPX-packed files and 2,000 mPress-packed files.

Test Methodology

Basic Test
The key criterion for testing the endpoint security solutions was recognition rate (effectiveness). All Endpoint Security solutions were tested under the same conditions in the iT-CUBE test lab over 14 days. Test Methodology included, inter alia:

- Signature databases and all other modules updated to the latest available versions.
- Internet connection was provided to enable the AV solutions to access reputation databases, intelligence in the cloud and sandboxes.
- Using a scanning function, malware samples were scanned before execution and the detection rate was determined.
- The remaining samples were then executed (Execution Test).
- For executed malware to perform C2 communication and loading of additional malicious code, internet access was enabled (detection rate online).
- In addition, a test was performed with all samples without 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 came from various public sources: *http://malwr.com*, *http://dasmalwerk.com*, *http://malc0de.com/database*, *http://testmyav.com*, *http://virustotal.com*

Holiday Test
The second test scenario was the Holiday Test. Test devices were disconnected from the internet 14 days prior to the test and were no longer updated. Then the 8,000 malware samples were copied to the systems and scanned. This test represented a realistic scenario in which an employee returned from vacation and was infected with malware before the signature databases could be updated. This 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

The newest solutions from Palo Alto Networks with Traps and Cylance with CylancePROTECT consistently reached very high detection rates (Traps 99.8% and Cylance 99.7%). Sophos with Intercept X reached 87.3%.

The Holiday Test confirmed the effectiveness of signature-free approaches of Palo Alto Networks and Cylance. Other solutions did not provide adequate protection without continually updating their signature databases or without internet access.

The results showed that an enhanced multi-method prevention approach, new content updates and the new Anti-Ransomware protection of Palo Alto Networks version 4.1 were able to demonstrate its benefits.

Degree of maturity of the AI model from CylancePROTECT again shows high reliability and very high consistent recognition rates – all without execution of a file.

Conventional AV-Solutions

Regarding conventional AV solutions, the sole use of signature databases would not have been sufficient; for example, Trend Micro would have achieved a detection rate of only 25%. Using additional modules – static analysis, behavioural analysis and privacy surveys – significantly higher rates of almost 70% to 90% were reached (Kaspersky and Sophos). However, these are still far behind the endpoint solutions of Palo Alto Networks and Cylance.

The test candidates McAfee and Trend Micro were disappointing. Despite using innovative technologies and modules, both failed to achieve satisfactory recognition rates. The products were not convincing. The Windows Defender, as a cost-free protection integrated in Microsoft Windows, was included into the test as a reference. Surprisingly, Windows Defender was partially able to outperform other manufacturers.

SOLUTIONS IN COMPARISON – BASIC TEST

Solution	Scenario			
	Detection rate before execution offline	Detection rate before execution online	Detection rate at execution offline	Detection rate at execution online
Palo Alto Networks Traps 4.1.0	*See **	*See **	99.81 %	99.79 %
CylanceProtect 1450	98.66 %	99.73 %	98.66 %	99.73 %
Kaspersky Endpoint Security 10	75.84 %	76.30 %	93.88 %	94.24 %
Sophos Endpoint Protection 2017 (11.5.6) with Intercept X (3.7.0)	53.38 %	72.06 %	65.73 %	87.34 %
Symantec Endpoint Protection Cloud	51.06 %	56.31 %	60.13 %	68.48 %
McAfee ENS 10.5	45.40 %	47.05 %	60.25 %	63.81 %
TrendMicro OfficeScan	25.13 %	28.19 %	55.41 %	59.39 %
Windows Defender	37.90 %	38.16 %	48.05 %	48.38 %

** A scanning functionality currently exists for standard and golden images. Roadmap Sessions are organised on request from Palo Alto Networks.*

SOLUTIONS IN COMPARISON – HOLIDAY TEST

Solution	Scenario
	Detection rate Offline for Holiday Test-Scenario
Palo Alto Networks Traps 4.1.0	99.81 %
CylancePROTECT 1450	98.66 %
Kaspersky Endpoint Security 10	75.59 %
Sophos Endpoint Protection 2017 (11.5.6) with Intercept X (3.7.0)	47.30 %
McAfee ENS 10.5	45.21 %
Trend Micro OfficeScan	25.26 %
Symantec Endpoint Protection Cloud	17.04 %
Windows Defender	11.81 %

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

SYSTEM RESOURCE CONSUMPTION

To evaluate the system resource consumption CPU and memory utilization, processes belonging to the respective solutions were monitored and measured. The system utilisation is, of course, higher during an ongoing attack. However, there were significant differences in how much the load increased 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.

CylancePROTECT and Palo Alto Networks Traps used 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 applied to the memory usage, which was in the range of 20–50 MB maximum.

All other solutions tested consumed far more system resources.

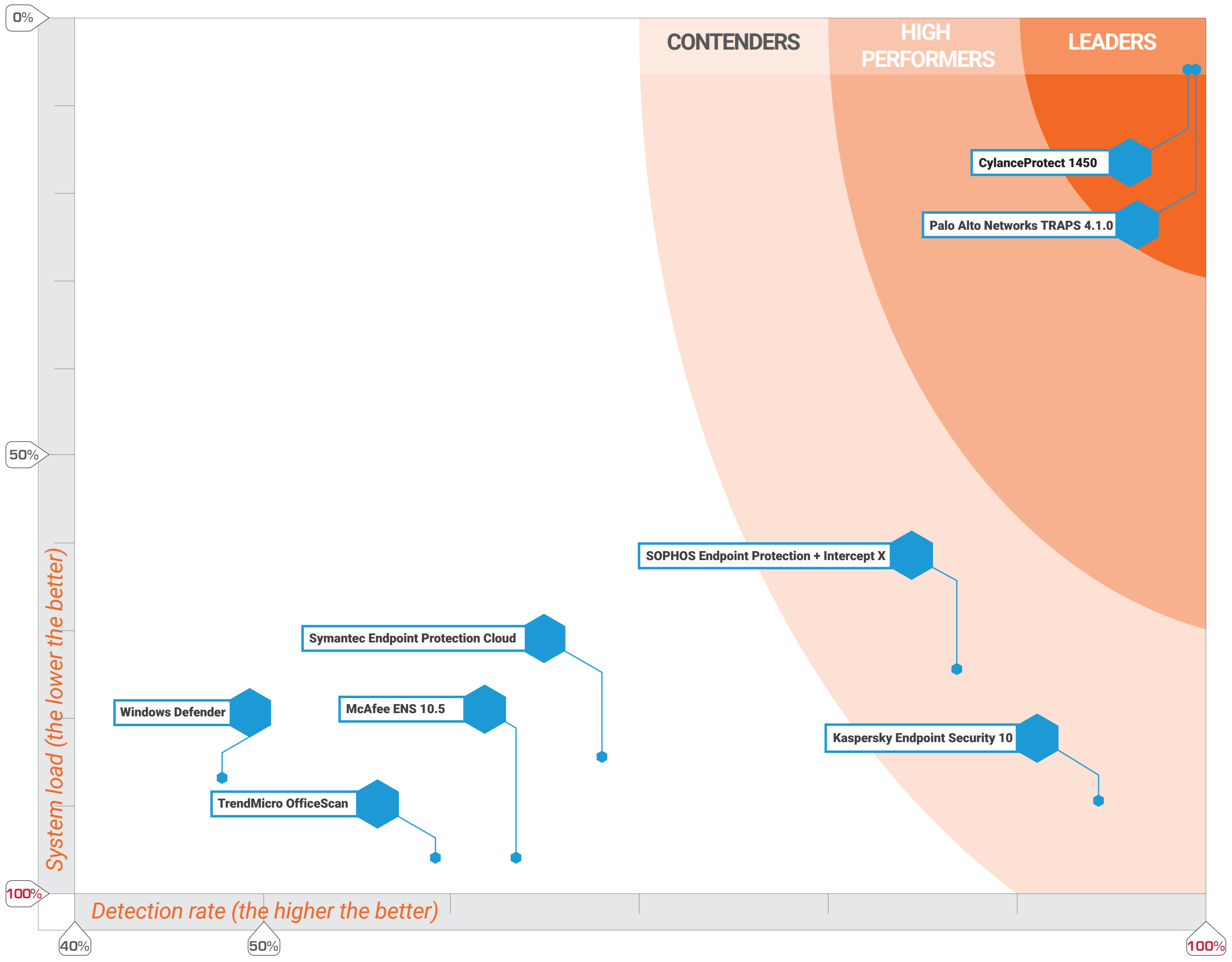
The solutions were still quite modest during normal operation, with a CPU load of about 2–4%, but during an attack attempt, this increases to up to 100% CPU load. The memory usage rose to several hundred megabytes, and in some cases, even several gigabytes. This renders the computer practically useless, at least during the time of the attack.

SUMMARY

The results of this test show a significant increase in detection rates, especially when using the latest versions.

The next-generation solutions came even closer to a 100% detection rate than during the first two tests. However, the rest of the tested solutions also improved. The new solutions are still unrivalled concerning system resource consumption. The new generation gets significantly better results than any of the conventional solutions.

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


System load (the lower the better)
Detection rate (the higher the better)
CONTENDERS
HIGH PERFORMERS
LEADERS
CylanceProtect 1450
Palo Alto Networks TRAPS 4.1.0
SOPHOS Endpoint Protection + Intercept X
Symantec Endpoint Protection Cloud
Windows Defender
McAfee ENS 10.5
Kaspersky Endpoint Security 10
TrendMicro OfficeScan