Anti-Virus Comparative

Symantec Endpoint Protection 14.0

Language: English
October 2016
Last revision: 2nd December 2016

http://www.av-comparatives.org
http://www.mrg-effitas.com

Commissioned by Symantec

Introduction

For this assessment, MRG Effitas and AV-Comparatives combined their strengths to conduct a joint test. The Malware Protection Test was performed by AV-Comparatives, and the Exploit Test was performed by MRG Effitas. This test was commissioned by Symantec.

General

Malicious software poses an ever-increasing threat, not only because the number of malware programs are increasing, but also due to the continuously changing threat-landscape. Attackers are targeting users: deceiving them into visiting infected web pages, through cyber espionage, ransomware, and malicious attachments in email. To address this change in threat-landscape, the endpoint protection solutions must evolve. Gone are the days when traditional antivirus programs using signatures and heuristics are enough. Instead endpoint protection is being strengthened by URL-blockers, content filtering, reputation systems, cloud-based methodologies and user-friendly behavior-blockers. When all these technologies work in coordination, protection against threats increase. It is important to realize that not all malware enters computer systems via the internet, so you cannot rely on one technology alone for adequate protection. All threat surfaces must be protected. For example, a URL blocker is ineffective against malware introduced onto a PC via a USB flash drive or over the local area network. Therefore, as a part of this report, we measured the effectiveness of 7 different products on several different attack vectors, ranging from internet based attacks, like real-world attacks and exploits, as well as attacks that use other medium to enter the environment.

Tested Products

The following products and versions/builds (chosen by Symantec) were tested under Windows 10 64-bit and included in this report:

Vendor	Product	Version
SentinelOne	Endpoint Protection	1.6.2.5020
Cylance	CylancePROTECT	1.2
Sophos	Endpoint Security and Control	10.6
Trend Micro	OfficeScan	11.0 SP3
McAfee	VirusScan Enterprise with ePO	10.2
Microsoft	Windows Defender for Enterprise	4.10
Symantec	Endpoint Protection	14.0.1214[1]

Settings

Some products required configuration changes for the tests. The changes were as follows:

SentinelOne: *Show Suspicious Activities* enabled, *Auto Immune* enabled, *Actions* set to *Quarantine*.

[1] At the time of the test, 14.0.1214 was a beta build of Symantec Endpoint Protection. Since then, Symantec Endpoint Protection 14 was publicly launched on Nov 1st.

Overview

In this test, the protection offered by the products were evaluated. The tests were performed from September till October 2016.

The following tests were performed:

Exploit Test: 21 exploits have been used in the Exploit test.

Whole-Product-Dynamic Test (WPDT): 50 malicious websites were tested by using our **Real-World Testing** Framework, which simulates the activities of a typical computer user (whether at home or in the office) surfing the Internet.

RTTL: 500 most prevalent malicious samples according to the AMTSO Real-Time Threat List (RTTL) were **executed** on the system.

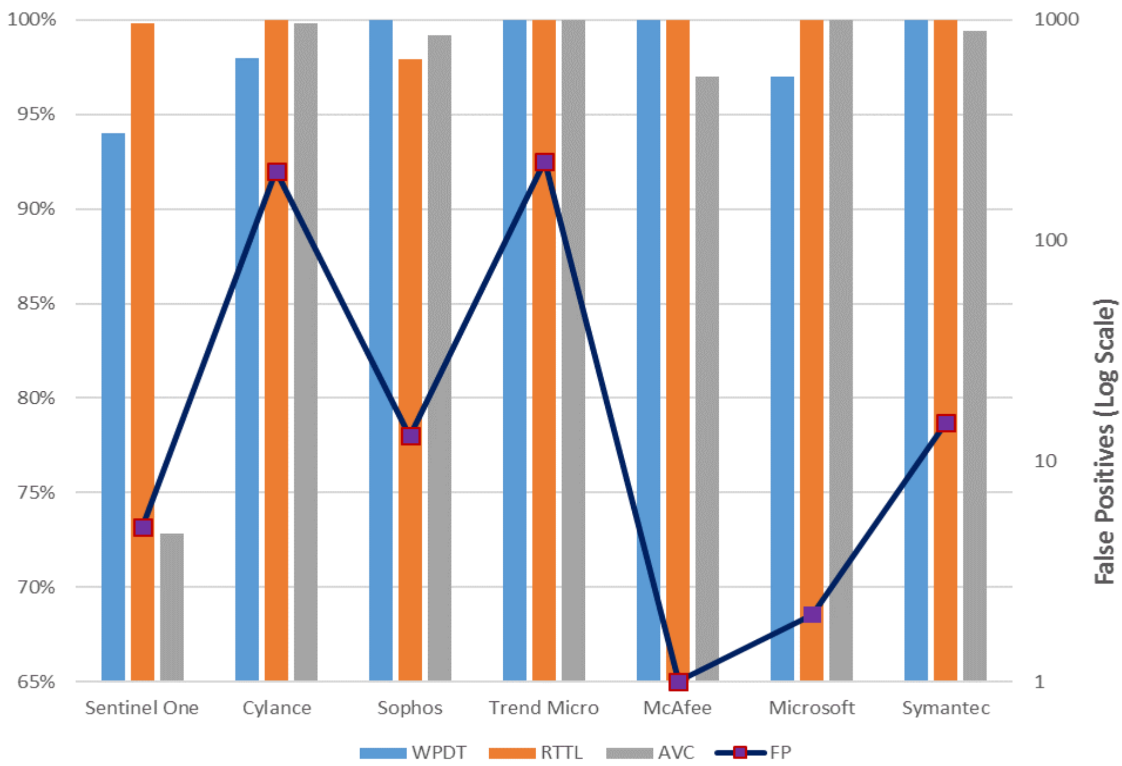
AVC: 500 most recent and prevalent malicious samples from our own database were **executed** on the system.

FPs: 1000 clean files were **executed** on the system and the number of false alarms was recorded.

Results

Malware Protection Test

The following chart shows the results of the malware protection test.



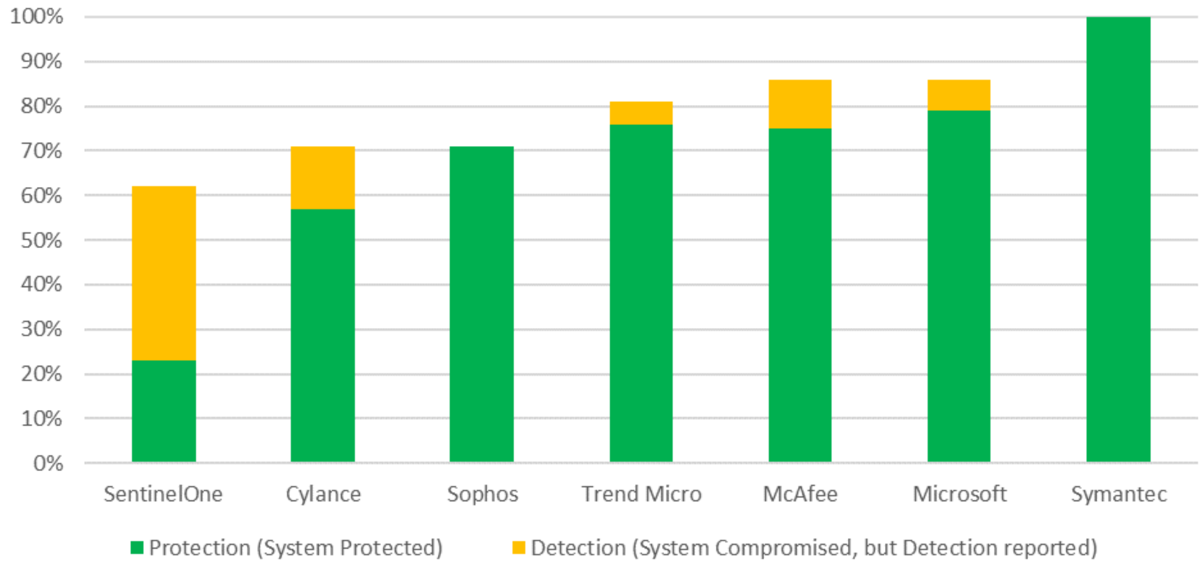
	WPDT	RTTL	AVC	FPs
SentinelOne	94%	99.8%	72.8%	0.5%
Cylance	98%	100%	99.8%	20.6%
Sophos	100%	97.9%	99.2%	1.3%
Trend Micro	100%	100%	100%	22.9%
McAfee	100%	100%	97.0%	0.0%
Microsoft	97%	100%	100%	0.2%
Symantec	100%	100%	99.4%	1.5%

Antimalware efficacy is not just about which vendor protects the most. Rather it should be viewed as an optimization problem where the 3 orthogonal dimensions are protection efficacy, accuracy (false positive percentage) and performance.

Symantec Endpoint Protection 14.0 struck the best balance of high efficacy and low false positives in this test. This ensures high stopping power against malware without operational overhead of false positives.

Exploit Protection Test

	Protected	Detected
SentinelOne	23%	62%
Cylance	57%	71%
Sophos	71%	71%
Trend Micro	76%	81%
McAfee	75%	86%
Microsoft	79%	86%
Symantec	100%	100%



Among the above tested products, Symantec Endpoint Protection 14 was the only product that garnered 100% for both protection and detection in the Exploit Protection Test.

Attackers are quick to take advantage of vulnerabilities in common software to gain a foothold in an organization. Given that it may take up to a month to obtain and implement a patch leaves organizations open to attack for far too long. The ability to block the attack on day 0 is critically important for not only endpoint security, but the organization's security posture in general. We used several popular exploit kits (like, Sundown, Neutrino, Metasploit, etc.) and used exploits that were targeting Adobe Flash, Internet Explorer, Microsoft Office (macro), Silverlight, Firefox and Java.

Scoring / Calculation of Results

Scoring Of The Exploit Protection/Detection Results

We defined the following stages, where the exploit could have been prevented by the endpoint protection system:

1. Blocking the URL (infected URL, exploit kit URL, redirection URL, malware URL) by the URL database (local or cloud). For example, a typical result is the browser displaying a “site has been blocked” message by the endpoint protection. The sooner the threat is detected in the exploit chain, the easier it is to remove the malicious files from the system, the less information can be gathered from the system by the attackers, and there is less risk of an attack targeting the particular security solution on an endpoint.

2. Analyzing and blocking the page containing a malicious HTML code, JavaScripts (redirects, iframes, obfuscated JavaScripts, etc.), or Flash files.

3. Blocking the exploit before the shellcode is executed.

4. Blocking the downloaded payload by analyzing the malware before it is started. For example, the malware payload download (either the clear-text binary or the encrypted/encoded binary) can be seen in the proxy traffic, but no malware process starts.

5. The malware execution is blocked (no process create, load library).

6. There was a successful start by the dropped malware.

7. There was a successful start by the dropped malware, but eventually, all dropped malware was terminated and deleted (“malware starts, but blocked later”).

The "protection" score was calculated as follows:

- 5 points were given to the product if no malicious, untrusted code was able to run on the endpoint. This could have been achieved by blocking the exploit in steps 1, 2, or 3 above.
- 4 points were given to the product if malicious, untrusted code ran on the endpoint (exploit shellcode, downloader code), but the final malware was not able to start. This could have been achieved by blocking the exploit in steps 4 or 5 above.
- 0 points were given to the product if both the exploit shellcode (or downloader code) and the final malware was able to run on the endpoint.

The "detection" score was calculated as follows:

- 1 point was given to the product if at any stage of the infection a medium or high severity alert was generated (even if the infection was not prevented).

We used this scoring for the following reasons:

- The scope of the test was exploit prevention and not the detection of malware running on the system.
- It is not possible to determine what kind of commands have been executed or what information exfiltrated by the malware. Data exfiltration cannot be undone or remediated.
- It cannot be determined if the malware exited because the endpoint protection system blocked it, or if malware quit because it detected monitor processes, virtualization, or quit because it did not find its target environment.
- Checking for malware remediation can be too time-consuming and remediation scoring very difficult in an enterprise environment. For example, in recent years we experienced several alerts that the endpoint protection system blocked a URL/page/exploit/malware, but still the malware was able to execute and run on the system. On other occasions, the malware code was deleted from the disk by the endpoint protection system, but the malware process was still running, or some parts of the malware were detected and killed, while others were not.
- In a complex enterprise environment multiple network and endpoint products protect the endpoints. If one network product alerts that malicious binary has been downloaded to the endpoint, administrators have to cross-check the alerts with the endpoint protection alerts, or do a full forensics investigation to be sure that no malware was running on the endpoint. This process can be time and resource consuming, which is why it is better to block the exploit before the shellcode starts.
- Usually the exploit shellcode is only a simple stage to download and execute a new piece of malware, but in targeted attacks, the exploit shellcode can be more complex.

We believe that such zero-tolerance scoring helps enterprises to choose the best products, using simple metrics. Manually verifying the successful remediation of the malware in an enterprise environment is a very resource-intensive process and costs a lot of money. In our view, malware needs to be blocked before it has a chance to run, and no exploit shellcode should be able to run.

Test Procedure / Methodology

Exploit Test Setup

Testing Cycle for Each Test Case

1) One default installation of Windows 10 64-bit on a virtual machine (VirtualBox) endpoint was created. The default HTTP/HTTPS proxy was configured to point to a proxy running on a different machine. SSL/TLS traffic was not intercepted on the proxy.

2) The security of the OS was weakened by the following actions:
   a) Microsoft Defender was disabled
   b) Internet Explorer SmartScreen was disabled
   c) Vulnerable software was installed, see "Software Installed" for details.
   d) Windows Update was disabled

3) From this point, different snapshots were created from the virtual machine, several with different endpoint protection products and one with none. This procedure ensured that the base system was exactly the same in all test systems.

   The following endpoint security suites, with the following configuration, were defined for this test:

   a) No additional protection (this snapshot was used to infect the OS and to verify the exploit replay)
   b) Product 1 installed
   c) Product 2 installed
   d) …

The endpoint systems were installed with default configuration, potentially unwanted software removal was enabled, and if it was an option during install, cloud/community participation was enabled.

4) The exploit sources can be divided into two categories. In-the-wild threats and Metasploit. VBscript based downloaders and Office macro documents were also in scope, as these threats are usually not included in other test scenarios.

5) The virtual machine was reverted to a clean state and traffic was replayed by the proxy server. The replay meant that the browser was used as before, but instead of the original webservers, the proxy server answered the requests based on the recorded traffic. When the "replayed exploit" was able to infect the OS, the exploit traffic was marked as a source for the tests. This method guarantees that exactly the same traffic will be seen by the endpoint protection systems, even if the original exploit kit goes down during the tests. This exploit replay is NOT to be confused with tcpreplay type replay.

6) After new exploit traffic was approved, the endpoint protection systems were tested. Before the exploit site was tested, it was verified that the endpoint protection had been updated to the latest version with the latest signatures and that every cloud connection was working. If there was a need to restart the system, it was restarted. In the proxy setup, unmatched requests were allowed to pass through and SSL/TLS was not decrypted to ensure AV connectivity. VPN was used during the test on

the host machine. When user interaction was needed from the endpoint protection (e.g. site visit not recommended, etc.), the block/deny action was chosen. When user interaction was needed from Windows, we chose the run/allow options. No other processes were running on the system, except the Process Monitor/Process Explorer from SysInternals and Wireshark (both installed to non-default directories).

7) After navigating to the exploit site, the system was monitored to check for new processes, loaded DLLs or C&C traffic.

8) The process went back to step 5, until all exploit site test cases were reached.

The following hardware was dedicated to the virtual machine:

- 4 GB RAM memory
- 2 processors dedicated from AMD FX 8370E CPU
- 65 GB free space
- 1 network interface
- SSD drive

The VirtualBox host and guest system for the exploit test had been hardened in a way that common virtualization and sandbox detection techniques could not detect the system as an analysis system.

Analysis Of The Exploit Kits Used In The Exploit Test

While there weren't very many newly disclosed exploits during the test duration for the OS configuration tested, we chose to use Metasploit and Neutrino kits to compare endpoint solutions' effectiveness against exploits.

We also used two specific samples that are non-PE downloaders, like an Office macro and a WSF downloader. We specifically added these "egsotic" file-types here, as these are quite prevalent in-the-wild, but often excluded from real world tests.

A total of 21 test cases were tested.

- 8 Sundown EK
- 5 Neutrino EK
- 4 Metasploit
- 1 Powershell Empire
- 1 Metasploit Macro
- 1 Locky malspam WSF
- 1 unknown EK

These exploit kits were targeting Adobe Flash, Internet Explorer, Microsoft Office (macro), Silverlight, Firefox and Java.

Software Installed

For the exploit test, the following vulnerable software were installed:

Vendor	Product	Version		Vendor	Product	Version
Adobe	Flash Player ActiveX - builtin	21.0.0.182		Microsoft	SilverLight	5.1.10411.0
AutoIT	AutoIT	3.3.12.0		Mozilla	Firefox	31.0
Microsoft	Internet Explorer	11.162.10586		Oracle	Java	1.7.0.17
Microsoft	Office	2016				

Scoring of the Malware Protection Results

The scoring for malware protection was straightforward:

- 0 points were given the product if the system was compromised by the malware
- 1 point was given the product if the malware was blocked or remediated
- 0.5 points were given the product if a pop-up prompted the user for a decision

False positive test

The same scoring principle as described above has been applied for the false alarms test. In this test, 1000 non-malicious applications were used.

Copyright and Disclaimer

For more information about AV-Comparatives / MRG Effitas and the testing methodologies please visit our website.

AV-Comparatives / MRG Effitas (December 2016)